ACD Direct

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

Table of Contents

SECTION 1

ASSERTION OF ACD DIRECT MANAGEMENT

ASSERTION OF ACD DIRECT MANAGEMENT

November 5, 2019

We have prepared the description of ACD Direct' ("ACD" or "the Company") health information security program for the Non-Profit Marketing and Pledge Call Center services system (the "description") for user entities of the system as of July 31, 2019. We confirm, to the best of our knowledge and belief, that:

a. Management's description fairly presents the health information security program for the Non-Profit Marketing and Pledge Call Center services system as of July 31, 2019. 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 Non-Profit Marketing and Pledge Call Center 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 Non-Profit Marketing and Pledge Call Center 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 Non-Profit Marketing and Pledge Call Center services system includes essential elements 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 met the standard and implementation guidance for safeguards as defined by the HIPAA Security Rule including the following:
        - Administrative Safeguards;
        - Physical Safeguards;
        - Organizational Safeguards; and
        - Breach Notification

Section 3 of this report includes ACD's description of the health information security program for the Non-Profit Marketing and Pledge Call Center services system that are covered by this assertion.

Dolores Lobato

Dolores Lobato
Director of IT
ACD Direct

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To ACD Direct:

We have examined ACD Direct's (ACD) assertion that the description of its health information security program for the ACD's Non Profit Marketing and Pledge Call Center services system listed in Section 3 (the "description") provided to user entities as of July 31, 2019, is fairly presented and that the health information security program governing the Non Profit Marketing and Pledge Call Center services system includes essential elements 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, is presented in accordance with the criteria set forth in ACD's assertion in Section 2. ACD's management is responsible for the assertion. Our responsibility is to express an opinion based on our examination.

ACD uses Flexential ("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 ACD's system; its controls relevant to the applicable HIPAA/HITECH requirements; and the types of controls that the service organization expects 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 ACD's health information security program for the Non Profit Marketing and Pledge Call Center services system and performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

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

In our opinion, in all material respects, based on the criteria described in ACD's assertion in Section 2:

a. The description fairly presents the health information security program for the Non Profit Marketing and Pledge Call Center services system that was designed and implemented as of July 31, 2019; and
b. The health information security program governing the Non Profit Marketing and Pledge Call Center services system includes essential elements of HIPAA and HITECH.

This report and the description of tests of controls and results thereof are intended solely for the information and use of ACD; user entities of ACD's Non Profit Marketing and Pledge Call Center services system as of July 31, 2019; 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 (which it then bullet points out some items):

- 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 how they interact with related controls at the service organization to meet the HIPAA security program
- The HIPAA security program
- The risks that may threaten the achievement of the HIPAA security program 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

November 5, 2019
Tampa, Florida

SECTION 3

ACD DIRECT'S DESCRIPTION OF ITS NON PROFIT MARKETING AND PLEDGE CALL CENTER SERVICES SYSTEM AS OF JULY 31, 2019

OVERVIEW OF OPERATIONS

Company Background

ACD was founded in 2003 as a contact center services and utilize their partnerships and the exposure to coast-to-coast markets to provide viable solutions, best practices and guidance when and where needed.

Experienced: Since 2003, ACD has been a virtual business continually working to expand their solutions and partnerships with public entities and nonprofit organizations across the U.S., while adhering to the core values of being people-centric, proactive and a solutions broker. ACD currently provides customized solutions to more than 150 clients, the majority being PBS stations.

Qualified: ACD strive to gain in-depth insight into their client's industry and to understand the needs, demands and challenges. ACD take the time to collaborate with experienced vendors and industry experts to help align with the goals and objectives of each client.

Responsive: ACD provides 24/7 support to everyone involved from the client and its constituents to the and their agents. ACD responds by providing inbound and outbound call services, web-based support options (chat, text, e-mail) and applications to facilitate customer information management.

Description of Services Provided

ACD provides a database management solution services with an advanced communications, throughout the United States. The Company was founded in 2003 to provide Non Profit Marketing and Pledge Call Center services to its customers. ACD's integration of a database management solution with an advanced communications platform will help automate and optimize communications.

