MealSuite, Inc.

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

2024

Table of Contents

SECTION 1

ASSERTION OF MEALSUITE, INC. MANAGEMENT

ASSERTION OF MEALSUITE, INC. MANAGEMENT

December 15, 2024

We have prepared the description of MealSuite, Inc.'s ('MealSuite,' or 'the service organization') health information security program for the Cloud-Based FoodService Software Services System (the "description") for user entities of the system as of October 31, 2024. We confirm, to the best of our knowledge and belief, that:

a. Management's description fairly presents the health information security program for the Cloud-Based FoodService Software Services System as of October 31, 2024. 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 Cloud-Based FoodService Software Services System
    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 Cloud-Based FoodService Software Services System 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 Cloud-Based FoodService Software Services System 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 October 31, 2024, 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 MealSuite's controls as of that date.

Section 3 of this report includes MealSuite's description of the health information security program for the Cloud-Based FoodService Software Services System that is covered by this assertion.

Sean Rowe
President & CEO
MealSuite, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To MealSuite, Inc.:

We have examined MealSuite's description of its health information security program for the MealSuite's Cloud-Based FoodService Software Services System listed in Section 3 (the "description"), and its health information security program governing the Cloud-Based FoodService Software Services System's 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"). MealSuite's management is responsible for its assertion. Our responsibility is to express an opinion about MealSuite's compliance with the specified requirements based on our examination.

MealSuite uses Digital Realty Trust, Inc. ('Digital Realty' or 'subservice organization') for data center hosting services. The description indicates that certain applicable HIPAA/HITECH requirements can only be met if controls at the subservice organization are suitably designed. The description presents MealSuite's system; its controls relevant to the applicable HIPAA/HITECH requirements; and the types of controls that the service organization expect to be implemented, and suitably designed at the subservice organization to meet certain applicable HIPAA/HITECH requirements. The description does not include any of the controls implemented at the subservice organization. Our examination did not extend to the services provided by the subservice organization.

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 MealSuite's health information security program for the Cloud-Based FoodService Software Services System 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 MealSuite 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 and inherent limitations, 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 MealSuite's assertion in Section 1:

a. The description fairly presents the health information security program for the Cloud-Based FoodService Software Services System that was designed and implemented as of October 31, 2024;
b. The health information security program governing the Cloud-Based FoodService Software Services System complied with applicable requirements of HIPAA and HITECH; and
c. the controls stated in MealSuite's description were suitably designed and implemented as of October 31, 2024, 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 MealSuite's controls as of that date.

This report is intended solely for the information and use of MealSuite; user entities of MealSuite's Cloud-Based FoodService Software Services System as of October 31, 2024; 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
December 15, 2024

SECTION 3

MEALSUITE, INC.'S DESCRIPTION OF ITS CLOUD-BASED FOODSERVICE SOFTWARE SERVICES SYSTEM AS OF OCTOBER 31, 2024

OVERVIEW OF OPERATIONS

Company Background

Founded in 1984 as a technology consulting business, MealSuite (formerly SureQuest) has developed into a FoodService Management leader, serving clients throughout North America.

Today MealSuite's web-based software platform serves over 3,000 healthcare operators, empowering them to automate and digitize their operations to ensure compliance, reduce risk and deliver the highest quality of care to patients and residents.

Description of Services Provided

MealSuite's web-based FoodService management software platform is scalable to assist various sizes of organizations. Whether a client is looking to operate in an entirely automated and paperless system or simply conduct a costing or nutrient analysis of an existing menu, MealSuite's modules can be turned on and off based on licensing. Modules include:

- Menu Management
- Nutritional Analysis - with integrations to major food manufacturers to ensure the most recent and accurate data
- Menu Costing - with integration with distributor partners to automate costing
- Inventory Management
- Meal Service Tools - Reports to meet compliance at time of delivery to residents or patients
- Digital Menu Boards
- Production Tools - Recipe scaling and forecasting to reduce food waste and ensure consistency
- Procurement - with integrations to major distributor partners
- People and Patient Management - with optional integration into customer Electronic Health Record (EHR)/Electronic Medical Record (EMR) systems
- Point of Sale
- MealSuite Touch - Add-on iDevice Operating System (IOS)/Android application, enabling customers to go paperless

In addition to the web-based platform provided to customers, MealSuite also sells equipment to support on-site operations. The equipment is manufactured, certified, and warrantied by third-party-vendors. Equipment includes but is not limited to:

- Digital touch-screen Menu Boards
- Tablets and portable devices for use in meal ordering, inventory, etc.
- Sensors to monitor food, refrigerator, and freezer temperatures
- Thermal Printers, Food Scales, Cash Drawers, and other accessories as required

Principal Service Commitments and System Requirements

MealSuite designs its processes to meet its objectives for its foodservice automation services. Those objectives are based on the service commitments that MealSuite makes to clients, the laws and regulations that govern the provision of the industry, and the financial, operational, and compliance requirements that MealSuite has established for the services. The foodservice automation services of MealSuite are subject to the security and privacy requirements of the Health Insurance Portability, as amended, including relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which MealSuite delivers services.

