360 ADVANCED

HIPAA SECURITY COMPLIANCE ASSESSMENT FOR PRINTING, MAILING, AND FULFILLMENT SERVICES

SHAPCO PRINTING, INC.

APRIL 30, 2018

SHAPCO PRINTING

SHAPCO PRINTING, INC.

Table of Contents

SECTION 1:

EXECUTIVE SUMMARY

EXECUTIVE SUMMARY

360 Advanced, Inc. ("360 Advanced") is pleased to submit this Health Insurance Portability and Accountability Act (HIPAA) Security Compliance Assessment Report for Shapco Printing, Inc. ("Shapco"). The services performed were an assessment of internal controls in place to satisfy the Omnibus Final Security Rule governing "protected health information" that the Department of Health and Human Services issued in January 2013. This compliance assessment involved understanding the Printing, Mailing, and Fulfillment Services provided by Shapco, and documenting and verifying the safeguards in place to meet the relevant aspects of the Omnibus final rule on behalf of covered entities who maintain health information within Shapco's software and facility.

This security compliance assessment included an analysis of the information technology (IT) processes and infrastructure, controls, policies, and procedures that affect the confidentiality, integrity, and availability of the information technology systems and data as they relate to Shapco's Printing, Mailing, and Fulfillment Services. In some cases, the HIPAA Rule did not apply to the services provided by Shapco and is noted as Not Applicable (N/A) in Section 6 (Testing Matrices) of this report.

Through a data collection process, review of pertinent security-related documentation, interviews with key personnel, walk-throughs of processes and procedures, and tests of controls, where applicable, the 360 Advanced assessors compiled the necessary data for the analysis and review. The results of the compliance assessment are detailed in Section 6 (Testing Matrices) and should be reviewed and interpreted by each covered entity to determine if the safeguards in place are sufficient to meet their unique HIPAA compliance needs.

Specifically, our procedures addressed each specification in the HIPAA Security Final Rule. The procedures applied were used to gain an understanding of the environment as it relates to the HIPAA Security Final Rule and to provide an independent assessment of the controls in place. Our review was not intended to provide an opinion regarding the design or operating effectiveness of the controls identified during this assessment. Rather, to present in an independent fashion the documented and verified controls in place at Shapco that relate to each HIPAA Security Final Rule requirement.

SECTION 2:

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

June 11, 2018

We have prepared the description of Shapco Printing, Inc.'s ("Shapco") Printing, Mailing, and Fulfillment Services for users of the services as of April 30, 2018 who have a sufficient understanding to consider the services, along with other information, including information about the controls implemented by Shapco that address the HIPAA Security Final Rule in regard to user entities' ePHI data. We confirm, to the best of our knowledge and belief, that

a. the description fairly presents the Printing, Mailing, and Fulfillment Services made available to users of the services as of April 30, 2018. The criteria we used in making this assertion were that the description

    i. presents how the processes, procedures and controls that support the services provided to users were designed and implemented to address the applicable safeguards defined within the HIPAA / HITECH Security Rule as they relate to our environment, including when applicable:

        1. the types of services provided
        2. the procedures, within both automated and manual systems, by which services are provided
        3. the control activities performed that address the applicable HIPAA Security Final Rule

    ii. does not omit or distort information relevant to the scope of the Printing, Mailing, and Fulfillment Services, while acknowledging that the description is presented to meet the common needs of a broad range of users of the system, and may not, therefore, include every aspect of the Printing, Mailing, and Fulfillment Services that each individual user of the services may consider important in its own particular environment.

b. the controls related to each HIPAA Security Final Rule stated in the description were suitably designed and placed in operation as of April 30, 2018 to satisfy the Security Final Rule. The criteria we used in making this assertion were that

    i. the controls identified that address each HIPAA Security Final Rule stated in the description have been identified by management

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

/s/ Shapco Printing, Inc.

Joel Shapiro – CEO / President

Paresh Patel – VP of Technologies

SECTION 3:

SCOPE, OBJECTIVES, AND COMPANY OVERVIEW

SCOPE AND OBJECTIVES

The HIPAA Security Compliance Assessment addressed Administrative, Technical, and Physical Safeguards, with primary focus on the Security Final Rule as they relate to Shapco's Printing, Mailing, and Fulfillment Services. More specifically:

- **Administrative Safeguards** security includes the overall security management process; assigned security responsibility, workforce security, information access management, security awareness and training, security incident procedures, contingency planning, evaluation, and business associate contracts or other arrangements
- **Technical Safeguards** security includes audit controls, integrity, personnel or entity authentication, and transmission security
- **Physical Safeguards** security includes facility access controls, workstation use, workstation security, as well as portable devices and media controls
- **Organizational Requirements** implement BAA contracts that comply with the security measures
- **Policies and Procedures and Documentation Requirements** implement reasonable and appropriate policies and procedures to comply with standards, implementation specifications, or other requirements

Geographically, the scope included an on-site assessment of Shapco's facility in Minneapolis, Minnesota the week of April 9, 2018.