Description of Services:

- Outbound and Inbound Call Services
- Web Based Chat Support
- Click to Dial - The "Click to Chat" option allows visitors on the customer's website to be quickly connected to one of ACD's agents
- Text Messaging/E-mail Support
- Tiered Member Services Support - Member Services Support (MSS) provides customers with scalable support. This skill-based tiering allows customers to choose the level of support necessary from solving coverage issues
- Custom Development Team - ACD's development team can create a customizable solution to meet customer's specific needs
- Simple Script - Simple Script is a dynamic and fully customizable scripting solution for call handling needs. All payment processing is handled through third-party API. Data captured within Simple Script can be exported in a wide variety of formats via several secure transmission vehicles. (i.e. Web Service, FTP Transfer, Direct Download)
- Ticketing-Based Help Desk Application - Issue tracking is handled through ACD's Help Desk Application
- TroubleShooter - ACD's Troubleshooter is built on a foundation of decision tree scripting. Quick answers to common questions allows a call path to be handled efficiently. Additional options can be added at any time
- Referral Database Warehousing - Simple Script is ACD's Referral Database module which streamlines information storage by housing lists of contacts in a searchable, easily accessible format. Information will be at the ready when needed
- Mobile Responsive Online Data Entry Web Forms - Capture data from anywhere or anytime. The application was built on the same premise of Simple Script
- Payment Processing Integration - ACD has integrated with several major payment processing gateways. ACD is Level 1 PCI Compliant

- Reporting Suite - ACD's reporting suite allows customers the ability to track calls and transactions with ease. Reports can be accessed from anywhere allowing customers to gauge the success of their campaign 24/7/365
- Pledge Cart 3.0 - Pledge Cart 3.0 provides a simple, clean, mobile responsive approach to capturing online donations
- On Hold Streaming - On Hold Streaming is a service offered that provides callers with relevant content with the power of live streaming. This is optimized for the telecommunications medium to ensure that callers have the best listening experience
- Call-Center-In-A-Box Total.Care Solution - This is a web based platform that plays the role of switchboard, receptionist, and answering service, allowing customers to manage and route all phone calls, set users/voice-mails/greetings, and streamline communications
- Cloud Based Telephony Platform - By utilizing a cloud base telephony platform, ACD can offer a highly flexible, customized contact routing solution that supports call routing and web based chat support. Cloud based routing is secure and provides necessary redundancy to limit outages
- Toll Free/Local Number Procurement Assistance - ACD can help with procuring toll free or local numbers (i.e. Vanity Number). ACD can also assist with customers' search and purchase of this number

Donations are tracked through the payment cycle, from initial call assignment to completion of the payment. System-generated reports provide supporting documentation for donations.

Information is shared with user entities by telephone, fax, secure electronic exchange (FTP [file transfer protocol], e-mail, EDI [electronic data interchange]), and secured websites.

Electronic Protected Health Information (ePHI) Transmission, Processing & Reporting

ACD does not currently store, process or transmit customer ePHI data.

Principal Service Commitments and System Requirements

ACD designs its processes and procedures related to Non Profit Marketing and Pledge Call Center services to meet its objectives for its marketing and pledge call services. Those objectives are based on the service commitments that ACD makes to user entities, the laws and regulations that govern the provision of marketing and pledge call services, and the financial, operational, and compliance requirements that ACD has established for the services. The marketing and pledge call services of ACD are subject to the security and privacy requirements of the Health Insurance Portability and Accountability Act Administrative Simplification, as amended, including relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which ACD operates.

To safeguard ACD's information technology resources and to protect the confidentiality of data, adequate security measures must be taken. ACD's Full Security Policy reflects ACD's commitment to comply with required standards governing the security of sensitive and confidential information.

ACD minimizes inappropriate exposures of confidential or sensitive information, loss of data and inappropriate use of computer networks and systems by complying with reasonable standards (such as Payment Card Industry Data Security Standard), attending to the proper design and control of information systems, and applying sanctions when violations of this security policy occur.