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

- Security principles within the fundamental designs of MealSuite's software 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
- Best practices are followed to ensure the protection of clients' data

MealSuite establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in MealSuite'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 MealSuite Cloud-Based FoodService Software Services System.

Components of the System

Infrastructure

MealSuite utilizes a variety of hardware and software vendors to ensure the highest level of security and up-time for both internal and external customers. These vendors include system virtualization, firewalls, security-as-a-service, and dev-ops-as-a-service. MealSuite's internal systems are cloud-based with remote access capabilities globally for employees, reducing dependencies on internal networks and offices.

Software

Primary software used to provide MealSuite's Cloud-Based FoodService Software Services System includes the use of open-sourced Linux Based Technologies including PostgreSQL, Ubuntu, Ruby On Rails, Redis and Angular. Third-party software vendors including Salesforce, Microsoft Office, JIRA and Zendesk are utilized to support the customer and internal teams.

People

MealSuite is owned by CloudStorm Ventures, where it gains access to shared resources such as Human Resources (HR), Marketing, Software Engineering, IT (Administration and Security) and Finance.

There is a dedicated team of 130+ individuals that are not shared with other portfolio companies, with a further group of 40 resources that may service one or more organizations within the portfolio.

<u>Finance Operations</u>

Responsible for payroll administration, accounts payable, accounts receivable, tax and financial filings. A third-party firm is engaged for payroll and compliance in Vietnam.

<u>Human Resources</u>

Compliance, recruiting, people operations, on-boarding and benefits administration.

<u>Sales & Marketing</u>

Product sales, marketing & partner channel support.

Nutrition Services

A team of registered dieticians or similar qualifications, responsible for quality assurance (QA) and the creation and maintenance of starting base recipes and menus for customers. This team are also engaged to assist customers with data entry and initial data setup of the system.

Product Management

Responsible for planning the software release roadmap, collecting customer feedback, feature design and validation.

Engineering

Software development, Artificial Intelligence (AI) & Machine learning, manual and automated QA testing teams and database management.

Customer Support

Technical and functional support of the software and hardware platforms. Available during regular business hours with 24/7 coverage for any critical issues outside regular hours.

Onboarding

Responsible for the training and successful onboarding of new customer facing projects.

Project Management

A dedicated project management office with oversight of internal corporate projects, privacy, risk and security compliance.

IT Operations

Employee hardware administration, office networks, telephone system management, internal user access rights management, network and device security monitoring and support of internal tools used by staff.

Data

Data, as defined by MealSuite, constitutes the following:

- Resident & Patient Data
- Food Nutrient Data
- Distributor/Procurement Vendor Data
- Compiled Reports
- Menus & Recipes

People Data is stored in the MealSuite system to provide clients with the opportunity to offer and serve foods that are appropriate for each person's specific allergies, dislikes, preferences, and diet order.

People Data is input into food service provider's application through a number of secure methods:

1. Manually by a user (Password and role authorization required).
2. Secure File Transfer Protocol (SFTP).
3. Secure Websites through Application Programming Interface (API) or Webservices transactions from secure Patient Information Systems.

Output Reports of people information are available in Portable Document Format (PDF) or Excel format, the availability of these reports can only be generated directly from the password protected MealSuite application.

Nutrient Data is stored in the MealSuite system to provide clients with detailed nutritional information that can be utilized to ensure that the recommended dietary allowance for each resident is being met, or that the information is readily available to their clients so that they can make their own informed decisions about their dietary choices.

Nutrient Data is provided from either an authorized government website or provided from a trusted Data Provider. Nutrient data is then imported into the MealSuite Master Data system and reviewed by the Nutrition Services team.

Output Reports are available in PDF or Excel format and can only be generated directly from the password protected MealSuite application. Nutrient Data can also be transmitted to a client's website using a MealSuite developed API connections secured by trusted security certificates.

Vendor Product Data is stored in the MealSuite system to provide the opportunity to cost their recipe and food data.

Master Recipe and Menu Data is available to clients within their database.

Facility specific Recipe and Menu data can only be input manually by the user directly into the password protected MealSuite database.

