A-LIGN

PlanSource Benefits Administration, Inc.

Type 1 Attestation
(AT-C 105, AT-C 205 and AT-C 315)
HIPAA/HITECH

2023

PLANSOURCE

Table of Contents

SECTION 1

ASSERTION OF PLANSOURCE BENEFITS ADMINISTRATION, INC. MANAGEMENT

ASSERTION OF PLANSOURCE BENEFITS ADMINISTRATION, INC. MANAGEMENT

July 15, 2023

We have prepared the description of PlanSource Benefits Administration, Inc.'s ('PlanSource') health information security program for the Human Capital Management (HCM) and BenAdmin Services Systems (the "description") for user entities of the system as of June 30, 2023. We confirm, to the best of our knowledge and belief, that:

a. Management's description fairly presents the health information security program for the HCM and BenAdmin Services Systems as of June 30, 2023. The criteria we used in making this assertion were that the description:
   i. fairly presents how the health information security program was designed and implemented to govern the security policies and practices supporting the HCM and BenAdmin Services Systems.
   ii. describes the specified controls within the security program designed to achieve the security program's objectives.
   iii. does not omit or distort information relevant to the health information security program for the HCM and BenAdmin Services Systems and may not include every aspect that an individual user entity may consider important in its own particular environment.

b. The health information security program governing the HCM and BenAdmin Services Systems complied with applicable requirements of HIPAA and HITECH. The criteria we used in making this assertion were that:
   i. management determined the applicable controls (the "controls") included in the health information security program.
   ii. the controls documented complied with the standard and implementation guidance for safeguards as defined by the HIPAA Security Rule including the following:
      - Administrative Safeguards
      - Physical Safeguards
      - Technical Safeguards
      - Organizational Requirements
      - Breach Notification
   iii. the controls stated in the description were suitably designed and implemented as of June 30, 2023, to provide reasonable assurance that the applicable HIPAA and HITECH requirements would be met, if its controls operated effectively as of that date and if the subservice organizations and user entities applied the complementary controls assumed in the design of PlanSource's controls as of that date.

Section 3 of this report includes PlanSource's description of the health information security program for the HCM and BenAdmin Services Systems that is covered by this assertion.

Justin Kazmark
Vice President of Vendor Management
PlanSource Benefits Administration, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To PlanSource Benefits Administration, Inc.:

We have examined PlanSource's description of its health information security program for the PlanSource's HCM and BenAdmin Services Systems listed in Section 3 (the "description"), and its health information security program governing the HCM and BenAdmin Services Systems' compliance with applicable requirements of the Health Insurance Portability and Accountability Act Security Rule of 2003 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH"), enacted as part of the American Recovery and Reinvestment Act of 2009 ("HIPAA/HITECH requirements"). PlanSource's management is responsible for its assertion. Our responsibility is to express an opinion about PlanSource's compliance with the specified requirements based on our examination.

PlanSource uses Amazon Web Services, Inc. ('AWS') for disaster recovery services, DataSite for colocation services, SecureWorks, Inc. ('SecureWorks') for managed security services, and Ultimate Software Group, Inc. ('Ultimate Software') for HCM platform application development and hosting services (collectively, the 'subservice organizations'). The description indicates that certain applicable HIPAA/HITECH requirements can only be met if controls at the subservice organizations are suitably designed. The description presents PlanSource's system; its controls relevant to the applicable HIPAA/HITECH requirements; and the types of controls that the service organizations expect to be implemented, and suitably designed at the subservice organizations to meet certain applicable HIPAA/HITECH requirements. The description does not include any of the controls implemented at the subservice organizations. Our examination did not extend to the services provided by the subservice organizations.

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 supporting the fairness of the presentation of the description and the design of PlanSource's health information security program for the HCM and BenAdmin Services Systems and performing such other procedures as we considered necessary in the circumstances. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether management's assertion about compliance with the specified requirements is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about whether management's assertion is fairly stated, in all material respects. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risks of material misstatement of management's assertion, whether due to fraud or error. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination does not provide a legal determination on PlanSource compliance with the specified requirements.

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

A-LIGN ASSURANCE did not perform procedures regarding the operating effectiveness of the controls stated in the description and, accordingly, do not express an opinion thereon. Because of their nature, controls at a service organization may not prevent, or detect and correct, all errors or omissions relevant to meet the applicable HIPAA/HITECH requirements. 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 meet the applicable HIPAA/HITECH requirements is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

In our opinion, in all material respects, based on the criteria described in PlanSource's assertion in Section 1:

a. The description fairly presents the health information security program for the HCM and BenAdmin Services Systems that was designed and implemented as of June 30, 2023;
b. The health information security program governing the HCM and BenAdmin Services Systems complied with applicable requirements of HIPAA and HITECH; and
c. the controls stated in PlanSource's description were suitably designed and implemented as of June 30, 2023, to provide reasonable assurance that the applicable HIPAA and HITECH requirements would be met, if its controls operated effectively as of that date and if the subservice organizations and user entities applied the complementary controls assumed in the design of PlanSource's controls as of that date.

This report is intended solely for the information and use of PlanSource; user entities of PlanSource's HCM and BenAdmin Services Systems as of June 30, 2023; and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, subservice organizations, or other parties
- Internal control and its limitations
- Complementary user-entity controls and complementary subservice organization controls and how they interact with related controls at the service organization to meet the HIPAA/HITECH requirements
- The HIPAA/HITECH requirements
- The risks that may threaten the achievement of the HIPAA/HITECH requirements and how controls address those risks

This report is not intended to be and should not be used by anyone other than these specified parties.

A-LIGN ASSURANCE

Tampa, Florida
July 15, 2023

SECTION 3

PLANSOURCE BENEFITS ADMINISTRATION, INC.'S DESCRIPTION OF ITS HCM AND BENADMIN SERVICES SYSTEMS AS OF JUNE 30, 2023

OVERVIEW OF OPERATIONS

Company Background

PlanSource was founded in early 2007 and offers benefits and Human Resources (HR) professionals a means to select, implement and manage employee benefit programs for growing and medium-sized businesses. The company offers a platform capable of delivering self-service functionality in the areas of insurance procurement, customer onboarding, online enrollment, consolidated billing, and ongoing administration. The technology is designed to enable employers, brokers and insurance carriers to offer, enroll and manage a complete portfolio of employee benefits, healthcare products, and services.

Description of Services Provided

PlanSource BenAdmin

The PlanSource BenAdmin system provides employers with an online technology platform for benefits enrollment and year-round benefits management. It provides brokers with access to a broker portal where they can receive quotes from PlanSource's portfolio partners, configure administrator and employee sites for benefit content management and online enrollment, and perform day-to-day BenAdmin and management functions including premium billing. Brokers are the primary clients of PlanSource who then distribute the products throughout their client base.

There are three different models for delivering PlanSource BenAdmin Services:

Licensed BenAdmin

The broker provides the system to clients as a BenAdmin tool and performs the setup and support. The employer or broker performs day-to-day administration. The broker is also responsible for programming data feeds to carriers.

Co-Sourced BenAdmin

The broker provides the system to clients as a BenAdmin tool and performs the setup and support with PlanSource handling the data feeds and premium billing. The employer or broker performs day-to-day administration.

Outsourced BenAdmin

The broker provides the system to clients as a BenAdmin tool; however, PlanSource performs the setup, support, data feed management, and premium billing. The employer or broker performs day-to-day administration.

Human Capital Management (HCM)

The HCM platform helps customers to develop and implement HR and benefits strategies based on real-time business analytics and best practices. The employee and manager can access the information they need through the integrated portal. This product, delivered as HCM, combines payroll, benefit, and Human Resource Management (HRMS) technologies. To administer the benefits programs, PlanSource utilizes the proprietary, web-based BenAdmin technology integrated with the payroll and HRMS software. This solution allows customers to pass payroll and benefits data back and forth in real-time.