Security is the responsibility of everyone who uses ACD's information technology resources. It is the responsibility of employees, contractors, business partners, and agents of ACD Direct. Each is familiar with this policy's provisions and the importance of adhering to it when using ACD's computers, networks, data and other information resources. Each is responsible for reporting any suspected breaches of its terms. As such, all information technology resource users are expected to adhere to all policies and procedures mandated by the IT Supervisor and Director of IT at ACD Direct.

All ACD employees undergo background checks and participate in annual security trainings, security scans, and performance reviews. They acknowledge all company policies through ADP, ACD's payroll processor.

All ACD clients understand and acknowledge their security and confidentiality roles related to data, as spelled out in contracts and letters of agreement.

All ACD data partners and data vendors meet or exceed the compliance levels and standards as ACD Direct.

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 Non Profit Marketing and Pledge Call Center services.

Components of the System

Infrastructure

Primary infrastructure used to provide ACD Direct's Non Profit Marketing and Pledge Call Center services system includes the following:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Firewall	PaloAlto	Filters traffic from the internet to the MGMT.
Firewall	PaloAlto	Filters traffic redundantly to the DMZ network.
Switches	Cisco	Splits up network traffic between MGMT DMZ.
Switches	Cisco	Splits up network traffic between MGMT LAN.
Server Hardware	Dell ESX	1u host server MGMT
Server Hardware	Dell ESX	1u host server DMZ
Server Hardware	Dell ESX	1u host server LAN
VM's	VMware ESXi Host	Integrates ACD's ESX servers into a virtual environment.
NAC	Milton	This appliance is referenced by gateway and CWW for call center agents to be able to user ACD's applications. Users must comply with this devices security polices before being able to access their accounts in GW/CWW for the application.

Software

Primary software used to provide ACD Direct's Non Profit Marketing and Pledge Call Center services system includes the following:

Primary Software		
Software	**Operating System**	**Purpose**
VMware	VMware ESXi	enterprise-class, type-1 hypervisor developed by VMware for deploying and serving virtual computers.
Kayako	Ubuntu Linux (64-bit)	Help desk support ticket software
Microsoft SQL	Microsoft Windows Server 2012 (64-bit)	Database software
FortiSIEM	Red Hat Enterprise Linux 6 (64-bit)	Network monitoring software. Incident management
McAfee	Microsoft Windows Server 2012 (64-bit)	Antivirus Software

People

The ACD staff provides support for the above services in each of the following functional areas:

- Executive Management - provides general oversight and strategic planning of operations
- Development Team - responsible for delivering a responsive system that fully complies with the functional specification
- System Administrators - responsible for effective provisioning, installation/configuration, operation, and maintenance of systems hardware and software relevant to the system
- Contact Center - serves customers by providing service that includes resolving product and service issues
- Client Management & Sales - responsible for drafting and executing contracted services for each respective client
- Project Management - performs regularly scheduled audits relative to defined standards, provides continuous improvement feedback, and assesses legal and regulatory requirements

Data

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer contracts.

Such data includes, but is not limited to, the following:

- Alert notifications and monitoring reports generated from the commercial monitoring applications
- Alert notifications received from automated backup systems
- Vulnerability or security alerts received from various sources including security subscriptions, scanning tools, IDS alerts, or automated patching systems
- Incident reports documented via the ticketing systems

Output reports are available in electronic PDF, comma-delimited value file exports, or electronically from the various websites. Reports delivered externally will only be sent using a secure method—encrypted e-mail, secure FTP, or secure websites—to transportation providers, treating facilities, and governments or managed care providers using ACD Direct-developed websites or over connections secured by trusted security certificates. ACD uses Transport Layer Security to encrypt e-mail exchanges with government or managed care providers, facility providers, and transportation providers.

Health Information Security Program Processes, Policies and Procedures

ACD has developed a health information security management program to meet the information security and compliance requirements related to Non Profit Marketing and Pledge Call Center services and its customer base. The program incorporates the elements of the HIPAA and the HITECH. The description below is a summary of safeguards that ACD 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 ACD complies with the act:

- Management has adopted a written set of health information security policies and designated the information security officer to be responsible for developing and implementing the required policies and procedures.
- Procedures address access authorization, establishment, modification, and termination.
- Documented incident response policies for reporting security incidents are in place to guide employees in identifying, reporting, 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 on certain production servers.