Health Information Security Program Processes, Policies and Procedures

MealSuite has developed a health information security management program to meet the information security and compliance requirements related to Cloud-Based FoodService Software Services System and its customer base. The program incorporates the elements of HIPAA and HITECH. The description below is a summary of safeguards that MealSuite 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 MealSuite 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 and reporting of 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.
- Third-party organizations are engaged to scan and monitor the MealSuite systems, 24/7.

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 protected health information (PHI) transmitted electronically over open networks from being intercepted by anyone other than the intended recipient:

- Access to in-scope systems is 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 Requirements - 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.
- 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 PHI, 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 PHI 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 Cloud-Based FoodService Software Services System performed in the Dallas, Texas (United States) facility.

This report does not include the data center hosting services provided by Digital Realty.

HIPAA/HITECH REQUIREMENTS AND RELATED CONTROLS

Organizational Structure and Assignment of Authority and Responsibility

MealSuite’s organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

MealSuite's assignment of authority and responsibility activities includes factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring 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.
- Role descriptions are available for review by employees.
- Employee growth tracks and career ladders are published to employees globally.

Risk Assessment Process

MealSuite's risk assessment process identifies and manages risks that could potentially affect MealSuite's ability to provide reliable services to clients' organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. MealSuite identifies the underlying sources of risk, measures the impact to organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process has identified risks resulting from the nature of the services provided by MealSuite, and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk - changes in the environment, staff, or management personnel
- Strategic risk - new technologies, changing business models, and shifts within the industry
- Compliance - legal and regulatory changes
- Data Security & Privacy - unauthorized access to clients' data

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of MealSuite's health information security management program; as well as the nature of the components of the system result in risks that the requirements will not be met. MealSuite addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the requirements are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the requirements and the controls necessary to address the risks will be unique. As part of the design and operation of the system, MealSuite's management identifies the specific risks that the requirements will not be met and the controls necessary to address those risks.

Periodic Assessments

MealSuite 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 MealSuite 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 monthly by a committee with representation from each department:

- *Risk Assessment*: The risk assessment is performed by the Privacy Officer. 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 brought forward to a committee, with a dedicated meeting defined to brainstorm potential risks and improvement opportunities. 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.

Periodic Testing and Evaluation

MealSuite 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
- Control tests by third-parties

Information and Communications Systems

Information and communication is an integral component of MealSuite's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, IT. At MealSuite, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Various weekly calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. Additionally, town hall meetings are held monthly to provide staff with updates on the company and key issues affecting the organization and its employees. Senior executives lead the town hall meetings with information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues. General updates to entity-wide security policies and procedures are usually communicated to the appropriate MealSuite personnel via e-mail messages.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. MealSuite's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

MealSuite's management conducts QA monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in MealSuite's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of MealSuite's personnel.

Reporting Deficiencies

An internal tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

Policies and Procedures

Health information security policies and procedures have been implemented regarding the protection of information assets. 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:

- Health information security policy
- Asset management
- Data classification
- Business continuity
- Incident management
- Access control
- Physical security

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

Security Awareness Training

MealSuite 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 and weekly security training videos (and quizzes) through a third-party vendor.

Incident Response

MealSuite 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 MealSuite’s internal control system are identified 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 requirements are not applicable to the system:

Requirements Not Applicable to the System		
Safeguard	**Requirement**	**Reason**
Administrative Safeguard	164.308(a)(4)(ii)(A)	The entity is not a healthcare clearinghouse.
Physical Safeguard	164.310(c)	The entity is not a covered entity.
Organizational Requirement	164.314(a)(2)(ii)	The entity is not a government entity.

	164.314(b)(1)
	164.314(b)(2)
		The entity is not a plan sponsor.

Breach Notification	164.404(a)(1), 164.404(a)(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

This report does not include the data center hosting services provided by Digital Realty.

Subservice Description of Services

MealSuite contracts with Digital Realty to host primary infrastructure within their data center.

Complementary Subservice Organization Controls

MealSuite'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 MealSuite's services to be solely achieved by MealSuite control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of MealSuite.

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

Subservice Organization - Digital Realty		
Safeguard	**Requirement**	**Applicable Controls**
Physical Safeguard	164.310(a)(1), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(a)(2)(iv), 164.310(b), 164.310(d)(2)(iii)	Documented physical security policies and procedures are in place to guide personnel in physical security practices. A badge access system is in place to restrict physical access to the facility authorized personnel.
		Administrative access within the badge access system is authorized to authorized personnel.
		Badge access is revoked as a component of the termination process.
		Authorized personnel perform access reviews quarterly.
		Visitors are required to be escorted by an authorized employee at all times.
		Visitors are required to wear badges that clearly differentiate them from the entity personnel.
		Documented physical security policies and procedures are in place to guide personnel in physical security practices.
		A role-based security process has been defined with an access control system that is required to use roles when possible.
		Documented policies and procedures are in place to document repairs and modifications to the physical components of a facility which are related to security.
		Procedures are in place to implement physical safeguards for all workstations that access ePHI to restrict access to all authorized users.
		A record of the movements of hardware and electronic media is maintained.