Principal Service Commitments and System Requirements

PlanSource designs its processes and procedures related to HCM and BenAdmin Services to meet its objectives for its HCM and BenAdmin Services. Those objectives are based on the service commitments that PlanSource makes to user entities, the laws and regulations that govern the provision of HCM and BenAdmin Services, and the financial, operational, and compliance requirements that PlanSource has established for the services. The HCM and BenAdmin Services of PlanSource are subject to the security and privacy requirements of the Health Insurance Portability and Accountability Act (HIPAA) Administrative Simplification, as amended, including relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which PlanSource operates.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offered provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the HCM and BenAdmin services that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Use of encryption technologies to protect customer data both at rest and in transit.

PlanSource establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in PlanSource's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the HCM and BenAdmin Services.

Components of the System

Infrastructure

The HCM and BenAdmin Services Systems is limited to the services and infrastructure maintained by PlanSource at the Orlando, Florida; Charleston, South Carolina; Salt Lake City, Utah, USA and Bangalore India locations. The physical production systems are located at the DataSite Orlando (DataSite) third-party data center. DataSite is responsible for providing physical and environmental security that includes a secured data center facility with environmental control systems. The physical backup and disaster recovery systems are located at the AWS third-party data center. AWS is responsible for the physical and environmental security of those systems.

PlanSource's production systems are supported on physical and virtual machines. Multiple, redundant firewalls are implemented on the network perimeter to filter incoming traffic. In addition, an Intrusion Prevention System (IPS) and Intrusion Detection System (IDS) are in place to analyze network traffic, block suspected network security breaches and detect inappropriate, incorrect or anomalous activity. The IPS and IDS are managed and monitored by SecureWorks. SecureWorks is responsible for monitoring of PlanSource's network IPS and IDS, analyzing network events, and reporting possible or actual network security breaches to PlanSource's information security personnel. Potential or actual network security breach incidents are reported by SecureWorks via e-mail and/or phone (depending on the severity of the security incident) and are reviewed by PlanSource's information security personnel.

Primary infrastructure used to provide PlanSource's HCM and BenAdmin Services Systems includes the following:

Primary Infrastructure			
Hardware	**Type**	**Purpose**	**Physical Location**
PlanSource Benefits Application	Web-based, in-house developed application that manages benefits transactions, and educates employees through a self-service website that can be accessed by employers, employees, insurance carriers, and brokers	CentOS (64-bit) and Ubuntu (64- bit) including Percona / My Structured Query Language (SQL)	DataSite
UltiPro (HCM) Application	A third-party application that is utilized to support the HCM Services and is developed and maintained by Ultimate Software	Windows .NET implementation	Not applicable. maintained by Ultimate Software
Benefits Application Backup Servers	Servers that provide backup and recovery	CentOS (64 bit) and Ubuntu (64- bit)	AWS
Virtual Hypervisor	Provides authentication and restricts access to virtual hosts	VMWare vCenter	DataSite
Storage Area Network (SAN) Storage	Stores the backup data	Dell EMC	DataSite
Firewall	Firewalls used to filter and route traffic	Cisco ASA	DataSite
Domain Controller	Active Directory restricts access to production systems to authorized and authenticated personnel	Microsoft Windows (64-bit)	DataSite

Software

Primary software used to provide PlanSource's HCM and BenAdmin Services Systems includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
UltiPro	(Hosted by Ultimate)	Primary application for HCM
BenAdmin	Ubuntu Linux	Primary application for PlanSource BenAdmin

People

- Executive Management - Responsible for establishment of product vision, overseeing of company-wide activities, and attainment of business objectives.

Operations Management and Staff - Responsible for client implementation, renewal, account management, and day-to-day customer support. Additionally, monitors and manages inbound and outbound data flows and related processes.

- Information Technology (IT) Department - Manages, monitors, and supports information systems and responsible for day-to-day maintenance of system integrity, security, and availability.
- Software Development - Provides support for internally escalated issues from operations and IT departments.

Data

Data Used and Supported by the System		
Data Description	**Data Reporting**	**Classification**
PlanSource BenAdmin Client data that may include the following (depending upon the scope of services provided): • Employee and Dependent demographic and enrollment data • Payroll data, such as, salary, salary history, organizational structure, job classifications and assignments, payroll schedules, paid time off data, W4 data, etc. • Personal Health Information (PHI) may be collected under certain service arrangements • Benefits and payroll business rules	Provides the following data (depending upon the scope of services provided) in various exports and reports: • Enrollment and participation reports • Dependent and beneficiary data • Eligibility exports • Carrier billing reports • Payroll deductions • Payroll and W-2 data	Confidential
HCM Client data that may include the following (depending upon the scope of services provided): • Payroll data, such as, pay history, direct deposit organizational structure, job classifications and assignments, payroll schedules, paid time off data, W2 data, etc. • Payroll tax filing data	Provides the following data (depending upon the scope of services provided) in various exports and reports: • Payroll processing and exception reports • New hire reports • Payroll tax reports	Confidential

Health Information Security Program Processes, Policies and Procedures

PlanSource has developed a health information security management program to meet the information security and compliance requirements related to HCM and Ben Admin Services and its customer base. The program incorporates the elements of the HIPAA and the Health Information Technology for Economic and Clinical Health Act (HITECH). The description below is a summary of safeguards that PlanSource has implemented to adhere to the applicable components of HIPAA Final Security Rule and the breach notification requirements of HITECH.

Administrative Safeguards - Policies and procedures designed to show how PlanSource complies with the act:

- Management has adopted a written set of health information security policies and designated the information security officer to be responsible for developing and implementing the required policies and procedures.
- Procedures address access authorization, establishment, modification, and termination.
- Documented incident response policies for reporting security incidents are in place to guide employees in identifying, reporting, security incidents.
- Business continuity plans are documented to enable continuation of critical business processes in the event of an emergency.
- Privileged administrative access to systems is restricted to authorized individuals.
- Automated backup systems are in place to perform scheduled replication of production data and systems at pre-defined intervals.
- Antivirus software is utilized to detect and eliminate data or files that contain certain virus signatures on certain production servers.

Physical Safeguards - Controlling physical access to protected data:

- Documented physical security policies and procedures are in place to guide personnel in physical security administration.
- Physical access procedures are in place to restrict access, log visitors, and terminate access to the office facility.
- Inventory listings are utilized to track and monitor hardware and removable media.
- Data destruction procedures are in place to guide the secure disposal of data and media.

Technical Safeguards - Controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient:

- Access to in-scope systems are restricted to authorized personnel based on a valid user account and password.
- Systems are configured to enforce pre-determined thresholds to lock user sessions due to invalid login attempts.
- Security monitoring applications and manual reviews are utilized to monitor and analyze the in-scope systems for possible or actual security breaches.

Organizational Safeguards - Adherence to policies and procedures in regard to PHI documentation availability, as well as documentation retention:

- Documented policies address the confidentiality threshold of PHI documents and the length of time they should be retained before being destroyed.
- Contractual responsibilities by subparts of an organization are written and maintained in contracts.
- Separation of duties exists in order to protect confidentiality, availability, and integrity of PHI.
- Ensure that only appropriate parties gain access to PHI internally and external to the organization.

Breach Notification - A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach:

- Documented policies and procedures are in place to guide personnel in notifying the covered entity upon discovery of a breach.
- Documented policies and procedures are in place to guide personnel in responding to discovery of a breach.
- Documented policies and procedures require disclosure of the unsecured protected health information and include, to the extent possible, the identification of each individual and a description of the event.
- Documented policies and procedures are in place to guide personnel in the exception processes of delaying and documenting notifications.
- Documented policies and procedures are in place to guide personnel in documentation of administrative requirements for demonstrating that notifications were made as required.

Boundaries of the System

The scope of this report includes the Human Capital Management (HCM) and BenAdmin Services Systems performed in the Orlando, Florida; Charleston, South Carolina; Salt Lake City, Utah, USA and Bangalore, India locations facility.

This report does not include the disaster recovery services provided by AWS, the colocation services provided by DataSite in Orlando, Florida, the managed security services (MSS) provided by SecureWorks and the HCM platform application development and hosting services provided by Ultimate Software.