Physical Safeguards - Controlling physical access to protected data:

- Documented physical security policies and procedures are in place to guide personnel in physical security administration.
- Physical access procedures are in place 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.

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

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

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

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

Boundaries of the System

The scope of this report includes the Health Information Security Program for Non Profit Marketing and Pledge Call Center services system performed in the Orem, Utah facility.

HIPAA/HITECH REQUIREMENTS AND RELATED CONTROLS

Organizational Structure and Assignment of Authority and Responsibility

ACD Direct'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.

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

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

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

Risk Assessment Process

ACD Direct's risk assessment process identifies and manages risks that could potentially affect ACD's ability to provide reliable call center services to non-profit organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. ACD 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 ACD, 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 non-profit industry
- Compliance - legal and regulatory (PCI / SOC2) changes

ACD has established a Compliance Team that is responsible for identifying risks to the entity and monitoring the operation of the firm's internal controls. The approach is intended to align the entity's strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing non-profit marketplace. ACD does actively identify and mitigate significant risks through the implementation of various security initiatives and continuous communication with other leadership committees and senior management.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of ACD Direct's Non Profit Marketing and Pledge Call Center services system; as well as the nature of the components of the system result in risks that the safeguards will not be met. ACD addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the safeguards are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the safeguards and the controls necessary to address the risks will be unique. As part of the design and operation of the system, ACD Direct's management identifies the specific risks that the safeguards will not be met and the controls necessary to address those risks.

Periodic Assessments

ACD 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 ACD to assess the risks while providing services and develop mitigation strategies to address those risks. This process requires the Company to identify risk based on management's internal knowledge of its operations. The following risk factors are discussed among the executive management including the Director of IT and IT Supervisor at periodic intervals:

- *Risk Assessment*: The risk assessment is performed by the risk management personnel. Risk factors associated with the delivery or implementation of services to customers are evaluated considering process owners, dependencies, timelines and quality

Health Information Security Risks: Health information security risks are assessed by Director of IT. Risk factors associated with the organization are evaluated considering compliance obligations, laws and regulations, policies and procedures, contracts and best practices to which the organization has committed to. Information security assessments carried out by risk management personnel are rolled up to the Director of IT and IT Supervisor of the organization.

Periodic Testing and Evaluation

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

- Internal risk assessments
- Corrective action plans
- Management reviews

Information and Communications Systems

Information and communication is an integral component of ACD'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, information technology. At ACD, 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 through Skype to provide staff with updates on the firm 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 ACD personnel via e-mail messages.

Specific information systems used to support ACD Direct's Non Profit Marketing and Pledge Call Center services system are described in the Description of Services section above.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. ACD'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

ACD's management conducts quality assurance 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 ACD'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 ACD'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. The policies and procedures act as a guide for all ACD personnel. These policies and procedures define guidelines for the health information security program related to scope of services, which includes implementing and managing logical access security and controls, including the following:

- 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

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

Incident Response

ACD 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 ACD Direct's internal control system surface from many sources, including the Company's ongoing monitoring procedures, separate evaluations of the internal control system, and external parties. Management has developed protocols to help ensure findings, if identified, of internal control non-compliant items should be reported not only to the individual responsible for the function or activity involved, who is in the position to take corrective action. This process enables that individual to provide needed support or oversight for taking corrective action, and to communicate with others in the organization whose activities may be affected. Management evaluates the specific facts and circumstances related to areas of non-compliance in internal control procedures and make the decision for addressing any non-compliant items based on whether the incident was isolated or requires a change in the Company's procedures or personnel.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the review date.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the review date.

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 Safeguards	164.308 (a)(4)(ii)(A)	The entity is not a healthcare clearinghouse.
Organizational Requirements	164.314 (a)(2)(ii)	The entity is not a government entity.
	164.314 (b)(1)	The entity is not a plan sponsor.
	164.314 (b)(2)	
Breach Safeguards	164.402	The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.