COMPLEMENTARY USER ENTITY CONTROLS

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

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the HIPAA/HITECH requirements 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 understanding and complying with their contractual obligations to MealSuite.
2. User entities are responsible for notifying MealSuite of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of MealSuite services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize MealSuite services.
6. User entities are responsible for providing MealSuite with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying MealSuite of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

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 are in place to guide personnel in addressing the threats posed by security incidents. 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 detection, logging, and monitoring of unknown or unauthorized components into the environment. The monitoring software is configured to alert IT personnel when thresholds have been exceeded. Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. An IPS is utilized to analyze network events and report possible or actual network security breaches. The IPS is configured to notify personnel upon intrusion prevention. File integrity monitoring (FIM) software is in place to ensure only authorized changes are deployed into the production environment. The FIM software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected. 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. Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available. The antivirus software is configured to scan workstations on a continuous basis.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		Internal and external vulnerability scans and penetration tests are performed on at least an annual basis and remedial actions are taken where necessary.
164.308 (a)(1)(ii)(A)	**Risk analysis:** an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI).	A formal risk assessment is performed on an annual basis to identify threats that could impair systems security, confidentiality, integrity, and availability of ePHI.
164.308 (a)(1)(ii)(B)	**Risk management:** Ensures the company implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306. Factors identified in §164.306 include: • The size, complexity, capability of the covered entity • The covered entity’s technical infrastructure • The costs of security measures • The probability and criticality of potential risks to ePHI	Management develops risk mitigation strategies to address risks identified during the risk assessment process. Internal and external vulnerability scans and penetration tests are performed on at least an annual basis and remedial actions are taken where necessary.
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.	The entity maintains policy and procedure documents that outline the process of sanctioning personnel who fail to comply with the security policies and procedures.
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.	Regular monitoring and review of log-ins and log-in attempts to the system is in place. Discrepancies and potentially inappropriate or illegal activities are reported to senior management, legal counsel and/or human resources, as appropriate.
	Network (Microsoft 365)	
		Network audit logging settings are in place. Network audit logs are maintained and reviewed as needed.
	Operating System (Linux)	
		Operating system audit logging settings are in place. Operating system audit logs are maintained and reviewed as needed.
	Database (PostgreSQL)	
		Database audit logging settings are in place. Database audit logs are maintained and reviewed as needed.
	Application (Ruby on Rails)	
		The application is configured to log user actions and system events.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		Application audit logs are maintained and reviewed as needed. Resolution of incidents are documented within the ticket and communicated to affected users. Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.
164.308 (a)(2)	**Assigned security responsibility:** Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity.	Responsibility for the development, implementation, and regular maintenance of the policies and procedures that govern the security of protected ePHI is assigned to the IT Senior Security Engineer.
164.308 (a)(3)(i)	**Workforce security:** Policies and procedures are implemented to ensure that all members of the workforce have appropriate access to ePHI, as provided under the Information Access Management standard and to prevent those who do not have appropriate access from obtaining access to ePHI. Policies and procedures should include Authorization and/or Supervision procedures, Workforce Clearance Procedure, and Termination Procedures.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring. Control self-assessments that include logical access reviews and backup restoration tests are performed at least on an annual basis. Logical access to systems is approved and granted to an employee as a component of the hiring process. Logical access to systems is revoked for an employee as a component of the termination process.
	Network	
		Network user access is restricted via role-based security privileges defined within the access control system. Network administrative access is restricted to user accounts accessible by authorized personnel.
	Operating System	
		Operating system user access is restricted via role-based security privileges defined within the access control system. Operating system administrative access is restricted to user accounts accessible by authorized personnel.
	Database	
		Database user access is restricted via role-based security privileges defined within the access control system. Database administrative access is restricted to user accounts accessible by authorized personnel.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
	Application	
		Application user access is restricted via role-based security privileges defined within the access control system. Application administrative access is restricted to user accounts accessible by authorized personnel.
	Remote Access	
		Virtual Private Network (VPN) user access is restricted via role-based security privileges defined within the access control system. The ability to administer VPN access is restricted to user accounts accessible by authorized personnel.