HIPAA/HITECH REQUIREMENTS AND RELATED CONTROLS

Organizational Structure and Assignment of Authority and Responsibility

PlanSource's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. PlanSource's management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility and appropriate lines of reporting. PlanSource has developed an organizational structure suited to its needs. This organizational structure is based, in part, on its size and the nature of its activities. PlanSource'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 business practices, knowledge and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at helping to ensure 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.

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

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.

Risk Assessment Process

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

Risk Identification

PlanSource has considered significant interactions between itself and relevant external parties and risks that could affect the organization's ability to provide reliable service to its user entities. Key members of the internal staff and executive management have identified and documented risks to the system. The process included identification of the business assets and associated business owners, which is followed by establishing threats, vulnerabilities, and risk levels.

Risk Factors

Management considers risks that can arise from both external and internal factors including the following:

External Factors

- Technological developments
- Changing customer needs or expectations
- Competition that could alter marketing or service activities
- New legislation and regulation that could force changes in policies and strategies
- Natural catastrophes that could lead to changes in operations or information systems
- Economic changes that could have an impact on management decisions

Internal Factors

- Significant changes in policies, processes or personnel
- Types of fraud
- Fraud incentives, opportunities and pressures for employees
- Employee attitudes and rationalizations for fraud
- A disruption in information systems processing
- The quality of personnel hired, and methods of training utilized
- Changes in management responsibilities

Risk Analysis

Risk analysis is an essential process to the entity’s success. Each defined threat and vulnerability has been analyzed for controls that mitigate the risk. Risks that are not currently mitigated by controls are analyzed and projects are scheduled to implement controls that mitigate the associated risk. The control activities that are associated with the security, availability, processing integrity and confidentiality principles have been documented in the Testing Matrices.

Integration with Risk Assessment

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of the security, availability, processing integrity, and confidentiality principles.

Periodic Assessments

PlanSource has a risk assessment process in place to identify and manage the risks that could affect the Company's ability to provide services to its user entities. The risk assessment procedure defines the responsibility, methodologies and processes used by PlanSource to assess the risks while providing services and develop mitigation strategies to address those risks. This process requires the Company to identify risk based on management's internal knowledge of its operations. The following risk factors are discussed among the executive management including the Chief Information Security Officer (CISO) and Chief Product and Technology Officer (CPTO) at periodic intervals:

- Risk Assessment: The risk assessment is performed by the risk management personnel. Risk factors associated with the delivery or implementation of services to customers are evaluated considering process owners, dependencies, timelines and quality.
- Health Information Security Risks: Health information security risks are assessed by the CISO and CPTO. Risk factors associated with the organization are evaluated considering compliance obligations, laws and regulations, policies and procedures, contracts and best practices to which the organization has committed to. Information security assessments carried out by risk management personnel are rolled up to the CISO and CPTO of the organization.

Periodic Testing and Evaluation

PlanSource completes evaluations throughout each calendar year regarding the effectiveness of the health information security program that include, but are not limited to, the following:

- Internal risk assessments.
- Corrective action plans.
- Management reviews.

Information and Communications Systems

Internal Communications

PlanSource has implemented various methods of communication to help provide assurance that employees understand their individual roles and responsibilities and that significant events are communicated. These methods include orientation for new employees, training for employees, and the use of e-mail messages to communicate time-sensitive information. Employees are encouraged to communicate with their supervisor/manager or executive management.

If incidents are communicated, personnel follow documented incident response plan. For example, if a change in procedure is required, the project manager is advised of the change. Formal procedure changes are distributed to management before they are incorporated into the policy and distributed to relevant parties. Incidents are documented within the ticketing system and tracked by management until resolved.

External Communications

PlanSource has also implemented various methods of communication to help provide assurance that customers understand the roles and responsibilities in processing their transactions and communication of significant events. These methods include the use of e-mail messages and communication via the assigned account manager for time-sensitive information.

Monitoring Controls

Management's close involvement in operations helps to identify significant variances from expectations regarding internal controls. Senior management immediately evaluates the facts and circumstances related to any suspected control breakdowns. A decision for addressing any controls weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel.

On-Going Monitoring

Examples of PlanSource's ongoing monitoring activities include the following:

- Organizational structure and supervisory activities provide oversight of control functions and identification of deficiencies.
- Regular review of incidents that are reported and documented by the information security team.
- Alert notifications received from automated backup systems and enterprise monitoring software.
- Vulnerability or security alerts received from various sources including security subscriptions, scanning tools, penetration test reports, or automated patching systems.

Reporting Deficiencies

The nature, timing and extent of the incidents identified are documented within an internal SharePoint, for management tracking and review. Deviations or deficiencies associated with controls are immediately escalated to management for immediate correction action. Results of third-party assessments and audits are reviewed by senior management, and corrective action, if required, is assigned to an individual and documented once those required actions are complete.

Policies and Procedures

Health information security policies and procedures have been implemented regarding the protection of information assets. The policies and procedures act as a guide for PlanSource personnel. These policies and procedures define guidelines for the health information security program related to scope of services, which includes implementing and managing logical access security and controls, including the following:

- Asset Management
- Data Classification
- Business Continuity and Disaster Recovery
- Incident Management
- Access Control
- Physical Security

These policies are reviewed and approved by management on an annual basis.

Security Awareness Training

PlanSource employees receive security awareness training for health information security as part of the onboarding process. This training is reinforced by security awareness communications on current issues which are distributed periodically. Additionally, employees are also required to participate in annual security awareness training.

Incident Response

PlanSource maintains a documented incident response plan including breach notification requirements as mandated by HITECH. The procedures include, but are not limited to, the identification, response, escalation, and remediation of security breaches and other incidents. A formal breach notification process is utilized to document and track resolution of incidents noted. The incident response procedures are tested during the normal course of business and are updated as needed.

Remediation and Continuous Improvement

Areas of non-compliance in PlanSource'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, if identified, of internal control non-compliant items should be reported not only to the individual responsible for the function or activity involved, who is in the position to take corrective action. 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 areas of non-compliance in internal control procedures and make the decision for addressing any non-compliant items based on whether the incident was isolated or requires a change in the Company's procedures or personnel.

Changes to the System Since the Last Review

No significant changes have occurred to the services provided to user entities since the organization's last review.

Incidents Since the Last Review

No significant incidents have occurred to the services provided to user entities since the organization's last review.

Requirements Not Applicable to the System

The following HIPAA/HITECH requirements are not applicable to the system:

HIPAA/HITECH Requirements Not Applicable to the System		
Category	**Criteria**	**Control**
Administrative Safeguard	164.308(a)(4)(ii)(A)	The entity is not a healthcare clearinghouse.
	164.308(b)(1)	The entity is not a covered entity.
Physical Safeguard	164.310(c)	The entity is not a covered entity.
Organizational Safeguard	164.314(a)(2)(ii)	The entity is not a government entity.
	164.314(b)(1)	The entity is not a plan sponsor.
	164.314(b)(2)	The entity is not a group health plan.
Breach Notification	164.404(a), 164.404(2), 164.404(b), 164.404(c)(1), 164.404(c)(2), 164.404(d)(1)(i), 164.404(d)(1)(ii), 164.404(d)(2), 164.404(d)(2)(i), 164.404(d)(2)(ii), 164.404(d)(3), 164.406, 164.408(a), 164.408(b), 164.408(c)	The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.

Subservice Organizations

The scope of this report includes the Human Capital Management (HCM) and BenAdmin Services Systems performed in the Orlando, Florida; Charleston, South Carolina; Salt Lake City, Utah, USA and Bangalore, India locations facility.

This report does not include the disaster recovery services provided by AWS, the colocation services provided by DataSite in Orlando, Florida, the MSS provided by SecureWorks and the HCM platform application development and hosting services provided by Ultimate Software.

Subservice Description of Services

AWS provides disaster recovery services which includes implementing physical security controls for the housed in-scope systems. Controls include but are not limited to requiring visitor sign ins, requiring badges for authorized personnel, and monitoring and logging of physical access to the facilities.