COMPANY OVERVIEW AND PRINTING, MAILING, AND FULFILLMENT SERVICES

Shapco was founded in 1976 by the Shapiro family with the vision that a printing company could succeed by crafting rather than merely manufacturing a printed product. Since that time the company has grown to approximately 120 employees serving multiple industries and clients across North America. Shapco provides: conventional printing, digital printing, large format printing, books, packaging, annual reports, ultra-violet (UV), kitting, finishing and direct mailing. Shapco operates from its print facility located in Minneapolis, Minnesota which includes 80,000 square feet for dedicated printing activities and a 360 square foot data center.

Shapco's Printing, Mailing, and Fulfillment Services system includes for the following forms of service:

- **Prepress** – The ability for clients to upload files to Shapco's secure site or scan them using a high-resolution drum or flatbed scanner. Shapco prepares the client's files and sends the client a soft proof and a realistic proof from their system using real ink dyes.
- **Conventional** – Conventional printing services, as well as two eight-color, and one six-color UV presses allowing for the addition of coatings.
- **UV** – The two eight-color, and one six-color UV presses print UV inks on paper, plastic or other substrates up to 40 points thick.
- **Digital Printing**:
    - Variable data including tailored printing to include custom colors, photos or text to individuals in the mailing lists.
    - Point-of-purchase displays, booth graphics, decals, banners, outdoor signage on paper, vinyl or other substrates, accommodating 96 inch to 120 inch wide capability with multiple colors.
    - Direct mail capability to individuals or geographic areas on client mailing.

- **Finishing –** Cutting, folding, gluing, binding, assembling, and kiting print jobs.
- **Mailing and Fulfillment** – Managing clients' databases, sealing and metering pieces, and drop-shipping them.

SECTION 4:

METHODOLOGY

OVERVIEW

The methodology employed in conducting this HIPAA Security Compliance Assessment applied a structured approach to identify and evaluate the controls in place associated with the operations of the IT environment and the business operations environment.

Procedures Performed

360 Advanced assembled a team to perform the data collection and analysis for this project. Data collection and analysis for this project employed the following four distinct methods:

1. **Reviewing pertinent documentation –** 360 Advanced requested and received numerous documents relevant to IT security, enterprise networks, and business operations at Shapco. The information extracted from these documents was critical to the analysis of Shapco's IT security and business operations posture
2. **Interviewing key personnel –** 360 Advanced collected technical security and business process information through technical interviews and physical walk-throughs. Interviews were conducted with key staff members and executive management, which further served to identify physical and operational facets of the Shapco's security program. These interviews gathered information to ascertain existing security risks and controls for each identified component. These procedures involved inquiries of the following key personnel:
    - Paresh Patel – Vice President of Technologies
    - Rick Holtgrave – Controller
3. **Facility walk-through –** An escorted physical walkthrough of Shapco's facility was conducted by 360 Advanced to observe first-hand physical security, IT security, and the general business operations environment
4. **Test of controls –** 360 Advanced performed tests of controls, including sample testing, where applicable, to verify the controls were in place and operating as designed

Assumptions

Information provided to the 360 Advanced assessors was presumed to be accurate unless the interviewee indicated uncertainty in their answer in which case that is noted in the report.

Constraints

This report scope was limited to the information technology enterprise and Shapco's operations at their Minneapolis, Minnesota location, as they existed as of as of April 30, 2018.

The threats, risks, vulnerabilities and controls discussed in this report pertain to the previously identified location as they existed during the previously specified period of time. Changes made to the environment subsequent to that period of time may or may not be accurately reflected in this report.

No Shapco customer sites were visited and no customer information technology resources were assessed in the course of this assessment.

SECTION 5:

COMPLIANCE ABSTRACT

Regulatory Compliance

In general, compliance means conforming to a specification or policy, standard or law that has been clearly defined. There are a wide variety of these, including state laws which are often more stringent and preempt federal regulations, and Shapco must work to ensure that they are aware of and will or have taken steps to comply with applicable laws and regulations.

Within the context of this project, the assessment scope was predetermined to have a particular focus on compliance with the Omnibus Final Rule.

Security and Privacy

Security and Privacy are interlocking. Privacy is not possible unless Security is in place to protect the asset that is considered private. Without security, privacy is at risk. Controls are established to mitigate risk, sometimes lessening the prospect for threat materialization and eventual vulnerability exploit.