164.308 (a)(3)(ii)(A)	**Authorization and/or supervision:** Ensures the authorization and/or supervision of workforce members who work with ePHI or in locations where it might be accessed.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring. Control self-assessments that include logical access reviews and backup restoration tests are performed at least on an annual basis. Logical access to systems is approved and granted to an employee as a component of the hiring process. Logical access to systems is revoked for an employee as a component of the termination process.
164.308 (a)(3)(ii)(B)	**Workforce clearance procedure:** Access of a workforce member (employee or computing device) to ePHI is appropriate.	Access control and role-based build procedures are in place to restrict access to systems that maintain ePHI to only authorized personnel. Control self-assessments that include logical access reviews and backup restoration tests are performed at least on an annual basis. Logical access to systems is approved and granted to an employee as a component of the hiring process. Logical access to systems is revoked for an employee as a component of the termination process.
164.308 (a)(3)(ii)(C)	**Termination procedures:** Ensure that access to ePHI is terminated as soon as possible when a workforce member's employment ends.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring. Logical access to systems is revoked for an employee as a component of the termination process.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.308 (a)(4)(i)	**Information access management:** Policies and procedures are implemented that ensure authorizing access to ePHI and are consistent with the applicable requirements of the Privacy Rule. Policies and procedures should include: Isolating Health Care Clearinghouse Functions, Access Authorization and Access Establishment and Modification.	Management maintains policies and procedures that ensure the authorization of access to ePHI and are consistent with the applicable requirements of the Privacy Rule.
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 ePHI 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 an example, through access to a workstation, transaction, program, process, or other mechanism.	Access control and role-based build procedures are in place to restrict access to systems that maintain ePHI to only authorized personnel. Logical access to systems is approved and granted to an employee 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.	Access control and role-based build procedures are in place to restrict access to systems that maintain ePHI to only authorized personnel. Logical access to systems is approved and granted to an employee as a component of the hiring process. Logical access to systems is revoked for an employee as a component of the termination process. Control self-assessments that include logical access reviews and backup restoration tests are performed at least on an annual basis.
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.	Management conducts periodic security awareness training to establish the organization's commitments and requirements for employees. Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel. Upon hire, employees are required to complete information security and awareness training. Current employees are required to complete information security and awareness training on an annual basis.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.308 (a)(5)(ii)(A)	**Security reminders:** Periodic security updates.	Users are made aware of security updates and updates to security policies via e-mail notifications.
164.308 (a)(5)(ii)(B)	**Protection from malicious software:** Procedures for guarding against, detecting, and reporting malicious software.	A program of techniques, technologies, and methods to guard against, detect, and report the presence of malicious software is in place. Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available. The antivirus software is configured to scan workstations on a continuous basis. Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. An IPS is utilized to analyze network events and report possible or actual network security breaches. The IPS is configured to notify personnel upon intrusion prevention.
164.308 (a)(5)(ii)(C)	**Log-in monitoring:** Procedures for monitoring log-in attempts and reporting discrepancies.	Regular monitoring and review of log-ins and log-in attempts to the system is in place. Discrepancies and potentially inappropriate or illegal activities are reported to senior management, legal counsel and/or human resources, as appropriate.
	Network	
		Network audit logging settings are in place. Network audit logs are maintained and reviewed as needed.
	Operating System	
		Operating system audit logging settings are in place. Operating system audit logs are maintained and reviewed as needed.
	Database	
		Database audit logging settings are in place. Database audit logs are maintained and reviewed as needed.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
	Application	
164.308 (a)(5)(ii)(D)	**Password management:** Procedures for creating, changing, and safeguarding passwords.	The application is configured to log user actions and system events. Application audit logs are maintained and reviewed as needed. Resolution of incidents are documented within the ticket and communicated to affected users. Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution. Policies are in place to guide personnel in creating, changing, and safeguarding passwords for network devices and servers.
	Network	
		Networks are configured to enforce password requirements that include: • Password age • Password length • Complexity • Multifactor authentication (MFA)
	Operating System	
		Operating systems are configured to enforce secure shell (SSH) authentication configurations.
	Database	
		Databases are configured to enforce password requirements.
	Application	
		The application is configured to enforce password requirements that include password length and complexity.
	Remote Access	
164.308 (a)(6)(i)	**Security incident procedures:** Implement policies and procedures to address security incidents. Policies and procedures should include response reporting.	VPN users are authenticated via MFA prior to being granted remote access to the system. 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. The incident response and escalation procedures are reviewed at least annually for effectiveness.