DataSite Orlando provides colocation services which includes implementing physical security controls for the housed in-scope systems. Controls include but are not limited to requiring visitor sign ins, requiring badges for authorized personnel, and monitoring and logging of physical access to the facilities.

SecureWorks provides MSS which includes monitoring controls and IDS and IPS management. SecureWorks' IDS and IPS management service provides 24/7 proactive administration, monitoring and maintenance of customer's IDS and IPS infrastructure.

Ultimate Software provides platform hosting services used to host the HCM application. This includes business continuity, physical security and logical security controls for the housed in-scope systems. Controls include but are not limited to monitoring and logging of physical access to the facilities, business continuity and vulnerability management.

Complementary Subservice Organization Controls

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

The following subservice organization controls should be implemented by AWS to provide additional assurance that the Safeguards described within this report are met:

Subservice Organization - AWS		
Safeguard	**Requirement**	**Control**
Physical Safeguard	164.310(a)(1), 164.310(a)(2)(i), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(a)(2)(iv), 164.310(d)(1)	AWS maintains formal policies that provide guidance for information security within the organization and the supporting IT environment.
		Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.

Subservice Organization - AWS		
Safeguard	**Requirement**	**Control**
		Closed Circuit Television Cameras (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations.
		Access to server locations is managed by electronic access control devices.
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
		Amazon-owned data centers are protected by fire detection and suppression systems.
		AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards.
		Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics.
		Critical AWS system components are replicated across multiple Availability Zones and backups are maintained.
		Backups of critical AWS system components are monitored for successful replication across multiple Availability Zones.
		AWS contingency planning and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents. The AWS contingency plan is tested on at least an annual basis.
		AWS maintains a capacity planning model to assess infrastructure usage and demands at least monthly, and usually more frequently (e.g., weekly). In addition, the AWS capacity planning model supports the planning of future demands to acquire and implement additional resources based upon current resources and forecasted requirements.

The following subservice organization controls should be implemented by DataSite to provide additional assurance that the Safeguards described within this report are met:

Subservice Organization - DataSite		
Safeguard	**Requirement**	**Control**
Physical Safeguard	164.310(a)(1), 164.310(a)(2)(i), 164.310(a)(2)(ii),	Customer computer equipment is secured by locked cages or locked cabinets and the provided premises is exclusively occupied by only that specific customer.

Subservice Organization - DataSite		
Safeguard	**Requirement**	**Control**
	164.310(a)(2)(iii), 164.310(a)(2)(iv), 164.310(d)(1)	Access to each customer's computer equipment premises within the data center is restricted to appropriately authorized individuals.
		All DataSite Orlando employees, customers, vendors, and other visitors are recorded in the Master Record of Entry by the security officer or CET on duty.
		DataSite Orlando facility and data center is monitored by security officers 24 hours a day, 7 days a week, and 365 days a year.
		Surveillance cameras record access to the facility and data center and are viewable at all times by security officers.
		Video surveillance footage is recorded to a DVR (Digital Video Recorder) system and retained for one year.
		Customer access must be authorized by an appropriate approved customer designee or DataSite Orlando representative.
		Customers are issued a key to their exclusive computer equipment premises within the data center. The key is stored within the security officer station and is only issued upon verification of the person as they enter the facility.
		Access to the master key to the facility is limited to appropriate individuals.
		For deliveries, a DataSite Orlando representative meets the delivery party at the loading dock and freight is inspected.
		Upon exit, all customers are required to return to the security officer station to return their access badge and issued key.
		Access administration to the Avigilon system is restricted to appropriately authorized individuals.

The following subservice organization controls should be implemented by SecureWorks to provide additional assurance that the Safeguards described within this report are met:

Subservice Organization - SecureWorks		
Safeguard	**Requirement**	**Control**
Administrative Safeguard	164.308(a)(1)(i), 164.308(a)(1)(ii)(B)	Security monitoring applications are in place to analyze system activity and are configured to alert IT personnel when certain predefined thresholds have been reached.
		Logging and monitoring software is configured to collect data from system infrastructure components and endpoint systems to monitor system performance, potential security vulnerabilities, resource utilization and alert the information security team upon detection of unusual system activity or service request.

The following subservice organization controls should be implemented by Ultimate Software to provide additional assurance that the Safeguards described within this report are met:

Subservice Organization - Ultimate Software		
Safeguard	**Requirement**	**Control**
Administrative Safeguard	164.308(a)(1)(i), 164.308(a)(1)(ii)(B), 164.308(a)(8)	UKG conducts periodic vulnerability scans of the environment and had developed a process for the review and resolution of vulnerabilities.
	164.308(a)(1)(i), 164.308(a)(1)(ii)(B), 164.308(a)(8)	Penetration testing is performed on an annual basis. UKG evaluates vulnerabilities and tracks the vulnerabilities through the remediation process.
	164.308(a)(1)(i), 164.308(a)(1)(ii)(B), 164.308(a)(5)(ii)(B)	Unless exempted by UKG management, antivirus software is installed and in continuous use in the production environment.
	164.308(a)(7)(i), 164.308(a)(7)(ii)(B), 164.308(a)(7)(ii)(C), 164.308(a)(7)(ii)(D), 164.308(a)(8)	Business Continuity Planning (BCP) procedures are established and tested at least annually. The results of the BCP tests are reviewed by management.
Physical Safeguard	164.310(a)(1), 164.310(a)(2)(i), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(a)(2)(iv), 164.310(d)(1)	New physical access requests are formally documented and approved prior to access being granted.
	164.310(a)(1), 164.310(a)(2)(i), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(a)(2)(iv), 164.310(d)(1)	Physical Access is revoked timely in case of termination.
Technical Safeguard	164.312(a)(2)(ii)	BCP procedures are established and tested at least annually. The results of the BCP tests are reviewed by management.

PlanSource management, along with the subservice organizations, define the scope and responsibility of the controls necessary to meet all the relevant Safeguards through written contracts, such as service level agreements. In addition, PlanSource performs monitoring of the subservice organization controls, including the following procedures:

- Holding periodic discussions with vendors and subservice organizations
- Reviewing attestation reports over services provided by vendors and subservice organizations

Complementary User Entity Controls

PlanSource'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 Safeguards related to PlanSource's services to be solely achieved by PlanSource control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of PlanSource's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Safeguards 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 entities are responsible for performing testing and approvals of the implementation process to ensure that the information is accurate and complete and that the system is functioning as it was requested.
2. User entities are responsible for implementing controls to ensure that inputs are captured accurately, completely and timely.
3. User entities are responsible for implementing controls to ensure that modification of data is authorized.
4. User entities are responsible for maintaining their own system(s) of record.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize PlanSource services.
6. User entities are responsible for immediately notifying PlanSource of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.
7. User entities are responsible for configuring the appropriate authentication parameters and providing appropriate access to authorized users within the user entity's organization.