Requirements Not Applicable to the System		
Safeguard	**Requirement**	**Reason**
	164.404 (a)	The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
	164.404 (b)	The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
	164.404 (c)(1)	The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
	164.404 (c)(2)	The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
	164.404 (d)(1)(i)	The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
	164.404 (d)(1)(ii)	The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
	164.404 (d)(2)	The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
	164.404 (d)(2)(i)	The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
	164.404 (d)(2)(ii)	The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
	164.404 (d)(3)	The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
	164.406	The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
	164.408 (a)	The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
	164.408 (b)	The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
	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 Flexential.

Subservice Description of Services

Flexential provided data hosting services for ACD Direct. Flexential provided added security such as physical data center security, formal access procedures, as well as equipment delivery and storage.

Complementary Subservice Organization Controls

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

The following subservice organization controls have been implemented by Flexential and included in this report to provide additional assurance that the safeguards are met.

Subservice Organization - Flexential		
Safeguard	**Requirement**	**Control**
Physical Safeguards	164.310 (a)(1) 164.310 (a)(2)(ii)	Two separate two-factor authentication systems are utilized to control access to the data centers. The systems require the following before granting access: • Access card and PIN at building entrances • Access card and biometric scan at data center entrance
	164.310 (a)(2)(i)	The data centers are equipped with fueled electric power generators to provide backup power in the event of a power outage.
	164.310 (a)(2)(i)	The data centers are connected to multiple redundant UPS systems configured to provide temporary electricity in the event of a power outage.
	164.310 (a)(2)(iii)	Visitors are required to wear a visitor badge while visiting the data centers.
	164.310 (a)(2)(iii)	Data center visitors are required to be accompanied and supervised by an authorized Flexential employee or client escort.
	164.310 (a)(2)(iii)	Visitors are required to sign-in with onsite security personnel prior to entering the data centers.
	164.310 (a)(2)(iii)	Client equipment is maintained in lockable cages or racks within the data centers.

Subservice Organization - Flexential		
Safeguard	**Requirement**	**Control**
	164.310 (a)(2)(i) 164.310 (a)(2)(iii)	Documented security procedures are in place to govern vendor access to the data centers, and include, but are not limited to, the following: • Health and safety • Vendor Verification and Access • Vendor Accountability • Maintenance activity logging
	164.310(a)(2)(iv)	Vendors are required to sign a vendor accountability form to perform maintenance in the data centers.

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

- Reviewing attestation reports over services provided by vendors and subservice organization
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

Complementary User Entity Controls

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

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

1. User entities are responsible for understanding and complying with their contractual obligations to ACD Direct.
2. User entities are responsible for notifying ACD of changes made to technical or administrative contact information.
3. User entities are responsible for ensuring the supervision, management, and control of the use of ACD services by their personnel.
4. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize ACD services.
5. User entities are responsible for providing ACD with a list of approvers for security and system configuration changes for data transmission.
6. User entities are responsible for immediately notifying ACD of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

CONTROL ACIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

ADMINISTRATIVE SAFEGUARD		
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 policies and procedures are in place to guide personnel in the event of an incident. 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, as appropriate. An intrusion detection system (IDS) is in place to help mitigate the risk of malicious network activity. External penetration tests are performed on a monthly basis, and remedial actions are taken.
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. External penetration tests are performed on a monthly basis, and remedial actions are taken.
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.
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 Director of IT.

ADMINISTRATIVE SAFEGUARD		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
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.	Access control and role-based build procedures are in place to restrict access to systems that maintain ePHI to only authorized personnel. The IT Supervisor performs access reviews monthly. Administrative access to the network is restricted to authorized personnel only.
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.	Authorization and/or supervision procedures are in place regarding workforce members who work with ePHI or in locations where it might be accessed. Standardized user access request forms are utilized to request access to ePHI. Access must be approved by executive personnel to access being granted.
164.308 (a)(3)(ii) (B)	**Workforce clearance procedure:** Access of a workforce member (employee or computing device) to ePHI is appropriate.	Workforce members have appropriate access to ePHI. Access control and role-based build procedures are in place to restrict access to systems that maintain ePHI to only authorized personnel. The IT Supervisor performs access reviews monthly.
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.	Termination procedures require the removal of employee access to ePHI upon termination of employment. Access to ePHI is revoked as a component of the termination process.
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.