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.	The incident response policies and procedures define the classification of incidents based on its severity. Resolution of incidents are documented within the ticket and communicated to affected users. Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution. Identified incidents are reviewed, monitored and investigated by an incident response team. 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. 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. The incident response and escalation procedures are reviewed at least annually for effectiveness. The incident response policies and procedures define the classification of incidents based on its severity. Resolution of incidents are documented within the ticket and communicated to affected users. Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution. Identified incidents are reviewed, monitored and investigated by an incident response team. 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.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.308 (a)(7)(i)	**Contingency plan:** Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for an example, fire, vandalism, system failure, and natural disaster) that damages systems that contain ePHI.	Business continuity and disaster recovery plans are developed and updated on an annual basis. Business continuity and disaster recovery plans are tested on an annual basis. A business continuity plan is documented and in place that outlines the range of disaster scenarios and steps the business will take in a disaster to ensure the timely resumption of critical business operations.
164.308 (a)(7)(ii)(A)	**Data backup plan:** Establish and implement procedures to create and maintain retrievable exact copies of ePHI.	Procedures are in place to provide for complete, accurate, and timely storage of data. The ways in which critical data are backed up and stored are documented and reviewed annually. Data backup and restore procedures are in place to guide personnel in performing backup activities. Full backups of certain application and database components are performed on a daily basis. When a backup job fails, the backup tool sends an alert to the backup administrators who investigate and resolve the failure. Data backed up is replicated to an offsite facility in real-time. Control self-assessments that include backup restoration tests are performed on a semi-annual basis.
164.308 (a)(7)(ii)(B)	**Disaster recovery plan:** Establish (and implement as needed) procedures to restore any loss of data.	Business continuity and disaster recovery plans are developed and updated on an annual basis. Business continuity and disaster recovery plans are tested on an annual basis. The disaster recovery plan includes moving the business operations and supporting systems to an alternate site if needed. A business continuity plan is documented and in place that outlines the range of disaster scenarios and steps the business will take in a disaster to ensure the timely resumption of critical business operations.
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.	Business continuity and disaster recovery plans are developed and updated on an annual basis. Business continuity and disaster recovery plans are tested on an annual basis. The disaster recovery plan includes moving the business operations and supporting systems to an alternate site if needed.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		A business continuity plan is documented and in place that outlines the range of disaster scenarios and steps the business will take in a disaster to ensure the timely resumption of critical business operations.
164.308 (a)(7)(ii)(D)	**Testing and revision procedures:** Implement procedures for periodic testing and revision of contingency plans.	Business continuity and disaster recovery plans are developed and updated on an annual basis. Business continuity and disaster recovery plans are tested on an annual basis.
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 has defined what critical data is processed and how it is processed. Data and information critical to the system is assessed annually for relevance and use. For each critical system, the entity defines and documents what data and information is critical to support the system. The entity has defined the following components of the data critical to supporting the system: • A description of what the critical data is and is used for • Source of the data • How the data is stored and transmitted The entity's risk assessment process includes: • Identifying the relevant information assets that are critical to business operations • Prioritizing the criticality of those relevant information assets • Identifying and assessing the impact of the threats to those information assets • Identifying and assessing the impact of the vulnerabilities associated with the identified threats • Assessing the likelihood of identified threats and vulnerabilities • Determining the risks associated with the information assets • Addressing the associated risks identified for each identified vulnerability
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.	Changes to the business structure and operations are considered and evaluated as part of the annual comprehensive risk assessment. Changes in key management and personnel are considered and evaluated as part of the annual comprehensive risk assessment. Changes to the entity's systems, applications, technologies, and tools are considered and evaluated as part of the annual comprehensive risk assessment.

ADMINISTRATIVE SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
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.	The entity maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI.
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.
164.308 (b)(3)	**Written contract or other arrangement:** Document the satisfactory assurances required by paragraph (b)(1) [the Business Associates Contracts and Other Arrangements] of this section through a written or other 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.
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.

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 organization. Refer to the “Subservice Organizations” section above for controls managed by the subservice organization.
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.	Business continuity and disaster recovery plans are developed and updated on an annual basis. Business continuity and disaster recovery plans are tested on an annual basis.
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 organization. Refer to the “Subservice Organizations” section above for controls managed by the subservice organization.
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 organization. Refer to the “Subservice Organizations” section above for controls managed by the subservice organization.
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 an example, hardware, walls, doors, and locks).	This regulation is the responsibility of the subservice organization. Refer to the “Subservice Organizations” section above for controls managed by the subservice organization.
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. 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.
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.
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.
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 confidential data after it is no longer required to achieve the purpose for which the data was collected and processed.

PHYSICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		Policies and procedures are in place for removal of media storing critical data or software.
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.	Documented data retention and disposal policy and procedures are in place that include the following: • Defining, identifying and designating information as confidential • Storing confidential information • Protecting confidential information from erasure or destruction • Retaining confidential information for only as long as is required to achieve the purpose for which the data was collected and processed The entity purges confidential data after it is no longer required to achieve the purpose for which the data was collected and processed. An inventory log is maintained of assets with confidential data. Confidential information is protected from erasure or destruction during the specified retention period.
164.310 (d)(2)(iii)	**Accountability:** Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	This regulation is the responsibility of the subservice organization. Refer to the “Subservice Organizations” section above for controls managed by the subservice organization.
164.310 (d)(2)(iv)	**Data backup and storage:** Create a retrievable, exact copy of ePHI, when needed, before movement of equipment.	Procedures are in place to provide for complete, accurate, and timely storage of data. The ways in which critical data are backed up and stored are documented and reviewed annually. Data backup and restore procedures are in place to guide personnel in performing backup activities. Full backups of certain application and database components are performed on a daily basis. When a backup job fails, the backup tool sends an alert to the backup administrators who investigate and resolve the failure. Data backed up is replicated to an offsite facility in real-time. Control self-assessments that include backup restoration tests are performed on a semi-annual 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).	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring. Logical access to systems is approved and granted to an employee as a component of the hiring process. Logical access to systems is revoked for an employee as a component of the termination process.
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 settings, authentication, access, and security monitoring.
	Network	
		Network user access is restricted via role-based security privileges defined within the access control system. Network audit logging settings are in place. Network audit logs are maintained and reviewed as needed.
	Operating System	
		Operating system user access is restricted via role-based security privileges defined within the access control system. Operating system audit logging settings are in place. Operating system audit logs are maintained and reviewed as needed.
	Database	
		Database user access is restricted via role-based security privileges defined within the access control system. Database audit logging settings are in place. Database audit logs are maintained and reviewed as needed.
	Application	
		Application user access is restricted via role-based security privileges defined within the access control system. The application is configured to log user actions and system events.

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		Application audit logs are maintained and reviewed as needed.
	Remote Access	
		VPN user access is restricted via role-based security privileges defined within the access control system.
164.312 (a)(2)(ii)	**Emergency access procedure:** Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.	Business continuity and disaster recovery plans are developed and updated on an annual basis. Business continuity and disaster recovery plans are tested on an annual basis. A business continuity plan is documented and in place that outlines the range of disaster scenarios and steps the business will take in a disaster to ensure the timely resumption of critical business operations. The ways in which critical data are backed up and stored are documented and reviewed annually. Data backup and restore procedures are in place to guide personnel in performing backup activities. Full backups of certain application and database components are performed on a daily basis. When a backup job fails, the backup tool sends an alert to the backup administrators who investigate and resolve the failure. Data backed up is replicated to an offsite facility in real-time. Control self-assessments that include backup restoration tests are performed on a semi-annual basis.
164.312 (a)(2)(iii)	**Automatic logoff:** Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.
	Network	
		Network account lockout settings are in place that include: • Account lockout duration • Account lockout threshold
	Operating System	
		Operating system account lockout settings are in place for account lockout threshold and duration.
	Database	
		Database account lockout settings are in place.

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
	Application	
		Application account lockout settings are in place for lockout threshold and lockout duration.
	Remote Access	
		VPN account lockout settings are in place for account lockout threshold and lockout release timeout.
164.312 (a)(2)(iv)	**Encryption and decryption:** Implement a mechanism to encrypt and decrypt ePHI.	Server certificate-based authentication is used as part of the Transport Layer Security (TLS) encryption with a trusted certificate authority.
		VPN, TLS and other encryption technologies are used for defined points of connectivity.
		Transmission of digital output beyond the boundary of the system is encrypted.
		Critical data is stored in encrypted format using software supporting the Advanced Encryption Standard (AES).
		Backup media is stored in an encrypted format.
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.	Regular monitoring and review of log-ins and log-in attempts to the system is in place. Discrepancies and potentially inappropriate or illegal activities are reported to senior management, legal counsel and/or human resources, as appropriate.
	Network	
		Network audit logging settings are in place. Network audit logs are maintained and reviewed as needed.
	Operating System	
		Operating system audit logging settings are in place. Operating system audit logs are maintained and reviewed as needed.
	Database	
		Database audit logging settings are in place. Database audit logs are maintained and reviewed as needed.
	Application	
		The application is configured to log user actions and system events. Application audit logs are maintained and reviewed as needed.