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.308 (a)(1)(i)	**Security management process:** Implement policies and procedures to prevent, detect, contain and correct security violations.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints. Policies and procedures are in place regarding preventing, detecting, containing, and correcting security violations. Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. The monitoring software is configured to alert IT personnel when thresholds have been exceeded. An IDS and an IPS are utilized to analyze network events and report possible or actual network security breaches. The IDS and IPS are configured to notify personnel upon intrusion detection. A code repository is utilized to help detect unauthorized changes within the production environment. A code repository is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected. Centralized antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the centralized antivirus software. Antivirus software is installed on servers to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. Internal and external vulnerability scans are performed monthly and remedial actions are taken where necessary. A third-party performs a penetration test annually to identify and exploit vulnerabilities identified within the environment.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
	Internal Network - Okta	
		Network account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset Network audit logging configurations are in place that include: • Account logon events • Account management • Logon events • Privilege use • Process tracking • System events Network audit logs are maintained and available for review when needed.
	Production Network - Window Active Directory	
		Production network account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset Production network audit logging configurations are in place that include: • Account logon events • Account management • Logon events • Privilege use • Process tracking • System events Production network audit logs are maintained and available for review when needed.
	Production Servers - Windows, Linux	
		Production server account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset Production server audit logging configurations are in place that include: • Account logon events • Account management • Logon events • Object access • Policy changes • Privilege use • System events Production server audit logs are maintained and available for review when needed.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
	Production Databases - MySQL Server	
		Production databases account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset Production database audit logging configurations are in place to log user activity and system events. Production databases audit logs are maintained and available for review when needed.
	Production Applications - BenAdmin and HCM	
164.308 (a)(1)(ii)(A)	**Risk analysis:** 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.	Production application account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold Production application audit logging configurations are in place to log user activity and system events. Production application audit logs are maintained and available for review when needed. Part of this regulation is the responsibility of the subservice organizations. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organizations. Documented policies and procedures are in place to guide personnel when performing a risk assessment. Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances. A formal risk assessment is performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		The entity's risk assessment process includes: • Setting the context and scope of assessment • Identification and prioritization of the threats to Information Resources • Identification and prioritization of the vulnerabilities of Information Resources • Identification of a threat that may exploit a vulnerability • Qualitative and/or quantitative identification of the impact to the confidentiality, integrity and availability of Information Resources if a threat exploits a specific gap • Identification and definition of measures and/or controls used to protect the confidentiality, integrity and availability of Information Resources
164.308 (a)(1)(ii)(B)	**Risk management:** Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a). 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 • The probability and criticality of potential risks to ePHI	The entity's risk assessment process includes: • Setting the context and scope of assessment • Identification and prioritization of the threats to Information Resources • Identification and prioritization of the vulnerabilities of Information Resources • Identification of a threat that may exploit a vulnerability • Qualitative and/or quantitative identification of the impact to the confidentiality, integrity and availability of Information Resources if a threat exploits a specific gap • Identification and definition of measures and/or controls used to protect the confidentiality, integrity and availability of Information Resources Risks identified as a part of the risk assessment process are addressed using one of the following strategies: • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk Management develops risk mitigation strategies to address risks identified during the risk assessment process. An IDS and an IPS are utilized to analyze network events and report possible or actual network security breaches.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		The IDS and IPS are configured to notify personnel upon intrusion detection. A code repository is utilized to help detect unauthorized changes within the production environment. A code repository is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected. Centralized antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the centralized antivirus software. Antivirus software is installed on servers to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. Internal and external vulnerability scans are performed monthly and remedial actions are taken where necessary. A third-party performs a penetration test annually to identify and exploit vulnerabilities identified within the environment. A firewall is in place to filter unauthorized inbound network traffic from the Internet. The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule. Part of this regulation is the responsibility of the subservice organizations. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organizations.
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 or business associate.	Sanction policies, which include probation, suspension, and termination, are in place for employee misconduct.
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 reports, and security incident tracking reports.	Documented policies and procedures are in place regarding system configurations, authentication, access, and security monitoring.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
	Internal Network - Okta	
		Network audit logging configurations are in place that include: • Account logon events • Account management • Logon events • Privilege use • Process tracking • System events Network audit logs are maintained and available for review when needed.
	Production Network - Windows Active Directory	
		Production network audit logging configurations are in place that include: • Account logon events • Account management • Logon events • Privilege use • Process tracking • System events Production network audit logs are maintained and available for review when needed.
	Production Servers - Windows, Linux	
		Production server audit logging configurations are in place that include: • Account logon events • Account management • Logon events • Object access • Policy changes • Privilege use • System events Production server audit logs are maintained and available for review when needed.
	Production Databases - MySQL Server	
		Production database audit logging configurations are in place to log user activity and system events. Production databases audit logs are maintained and available for review when needed.
	Production Applications - BenAdmin and HCM	
		Production application audit logging configurations are in place to log user activity and system events. Production application audit logs are maintained and available for review when needed.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
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 covered entity or business associate.	Responsibility for the development, implementation, and regular maintenance of the policies and procedures that govern the security of protected ePHI is formally documented and assigned to a job role.
164.308 (a)(3)(i)	**Workforce security:** Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, 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.	Policies and procedures are formally defined and documented regarding accessing ePHI. Users accessing ePHI are authenticated via individually assigned user accounts and passwords. Access to ePHI is restricted to authorized personnel. Users with access to ePHI are reviewed by management annually.
164.308 (a)(3)(ii)(A)	**Authorization and/or supervision:** 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.	Policies and procedures are formally defined and documented regarding authorization of access to ePHI. Logical access to systems is approved and granted to personnel as a component of the hiring process.
164.308 (a)(3)(ii)(B)	**Workforce clearance procedure:** Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	Policies and procedures are formally defined and documented regarding accessing ePHI. Users accessing ePHI are authenticated via individually assigned user accounts and passwords. Access to ePHI is restricted to authorized personnel. Users with access to ePHI are reviewed by management annually.
164.308 (a)(3)(ii)(C)	**Termination procedures:** 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) [the Workforce Clearance Procedure] of this section.	Policies and procedures are formally defined and documented regarding revoking access following termination. Logical access to systems is revoked from personnel as a component of the termination process.
164.308 (a)(4)(i)	**Information access management:** Implement policies and procedures for authorizing access to electronic protected health information that 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.	Management maintains policies and procedures that ensure the authorization of access to ePHI and are consistent with the applicable requirements of the Privacy Rule.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.308 (a)(4)(ii)(A)	**Isolating healthcare clearinghouse functions:** 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.	Not applicable. The entity is not a healthcare clearinghouse.
164.308 (a)(4)(ii)(B)	**Access authorization:** Implement policies and procedures for granting access to ePHI, for example, through access to a workstation, transaction, program, process, or other mechanism.	Policies and procedures are formally defined and documented regarding authorization of access to ePHI. Logical access to systems is approved and granted to personnel as a component of the hiring process.
164.308 (a)(4)(ii)(C)	**Access establishment and modification:** 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.	Policies and procedures are formally defined and documented regarding authorization of access to ePHI. Users with access to ePHI are reviewed by management annually.
164.308 (a)(5)(i)	**Security awareness and 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.	Executive management has created a training program for its employees. Upon hire, employees are required to read and acknowledge the information security policies and procedures and complete information security and awareness training. Current employees are required to read and acknowledge the information security policies and procedures and complete information security and awareness training on an annual basis.
164.308 (a)(5)(ii)(A)	**Security reminders:** Periodic security updates.	Users are made aware of security updates and updates to security policies.
164.308 (a)(5)(ii)(B)	**Protection from malicious software:** Procedures for guarding against, detecting, and reporting malicious software.	Policies and procedures are formally documented regarding preventing, detecting, and reporting the presence of malicious software. Centralized antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the centralized antivirus software. Antivirus software is installed on servers to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.308 (a)(5)(ii)(C)	**Log-in monitoring:** Procedures for monitoring log-in attempts and reporting discrepancies.	Part of this regulation is the responsibility of the subservice organization. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organization. Documented policies and procedures are in place regarding system configurations, authentication, access, and security monitoring.
	Internal Network - Okta	
		Network audit logging configurations are in place that include: • Account logon events • Account management • Logon events • Privilege use • Process tracking • System events Network audit logs are maintained and available for review when needed.
	Production Network - Windows Active Directory	
		Production network audit logging configurations are in place that include: • Account logon events • Account management • Logon events • Privilege use • Process tracking • System events Production network audit logs are maintained and available for review when needed.
	Production Servers - Windows, Linux	
		Production server audit logging configurations are in place that include: • Account logon events • Account management • Logon events • Object access • Policy changes • Privilege use • System events Production server audit logs are maintained and available for review when needed.
	Production Databases - MySQL Server	
		Production database audit logging configurations are in place to log user activity and system events. Production databases audit logs are maintained and available for review when needed.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
	Production Applications - BenAdmin and HCM	
164.308 (a)(5)(ii)(D)	**Password management:** Procedures for creating, changing, and safeguarding passwords.	Production application account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold Production application audit logging configurations are in place to log user activity and system events. Production application audit logs are maintained and available for review when needed. Policies are in place to guide personnel in creating, changing, and safeguarding passwords.
	Internal Network - Okta	
		The network is configured to enforce password requirements that include: • Password history • Password length • Complexity
	Production Network - Windows Active Directory	
		Production network is configured to enforce password requirements that include: • Password history • Password length • Complexity
	Production Databases - MySQL	
		Production databases are configured to enforce password requirements that include: • Password history • Password length • Complexity
	Production Applications - BenAdmin and HCM	
164.308 (a)(6)(i)	**Security incident procedures:** Implement policies and procedures to address security incidents. Policies and procedures should include response reporting.	The production applications are configured to enforce password requirements that include: • Password length • Complexity Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints. Incidents are documented and tracked within SharePoint folders and updated to reflect the planned incident and problem resolution.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
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 or business associate; and document security incidents and their outcomes.	Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints. Identified incidents are analyzed, classified and prioritized based on system impact to determine the appropriate containment strategy, including a determination of the appropriate response time frame and the determination and execution of the containment approach. Incidents are documented and tracked within SharePoint folders and updated to reflect the planned incident and problem resolution. Resolution of incidents are documented and communicated to affected users.
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 ePHI.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency. The business continuity and disaster recovery plan are tested on an annual basis. Part of this regulation is the responsibility of the subservice organizations. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organizations.
164.308 (a)(7)(ii)(A)	**Data backup plan:** Establish and implement procedures to create and maintain retrievable exact copies of ePHI.	Data backup policies and procedures are formally documented. Full backups of certain application and database components are performed on a weekly basis and incremental backups are performed on a daily basis.
164.308 (a)(7)(ii)(B)	**Disaster recovery plan:** Establish (and implement as needed) procedures to restore any loss of data.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency. The business continuity and disaster recovery plan are tested on an annual basis. A data backup restoration test is performed on an annual basis. Part of this regulation is the responsibility of the subservice organizations. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organizations.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
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.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency. The business continuity and disaster recovery plan are tested on an annual basis. The business continuity and disaster recovery plan and procedures are updated based on disaster recovery plan test results. Part of this regulation is the responsibility of the subservice organizations. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organizations.
164.308 (a)(7)(ii)(D)	**Testing and revision procedures:** Implement procedures for periodic testing and revision of contingency plans.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency. The business continuity and disaster recovery plan are tested on an annual basis. The business continuity and disaster recovery plan and procedures are updated based on disaster recovery plan test results. A data backup restoration test is performed on an annual basis. Part of this regulation is the responsibility of the subservice organizations. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organizations.
164.308 (a)(7)(ii)(E)	**Applications and data criticality analysis:** Assess the relative criticality of specific applications and data in support of another contingency plan component.	The entity maintains a policy to assess the relative criticality of applications, systems and other assets maintaining ePHI, so that such data can be properly protected during emergencies and during normal business operations. The entity maintains an asset inventory that categorizes and prioritizes systems and other assets maintaining ePHI.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		The entity's risk assessment process includes: • Setting the context and scope of assessment • Identification and prioritization of the threats to Information Resources • Identification and prioritization of the vulnerabilities of Information Resources • Identification of a threat that may exploit a vulnerability • Qualitative and/or quantitative identification of the impact to the confidentiality, integrity and availability of Information Resources if a threat exploits a specific gap • Identification and definition of measures and/or controls used to protect the confidentiality, integrity and availability of Information Resources
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.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency. Business continuity and disaster recovery plans are tested on an annual basis. The business continuity and disaster recovery plan and procedures are updated based on disaster recovery plan test results. Internal and external vulnerability scans are performed monthly and remedial actions are taken where necessary. A third-party performs a penetration test annually to identify and exploit vulnerabilities identified within the environment. Part of this regulation is the responsibility of the subservice organizations. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organizations.
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.	Not applicable. The entity is not a covered entity.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.308 (b)(2)	A business associate may permit a business that is a subcontractor to create, receive, maintain, or transmit ePHI 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.	The entity maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicate: • The permitted and required uses and disclosures of protected health information by the business associate • Terms, conditions and responsibilities between the involved parties • Just cause for termination
164.308 (b)(3)	**Written contract or other arrangement:** Document the satisfactory assurances required by paragraph (b)(1) or (b2) above of this section through a written or other arrangement with the business associate that meets the applicable requirements of 164.314(a) [the Organizational Requirements].	The entity maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicate: • The permitted and required uses and disclosures of protected health information by the business associate • Terms, conditions and responsibilities between the involved parties • Just cause for termination
164.308 (b)(4)	**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 arrangement with the business associate that meets the applicable requirements of 164.314(a).	The entity maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicate: • The permitted and required uses and disclosures of protected health information by the business associate • Terms, conditions and responsibilities between the involved parties • Just cause for termination

PHYSICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.310 (a)(1)	**Facility access controls:** Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	This regulation is the responsibility of the subservice organizations. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organizations.
164.310 (a)(2)(i)	**Contingency operations:** 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.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency. Business continuity and disaster recovery plans are tested on an annual basis. A data backup restoration test is performed on an annual basis. Part of this regulation is the responsibility of the subservice organizations. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organizations.
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.	This regulation is the responsibility of the subservice organizations. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organizations.
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.	This regulation is the responsibility of the subservice organizations. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organizations.
164.310 (a)(2)(iv)	**Maintenance records:** 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).	This regulation is the responsibility of the subservice organizations. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organizations.
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 surroundings of a specific workstation or class of workstation that can access ePHI.	Procedures that specify the proper functions, processes, and appropriate environments of workstations that access ePHI are in place.
164.310 (c)	**Workstation security:** Covered entities should implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.	Not applicable. The entity is not a covered entity.

PHYSICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.310 (d)(1)	**Device and media control:** Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility.	Procedures are in place to ensure that maintenance records of the movements of hardware and electronic media are documented. Part of this regulation is the responsibility of the subservice organizations. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organizations.
164.310 (d)(2)(i)	**Disposal:** Implement policies and procedures to address the final disposition of ePHI, and/or the hardware or electronic media on which it is stored.	Policies and procedures are in place to guide personnel in data, hardware and software disposal and destruction. The entity purges ePHI data after it is no longer required to achieve the purpose for which the data was collected and processed.
164.310 (d)(2)(ii)	**Media re-use:** Implement procedures for removal of ePHI from electronic media before the media are made available for re-use. Ensure that ePHI previously stored on electronic media cannot be accessed and reused. Identify removable media and their use. Ensure that ePHI is removed from reusable media before they are used to record new information.	The entity sanitizes media containing ePHI when the media is to be re-used. The entity purges ePHI data after it is no longer required to achieve the purpose for which the data was collected and processed.
164.310 (d)(2)(iii)	**Accountability:** Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	Procedures are in place to ensure that maintenance records of the movements of hardware and electronic media are documented.
164.310 (d)(2)(iv)	**Data backup and storage:** Create a retrievable, exact copy of ePHI, when needed, before movement of equipment.	Data backup policies and procedures are formally documented. Full backups of certain application and database components are performed on a weekly basis and incremental backups are performed on a daily basis.