The most basic definition of privacy is the confidential safekeeping of information that would not be reasonably available to others unless 'they' had explicit access permission or met other specific access requirements. Complexity begins with defining which information needs protection, as private, sensitive, or protected information, as these can mean something different to everyone based on personal values, cultural norms, business context, and many other factors. For this reason, Shapco policies and supporting training in the handling of private information must be explicit and conveyed frequently and done so in a manner that validates individual understanding of this topic.

Of specific concern is information in aggregate, or data "enriched" with other data sources to create a more valuable information set. Legal requirements for data protection tend to be less intuition-based than what one expects; however, the privacy compliance landscape by itself is by no means simple. The majority of states now have enacted data protection laws, many of which contain different requirements and definitions of covered data. When Shapco handles data, it needs to know with a high-level of precision exactly what is required to comply with privacy and security, even to the extent of knowing what the requirements are of other states if working in or with them, or handling data in or through them, ensuring the handling of information meets privacy and security handling as well as notification requirements.

Electronic Protected Health Information

In general, patient health information that has been converted to, stored in, or transmitted by electronic media is deemed to be "ePHI" and as such is to be controlled and protected under the HIPAA Privacy and Security Rules.

The following are examples of technology used to convert PHI to ePHI:

- Personal Computers with their internal hard drives used at work, home, or traveling
- External portable hard drives, including iPods
- Magnetic tape or disks
- Removable storage devices such as USB memory sticks / keys, CDs, DVDs, and floppy diskettes
- PDA's, smartphones
- Electronic transmission includes data exchange (e.g., email or file transfer) via wireless, ethernet, modem, DSL or cable network connections

As technology progresses, any new devices for accessing, transmitting, or receiving ePHI electronically will be covered by the HIPAA Security Rule.

Protected Health Information

PHI is defined under HIPAA, as any information about health status, provision of health care, or payment for health care that can be linked to an individual. This is interpreted rather broadly and includes any part of a patient's medical record or payment history. The following types of information are considered to be PHI:

1. Names
2. All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocode, except for the initial three digits of a zip code, if according to the current publicly available data from the Bureau of the Census: (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000.
3. Dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older.
4. Phone numbers.
5. Fax numbers.
6. Electronic mail addresses.
7. Social Security numbers.
8. Medical record numbers.
9. Health plan beneficiary numbers.
10. Account numbers.
11. Certificate and license numbers.
12. Vehicle identifiers and serial numbers, including license plate numbers.
13. Device identifiers and serial numbers.
14. Related (personal) Web Universal Resource Locators (URLs).
15. Internet Protocol (IP) address numbers.
16. Biometric identifiers, including finger and voice prints as well as DNA.
17. Full face photographic images and any comparable images.
18. Any other unique identifying number, characteristic, or code (note this does not mean the unique code assigned by the investigator to code the data).

The handling of PHI within Shapco must follow HIPAA requirements, and must be stringently adhered to for compliance purposes. It should be noted that ePHI, the electronic form of PHI, is more difficult to manage than the printed copy form of this protected information.

HIPAA – Health Insurance Portability and Accountability Act

The HIPAA Administration Simplification provisions address the *security and privacy* of health data. The standards are meant to improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in the U.S. health care system.