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.312 (c)(1)	**Integrity:** Implement policies and procedures to protect ePHI from improper alteration or destruction.	Data that entered into the system, processed by the system and output from the system is protected from unauthorized access. FIM software is in place to ensure only authorized changes are deployed into the production environment. FIM software is utilized to help detect unauthorized changes within the production environment. The FIM software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.
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.	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. FIM software is in place to ensure only authorized changes are deployed into the production environment. FIM software is utilized to help detect unauthorized changes within the production environment. The FIM software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.
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 settings, authentication, access, and security monitoring.
	Network	
		Network user access is restricted via role-based security privileges defined within the access control system. Network administrative access is restricted to user accounts accessible by authorized personnel. Networks are configured to enforce password requirements that include: • Password age • Password length • Complexity • MFA Network account lockout settings are in place that include: • Account lockout duration • Account lockout threshold

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		Network audit logging settings are in place. Network audit logs are maintained and reviewed as needed.
	Operating System	
		Operating system user access is restricted via role-based security privileges defined within the access control system. Operating system administrative access is restricted to user accounts accessible by authorized personnel. Operating systems are configured to enforce SSH authentication configurations. Operating system account lockout settings are in place for account lockout threshold and duration. Operating system audit logging settings are in place. Operating system audit logs are maintained and reviewed as needed.
	Database	
		Database user access is restricted via role-based security privileges defined within the access control system. Database administrative access is restricted to user accounts accessible by authorized personnel. Databases are configured to enforce password requirements. Database account lockout settings are in place. Database audit logging settings are in place. Database audit logs are maintained and reviewed as needed.
	Application	
		Application user access is restricted via role-based security privileges defined within the access control system. Application administrative access is restricted to user accounts accessible by authorized personnel. The application is configured to enforce password requirements that include password length and complexity. Application account lockout settings are in place for lockout threshold and lockout duration.

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		The application is configured to log user actions and system events. Application audit logs are maintained and reviewed as needed.
	Remote Access	
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.	VPN user access is restricted via role-based security privileges defined within the access control system. The ability to administer VPN access is restricted to user accounts accessible by authorized personnel. VPN users are authenticated via MFA prior to being granted remote access to the system. Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority. VPN, TLS and other encryption technologies are used for defined points of connectivity. Transmission of digital output beyond the boundary of the system is encrypted.
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.	Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority. VPN, TLS and other encryption technologies are used for defined points of connectivity. Transmission of digital output beyond the boundary of the system is encrypted. 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. FIM software is in place to ensure only authorized changes are deployed into the production environment. FIM software is utilized to help detect unauthorized changes within the production environment. The FIM software is configured to notify IT personnel via e-mail alert when a change to the production application code files is detected.
164.312 (e)(2)(ii)	**Encryption:** Implement a mechanism to encrypt ePHI whenever deemed appropriate.	Server certificate-based authentication is used as part of the TLS encryption with a trusted certificate authority.

TECHNICAL SAFEGUARDS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		VPN, TLS and other encryption technologies are used for defined points of connectivity. Transmission of digital output beyond the boundary of the system is encrypted. Critical data is stored in encrypted format using software supporting the AES. Backup media is stored in an encrypted format.

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.
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.
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.	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 plan sponsor.
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.	Management reviews policies, procedures and other control documents for accuracy and applicability on an annual basis. Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the entity's Intranet.
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.	Management reviews policies, procedures and other control documents for accuracy and applicability on an annual basis. Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the entity's Intranet.
164.316 (b)(1)(i)	**Time Limit:** Retain the documentation required by paragraph (b) (1) of this section for 6 years for the date of its creation or the date when it last was in effect, whichever is later.	The entity retains all documentation for a minimum period of six (6) years from the date of its creation or modification, or the date when it was last in effect.
164.316 (b)(1)(ii)	**Availability:** Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the entity's Intranet.

ORGANIZATIONAL REQUIREMENTS		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.316 (b)(1)(ii)	**Updates:** Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the ePHI.	Management reviews policies, procedures and other control documents for accuracy and applicability on an annual basis.

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.	The entity has documented policies and procedures in place that outline the security of protected health information to prevent a breach.
164.404 (a)(1)	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 (a)(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 that define the required steps to notify the covered entity following the discovery of a breach of unsecured protected health information.
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 whose unsecured ePHI has been accessed during the breach is disclosed during notification procedures.

BREACH NOTIFICATION		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
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.	The entity refrains from, or delays notifying HHS personnel, the covered entity, or other required persons following the discovery of a breach of unsecured protected health information when required by law.
164.414	**Administrative requirements and burden of proof**: 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 MealSuite was limited to the HIPAA/HITECH requirements and related control activities specified by the management of MealSuite and did not encompass all aspects of MealSuite’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.