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
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 §164.308(a)(4) [Information Access Management].	Documented policies and procedures are in place regarding system configurations, authentication, access, and security monitoring. Users accessing ePHI are authenticated via individually assigned user accounts and passwords. Access to ePHI is restricted to authorized personnel. Logical access to systems is approved and granted to personnel as a component of the hiring process. Logical access reviews are performed annually. Logical access to systems is revoked from personnel as a component of the termination process.
	Internal Network - Okta	
		The network is configured to enforce password requirements that include: • Password history • Password length • Complexity
	Production Network - Windows Active Directory	
		Production network is configured to enforce password requirements that include: • Password history • Password length • Complexity
	Production Databases - MySQL Server	
		Production databases are configured to enforce password requirements that include: • Password history • Password length • Complexity
	Production Applications - BenAdmin and HCM	
		The production applications are configured to enforce password requirements that include: • Password length • Complexity

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.312 (a)(2)(i)	**Unique user identification:** Assign a unique name and/or number for identifying and tracking user identity. Ensure that system activity can be traced to a specific user. Ensure that the necessary data is available in the system logs to support audit and other related business functions.	Documented policies and procedures are in place regarding system configurations, authentication, access, and security monitoring. Users accessing ePHI are authenticated via individually assigned user accounts and passwords. Access to ePHI is restricted to authorized personnel.
	Internal Network - Okta	
		The network is configured to enforce password requirements that include: • Password history • Password length • Complexity Network account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset Network audit logging configurations are in place that include: • Account logon events • Account management • Logon events • Privilege use • Process tracking • System events Network audit logs are maintained and available for review when needed.
	Production Network - Windows Active Directory	
		Production network is configured to enforce password requirements that include: • Password history • Password length • Complexity Production network account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset Production network audit logging configurations are in place that include: • Account logon events • Account management • Logon events • Privilege use • Process tracking • System events

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		Production network audit logs are maintained and available for review when needed.
	Production Servers - Windows, Linux	
		Production server account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset Production server audit logging configurations are in place that include: • Account logon events • Account management • Logon events • Object access • Policy changes • Privilege use • System events Production server audit logs are maintained and available for review when needed.
	Production Databases - MySQL Server	
		Production databases are configured to enforce password requirements that include: • Password history • Password length • Complexity Production databases account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold • Account lockout counter reset Production database audit logging configurations are in place to log user activity and system events. Production databases audit logs are maintained and available for review when needed.
	Production Applications - BenAdmin and HCM	
		The production applications are configured to enforce password requirements that include: • Password length • Complexity Production application account lockout configurations are in place that include: • Account lockout duration • Account lockout threshold Production application audit logging configurations are in place to log user activity and system events.

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		Production application audit logs are maintained and available for review when needed.
164.312 (a)(2)(ii)	**Emergency access procedure:** Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.	A documented disaster recovery plan is in place to guide personnel in the event of an emergency. The business continuity and disaster recovery plan are tested on an annual basis. Part of this regulation is the responsibility of the subservice organizations. Refer to the 'Subservice Organizations' section above for controls managed by the subservice organizations.
164.312 (a)(2)(iii)	**Automatic logoff:** Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Workstations are configured to terminate inactive sessions after fifteen minutes of inactivity. Users are required to re-validate with a username and password to gain control of the workstation.
164.312 (a)(2)(iv)	**Encryption and decryption:** Implement a mechanism to encrypt and decrypt ePHI.	Virtual Private Network (VPN), Secure Socket Layer (SSL)/Transport Layer Security (TLS) and other encryption technologies are used for defined points of connectivity. Server certificate-based authentication is used as part of the SSL/TLS encryption with a trusted certificate authority. Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.
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.	Documented policies and procedures are in place regarding system configurations, authentication, access, and security monitoring. A code repository is utilized to help detect unauthorized changes within the production environment. A code repository is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.
	Internal Network - Okta	
		Network audit logging configurations are in place that include: • Account logon events • Account management • Logon events • Privilege use • Process tracking • System events Network audit logs are maintained and available for review when needed.

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
	Production Network - Windows Active Directory	
		Production network audit logging configurations are in place that include: • Account logon events • Account management • Logon events • Privilege use • Process tracking • System events Production network audit logs are maintained and available for review when needed.
	Production Servers - Windows, Linux	
		Production server audit logging configurations are in place that include: • Account logon events • Account management • Logon events • Object access • Policy changes • Privilege use • System events Production server audit logs are maintained and available for review when needed.
	Production Databases - MySQL Server	
		Production database audit logging configurations are in place to log user activity and system events. Production databases audit logs are maintained and available for review when needed.
	Production Applications - BenAdmin and HCM	
164.312 (c)(1)	**Integrity:** Implement policies and procedures to protect ePHI from improper alteration or destruction.	Production application audit logging configurations are in place to log user activity and system events. Production application audit logs are maintained and available for review when needed. Policies and procedures are formally documented regarding protecting ePHI from improper alteration or destruction. VPN, SSL/TLS and other encryption technologies are used for defined points of connectivity. Server certificate-based authentication is used as part of the SSL/TLS encryption with a trusted certificate authority. Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.312 (c)(2)	**Mechanisms to authenticate ePHI:** Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.	A code repository is utilized to help detect unauthorized changes within the production environment. A code repository is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected. Critical data output from the system is stored and transmitted using secure encryption methods. Policies and procedures are formally documented regarding protecting ePHI from improper alteration or destruction. VPN, SSL/TLS and other encryption technologies are used for defined points of connectivity. Server certificate-based authentication is used as part of the SSL/TLS encryption with a trusted certificate authority. Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session. A code repository is utilized to help detect unauthorized changes within the production environment. A code repository is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected. Critical data output from the system is stored and transmitted using secure encryption methods.
164.312 (d)	**Person or entity authentication:** Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.	Documented policies and procedures are in place regarding system configurations, authentication, access, and security monitoring. Users accessing ePHI are authenticated via individually assigned user accounts and passwords. Access to ePHI is restricted to authorized personnel.
	Internal Network - Okta	
		The network is configured to enforce password requirements that include: • Password history • Password length • Complexity

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
	Production Network - Windows Active Directory	
		Production network is configured to enforce password requirements that include: • Password history • Password length • Complexity
	Production Databases - MySQL Server	
		Production databases are configured to enforce password requirements that include: • Password history • Password length • Complexity
	Production Applications - BenAdmin and HCM	
		The production applications are configured to enforce password requirements that include: • Password length • Complexity
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.	Policies and procedures are formally documented regarding protecting electronically transmitted ePHI from unauthorized access. VPN, SSL/TLS and other encryption technologies are used for defined points of connectivity. Server certificate-based authentication is used as part of the SSL/TLS encryption with a trusted certificate authority. Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.
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.	Policies and procedures are formally documented regarding protecting electronically transmitted ePHI from improper alteration or destruction during transmission. VPN, SSL/TLS and other encryption technologies are used for defined points of connectivity. Server certificate-based authentication is used as part of the SSL/TLS encryption with a trusted certificate authority. Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session.
164.312 (e)(2)(ii)	**Encryption:** Implement a mechanism to encrypt ePHI whenever deemed appropriate.	Policies and procedures are formally documented regarding the mechanisms used to encrypt ePHI.

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		VPN, SSL/TLS and other encryption technologies are used for defined points of connectivity. Server certificate-based authentication is used as part of the SSL/TLS encryption with a trusted certificate authority. Remote connectivity users are authenticated via an authorized user account and password before establishing a VPN session. Critical data output from the system is stored and transmitted using secure encryption methods.

ORGANIZATIONAL REQUIREMENTS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
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.	The entity maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicate: • The permitted and required uses and disclosures of protected health information by the business associate • Terms, conditions and responsibilities between the involved parties • Just cause for termination
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."	The entity maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI. The business associate agreements communicate: • The permitted and required uses and disclosures of protected health information by the business associate • Terms, conditions and responsibilities between the involved parties • Just cause for termination
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: (1) if it enters into a memorandum of understanding (MOU) with the business associate and the MOU contains terms which accomplish the objectives of the Business Associate Contracts section of the Security Rule; or (2) if other law (including regulations adopted by the covered entity or its business associate) contain requirements applicable to the business associate that accomplish the objectives of the business associate contract.	Not applicable. The entity is not a government entity.
164.314 (b)(1)	**Requirements for Group Health Plans:** Except when the only ePHI 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 ePHI created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.	Not applicable. The entity is not a plan sponsor.

ORGANIZATIONAL REQUIREMENTS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.314 (b)(2)	**Implementation Specifications:** 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 ePHI that it creates, receives, maintains, or transmits on behalf of the group health plan; (ii) Ensure that the adequate separation required by §164.504(f)(2)(iii) is supported by reasonable and appropriate security measures; (iii) Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and (iv) Report to the group health plan any security incident of which it becomes aware.	Not applicable. The entity is not a group health plan.
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. 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.	The entity creates and implements appropriate policies and procedures as required by applicable legislations, regulators, and customers. Policies and procedures are reviewed annually and updated, if necessary, and distributed, or otherwise made available to personnel.
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.	Policies and procedures are appropriately retained for a minimum of six (6) years from the date it was created or when it was last in effect, whichever is later. Policies and procedures are reviewed annually and updated, if necessary, and distributed, or otherwise made available to personnel. Policies and procedures are created and maintained in written and electronic form.
164.316 (b)(1)(ii)	**Documentation:** 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.	HIPAA related incidents and events are documented and tracked in SharePoint folders.