ADMINISTRATIVE SAFEGUARD		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.308 (a)(4)(ii) (B)	**Access authorization:** Implement policies and procedures for granting access to ePHI, for example, through access to a workstation, transaction, program, process, or other mechanism.	Access control and role-based build procedures are in place to restrict access to systems that maintain ePHI to only authorized personnel. Standardized user access request forms are utilized to request access to ePHI. Access must be approved by executive personnel to access being granted.
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. Standardized user access request forms are utilized to request access to ePHI. Access must be approved by executive personnel to access being granted. Access to ePHI is revoked as a component of the termination process. The IT Supervisor performs access reviews monthly.
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. New hires are required to read and acknowledge the employee handbook, including information security guidelines and requirements for employees, upon hire.
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. A central antivirus server is configured with antivirus software to protected servers and workstations with the following configurations: • Scan for updates to antivirus definitions on a daily basis • Scan servers and workstations on a daily basis • An IDS is in place to help mitigate the risk of malicious network activity

ADMINISTRATIVE SAFEGUARD		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
164.308 (a)(5)(ii) (C)	**Log-in monitoring:** Procedures for monitoring log-in attempts and reporting discrepancies.	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. Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.
164.308 (a)(5)(ii) (D)	**Password management:** Procedures for creating, changing, and safeguarding passwords.	Policies are in place to guide personnel in creating, changing, and safeguarding passwords for network devices and servers. Network users are authenticated via individually-assigned user account and passwords. Networks that contain ePHI are configured to enforce the following user account and password controls via account policies inherited from active directory: • History (password reuse) • Minimum age • Maximum age • Minimum length • Complexity
164.308 (a)(6)(i)	**Security incident procedures:** Implement policies and procedures to address security incidents. Policies and procedures should include response reporting.	Documented incident response policies and procedures are in place to guide personnel in the event of an incident. Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.
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.	Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.
164.308 (a)(7)(i)	**Contingency plan:** Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain ePHI.	A documented business continuity plan is in place to guide personnel in the event of an emergency. The business continuity plan is tested annually.
164.308 (a)(7)(ii) (A)	**Data backup plan:** Establish and implement procedures to create and maintain retrievable exact copies of ePHI.	Documented backup policy and procedure documentation is in place to guide personnel in performing backups of critical ePHI.

ADMINISTRATIVE SAFEGUARD		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
		Backups are performed on the entity network, including shared drives containing application data, patient information, financial data, and crucial system information as follows: • Daily Full backups • Incremental backups - every 4 hours
164.308 (a)(7)(ii) (B)	**Disaster recovery plan:** Establish (and implement as needed) procedures to restore any loss of data.	A documented business continuity plan is in place to guide personnel in the event of an emergency. The business continuity plan is tested annually.
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.	An established emergency mode operations plan that guides personnel in the implementation of procedures to enable the continuation of critical business processes for the protection of ePHI is in place. A documented business continuity plan is in place to guide personnel in the event of an emergency. The business continuity plan is tested annually.
164.308 (a)(7)(ii) (D)	**Testing and revision procedures:** Implement procedures for periodic testing and revision of contingency plans.	A documented policy on the testing and revision of the business resumption plan and procedure is in place. The business continuity plan is tested annually.
164.308 (a)(7)(ii) (E)	**Applications and data criticality analysis:** Assess the relative criticality of specific applications and data in support of another contingency plan component.	The entity maintains a policy to assess the relative criticality of all data, so that such data may be properly protected during emergencies and during normal business operations. 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)(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.	Management evaluates the emergency and contingency plan and procedures, as needed. A documented policy on the testing and revision of the business resumption plan and procedure is in place. The business continuity plan is tested annually.