ORGANIZATIONAL REQUIREMENTS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.316 (b)(2)(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.	Policies and procedures are appropriately retained for a minimum of six (6) years from the date it was created or when it was last in effect, whichever is later.
164.316 (b)(2)(ii)	**Availability:** Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	Policies and procedures are reviewed annually and updated, if necessary, and distributed, or otherwise made available to personnel.
164.316 (b)(2)(iii)	**Updates:** Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the ePHI.	Policies and procedures are reviewed annually and updated, if necessary, and distributed, or otherwise made available to personnel.

BREACH NOTIFICATION		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.402	Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information. (1)(i) For purposes of this definition, compromises the security or privacy of the protected health information means poses a significant risk of financial, reputational, or other harm to the individual. (ii) A use or disclosure of protected health information that does not include the identifiers listed at §164.514(e)(2), date of birth, and zip code does not compromise the security or privacy of the protected health information.	Breach notification procedures are in place to guide personnel in developing breach notification letters or e-mails to be used during a breach of ePHI. Notification procedures include: • Notice to parties alerting them to breaches "without unreasonable delay," but no later than 60 days after discovery of the breach • Notice to covered entities when breach is discovered • Notice to the secretary of Human Health Services (HHS) and prominent media outlets about breaches involving more than 500 individual subject's records • Notices to include what happened, the details of the breached unsecure PHI, steps to help mitigate harm to the party, and the covered entity's response • Annual notice to the secretary of HHS 60 days before the end of the calendar year about unsecure PHI breaches involving fewer than 500 patient records
164.404 (a)	A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used or disclosed as a result of such breach.	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (2)	For purposes of paragraph (a)(1) of this section, §§ 164.406(a), and 164.408(a), a breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency).	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (b)	Except as provided in §164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 days after discovery of a breach.	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.

BREACH NOTIFICATION		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.404 (c)(1)	Elements of the notification required by paragraph (a) of this section shall include to the extent possible: (A) a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known; (B) a description of the types of unsecured protected health information that were involved in the breach (Such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved); (C) any steps the individual should take to protect themselves from potential harm resulting from the breach; (D) a brief description of what the covered entity is doing to investigation the breach, to mitigate harm to individuals, and to protect against further breaches; and (E) contact procedures for individuals to ask questions or learn additional information which should include a toll-free number, an e-mail address, website, or postal address.	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (c)(2)	The notification required by paragraph (a) of this section shall be written in plain language.	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (d)(1)(i)	The notification required by paragraph (a) shall be provided in the following form: Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as more information becomes available.	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (d)(1)(ii)	The notification required by paragraph (a) shall be provided in the following form: If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual (as specified under §164.502(g)(4) of subpart E) , written notification by first-class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available.	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.

BREACH NOTIFICATION		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.404 (d)(2)	**Substitute notice**. In the case where there is insufficient or out-of-date contact information that precludes written notification to the individual under this paragraph (d)(1)(i) of this section, a substitute form of notice reasonable calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual under paragraph (d)(1)(ii).	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (d)(2)(i)	In the case where there is insufficient or out-of-date contact information for fewer than 10 individuals, then substitute notice may be provided by an alternative form of written notice, telephone or other means.	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (d)(2)(ii)	In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall: (A) be in the form of either a conspicuous posting for a period of 90 days on the home page of the web site of the covered entity involved, or conspicuous notice in a major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and (B) include a toll-free number that remains active for at least 90 days where an individual can learn whether the individual's secured protected health information may be included in the breach.	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (d)(3)	In any case deemed by the covered entity to require urgency because of possible imminent misuse of unsecured protected health information, the covered entity may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided under paragraph (d)(1) of this section.	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.406	§164.406(a) For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach, notify prominent media outlets serving the State or jurisdiction. (b) Except as provided in §164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. (c) The content of the notification required by paragraph (a) shall meet the requirements of §164.404(c).	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.408 (a)	A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in §164.404(a)(2), notify the Secretary.	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.

BREACH NOTIFICATION		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.408 (b)	For breaches of unsecured protected health information involving 500 or more individuals, a covered entity shall, expect as provided in §164.412, provide the notification required by paragraph (a) contemporaneously with the notice required by §164.404(a) and in the manner specified on the HHS web site.	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.408 (c)	For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) of this section for breaches occurring during the preceding calendar year, in a manner specified on the HHS web site.	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.410 (a)(1)	A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach.	Documented policies and procedures are in place to guide personnel in notifying the covered entity upon discovery of a breach of unsecured protected health information. Breach notification procedures are in place to guide personnel in developing breach notification letters or e-mails to be used during a breach of ePHI. Notification procedures include: • Notice to parties alerting them to breaches “without unreasonable delay,” but no later than 60 days after discovery of the breach • Notice to covered entities when breach is discovered • Notice to the secretary of Human Health Services (HHS) and prominent media outlets about breaches involving more than 500 individual subject’s records • Notices to include what happened, the details of the breached unsecure PHI, steps to help mitigate harm to the party, and the covered entity’s response • Annual notice to the secretary of HHS 60 days before the end of the calendar year about unsecure PHI breaches involving fewer than 500 patient records

BREACH NOTIFICATION		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.410 (a)(2)	(2) For the purposes of paragraph (1) of this section, a breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the federal common law of agency).	The entity acknowledges responsibility for notifying affected parties in the event of a breach of unsecured protected health information.
164.410 (b)	Except as provided in §164.412, a business associate shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach.	The entity notifies affected parties of a breach of ePHI no later than sixty (60) calendar days after the discovery of the breach.
164.410 (c)(1)	The notification required by paragraph (a) of this section shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been, or is reasonably believed by the business associate to have been accessed, acquired, used or disclosure during the breach.	The identification of each individual who's unsecured ePHI has been accessed during the breach is disclosed during notification procedures.
164.410 (c)(2)	A business associate shall provide the covered entity with any other information that the covered entity is required to include in the notification to the individual under §164.404(c) at the time of the notification required by paragraph (a) of this section or promptly thereafter as information becomes available.	Management provides the covered entity with any information that the covered entity is required to include in the notification to the individual at the time of the breach and as soon as it is available.
164.412	If a law enforcement official states to a covered entity or business associate that a notification, notice or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall: (a) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or (b) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) of this section is submitted during that time.	Documented policies and procedures are in place to guide personnel in the process of delaying and documenting notifications based on a law enforcement official's request due to a criminal investigation or national security.

BREACH NOTIFICATION		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.414	**Administrative requirements and burden of proof**: (a) covered entity is required to comply with the administrative requirements of § 164.530(b), (d), (e), (g), (h), (i), and (j) with respect to the requirements of this subpart. (b) In the event of a use or disclosure in violation of subpart E, the covered entity or business associate; as applicable, shall have the burden of demonstrating that all notifications were made as required by this subpart or that the use or disclosures did not constitute a breach as defined at §164.402. See §164.530 for definition of breach.	The entity acknowledges responsibility for notifying affected parties in the event of a breach of unsecured protected health information.

SECTION 4

INFORMATION PROVIDED BY THE SERVICE AUDITOR

GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR

A-LIGN ASSURANCE's examination of the controls of PlanSource was limited to the HIPAA/HITECH requirements and related control activities specified by the management of PlanSource and did not encompass all aspects of PlanSource's operations or operations at user entities. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) AT-C 105, AT-C 205 and AT-C 315.

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 the 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 HIPAA/HITECH requirements
- Understand the flow of ePHI through the service organization
- Determine whether the service organization's controls are suitably designed to meet the health information security program of the user entity's and determine whether they have been implemented