ADMINISTRATIVE SAFEGUARD		
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 SAFEGUARD		
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.	Documented physical security policies and procedures are in place to guide personnel in physical security practices. Physical keys to the office location are assigned to appropriate personnel and logged. Additional controls related to this criterion are the responsibility of the subservice organizations. Refer to the Subservice Organizations section for further details.
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.	Procedures that allow personnel access in support of restoration of lost data are in place. Additional controls related to this criterion are the responsibility of the subservice organizations. Refer to the Subservice Organizations section for further details.
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.	Documented physical security policies and procedures are in place to guide personnel in physical security practices.
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.	A role based security process has been defined with an access control system that is required to use roles when possible. Assets are assigned owners who are responsible for evaluating the appropriateness of access based on job roles. Additional controls related to this criterion are the responsibility of the subservice organizations. Refer to the Subservice Organizations section for further details.
164.310 (a)(2)(iv)	**Maintenance records:** Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).	Policies and procedures that require the documentation of repairs and modifications to the physical components of a facility are in place. Facility security maintenance records are created to document repairs and changes to physical elements of a facility related to security. Additional controls related to this criterion are the responsibility of the subservice organizations. Refer to the Subservice Organizations section for further details.

PHYSICAL SAFEGUARD		
Ref	**Regulation**	**Control Activity Specified by the Service 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.
164.310 (c)	**Workstation security:** Covered entities should implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.	Procedures are in place to implement physical safeguards for all workstations that access ePHI to restrict access to authorized users.
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 and maintained.
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.	Policy and procedure documents that address the final disposition of ePHI require that all ePHI-related media disposal be fully documented. Media is disposed of when deemed unusable. Digital media is deleted using methods that prevent recovery.
164.310 (d)(2)(ii)	**Media re-use:** Implement procedures for removal of ePHI from electronic media before the media are made available for re-use. Ensure that ePHI previously stored on electronic media cannot be accessed and reused. Identify removable media and their use. Ensure that ePHI is removed from reusable media before they are used to record new information.	The entity relinquishes media containing ePHI to a third-party vendor for sanitization when the asset is deemed no longer useable.
164.310 (d)(2)(iii)	**Accountability:** Maintain a record of the movements of electronic media and any person responsible therefore.	Maintenance records of the movements of electronic media are documented and maintained.
164.310 (d)(2)(iv)	**Data backup and storage:** Create a retrievable, exact copy of ePHI, when needed, before movement of equipment.	Documented backup policy and procedure documentation is in place to guide personnel in performing backups of critical ePHI. Backups are performed on the entity network, including shared drives containing application data, patient information, financial data, and crucial system information as follows: • Daily Full backups • Incremental backups - every 4 hours

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.	The entity creates and implements appropriate policies and procedures as required by law and as suggested by good business practices and general business ethics. Policies and procedures are reviewed and updated, if necessary; distributed, or otherwise made available to personnel; and are regularly maintained and secured.
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.	Officers, agents, employees, contractors, temporary workers, and volunteers who work for or perform any services (paid or unpaid) for the entity are obligated to document required activities. Documentation is created and maintained in written and electronic form. Actions, activities, or assessments that arise from HIPAA related events are documented.
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.	Documentation is distributed or made otherwise available to all affected workforce members.

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.	Documentation is reviewed annually and updated as needed in response to environmental or operation changes affecting the privacy or security of individually identifiable health information.

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.	**Not applicable** - The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (a)	A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used or disclosed as a result of such breach.	**Not applicable** - The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (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.
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.

BREACH NOTIFICATION		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
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.
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.

BREACH NOTIFICATION		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
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.
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.

BREACH NOTIFICATION		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
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.	Breach notification letters or e-mails are developed and prepared to be used during a breach of ePHI. Notification procedures include: • Notice to parties alerting them to breaches "without unreasonable delay," but no later than 60 days after discovery of the breach • Notice to covered entities when breach is discovered • Notice to the secretary of Human Health Services (HHS) and prominent media outlets about breaches • Notice to next of kin about breaches involving parties who are deceased • Notices to include what happened, the details of the breached unsecure PHI, steps to help mitigate harm to the party, and the covered entity's response • Annual notice to the secretary of HHS 60 days before the end of the calendar year about unsecure PHI breaches involving fewer than 500 patient records
164.410 (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.

BREACH NOTIFICATION		
Ref	**Regulation**	**Control Activity Specified by the Service Organization**
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.
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 ACD was limited to the HIPAA/HITECH requirements and related control activities specified by the management of ACD and did not encompass all aspects of ACD's operations or operations at user entities. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) AT-C 105 and AT-C 205.

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;