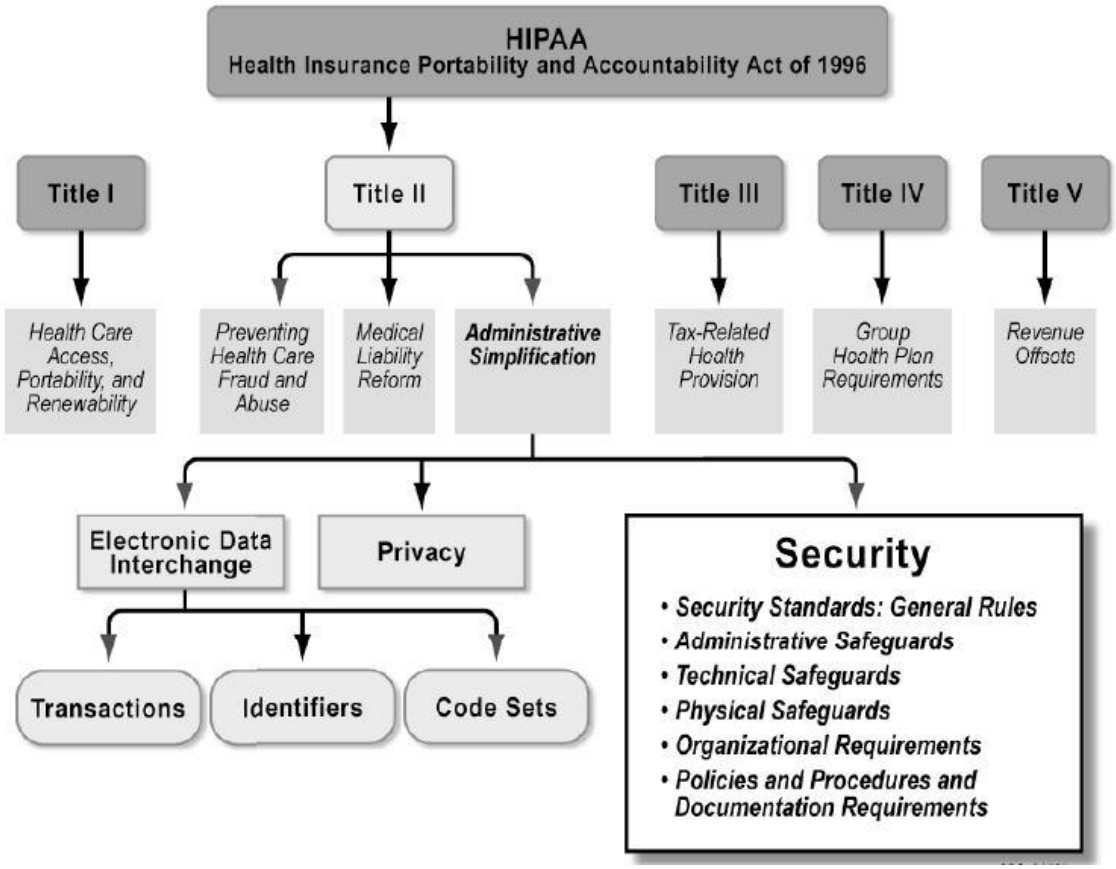
The HIPAA regulations apply to "covered entities" and "business associates" as defined by HIPAA. **Covered entities** include health plans, health care clearinghouses (such as billing services and community health information systems), and health care providers that engaged in electronic "standard transactions" that are regulated by HIPAA. A **Business associate** is a person or entity, other than a member of the workforce of a covered entity, who performs functions or activities on behalf of, or provides certain services to, a covered entity that involve access by the business associate to protected health information. A business associate also is a sub-contractor that creates, receives, maintains, or transmits protected health information on behalf of another business associate. The HIPAA Rules generally require that covered

entities and business associates enter into contracts with their business associates to ensure that the business associates will appropriately safeguard protected health information. The business associate contract also serves to clarify and limit, as appropriate, the permissible uses and disclosures of protected health information by the business associate, based on the relationship between the parties and the activities or services being performed by the business associate. A business associate is directly liable under the HIPAA rules and subject to civil and, in some cases, criminal penalties for making uses and disclosures of protected health information that are not authorized by its contract or required by law. A business associate also is directly liable and subject to civil penalties for failing to safeguard ePHI in accordance with the HIPAA Security Rule.

A written contract between a covered entity and a business associate must: (1) establish the permitted and required uses and disclosures of protected health information by the business associate; (2) provide that the business associate will not use or further disclose the information other than as permitted or required by the contract or as required by law; (3) require the business associate to implement appropriate safeguards to prevent unauthorized use or disclosure of the information, including implementing requirements of the HIPAA Security Rule with regard to electronic protected health information; (4) require the business associate to report to the covered entity any use or disclosure of the information not provided for by its contract, including incidents that constitute breaches of unsecured protected health information; (5) require the business associate to disclose protected health information as specified in its contract to satisfy a covered entity's obligation with respect to individuals' requests for copies of their protected health information, as well as make available protected health information for amendments (and incorporate any amendments, if required) and accountings; (6) to the extent the business associate is to carry out a covered entity's obligation under the Privacy Rule, require the business associate to comply with the requirements applicable to the obligation; (7) require the business associate to make available to HHS its internal practices, books, and records relating to the use and disclosure of protected health information received from, or created or received by the business associate on behalf of, the covered entity for purposes of HHS determining the covered entity's compliance with the HIPAA Privacy Rule; (8) at termination of the contract, if feasible, require the business associate to return or destroy all protected health information received from, or created or received by the business associate on behalf of, the covered entity; (9) require the business associate to ensure that any subcontractors it may engage on its behalf that will have access to protected health information agree to the same restrictions and conditions that apply to the business associate with respect to such information; and (10) authorize termination of the contract by the covered entity if the business associate violates a material term of the contract. Contracts between business associates and business associates that are subcontractors are subject to these same requirements.

Shapco may provide their customer's technical support and it is possible Shapco personnel would have access to their customer's data which may consist of electronic protected health information. As such, under the HIPAA Final Rule, Shapco is considered a business associate.

The figure below illustrates the structure of the HIPAA regulations. Note that the focus of this section is centered on the Security Rule requirements. The requirements for covered entities outlined on the following pages apply equally to Shapco as a business associate.



The Privacy Rule

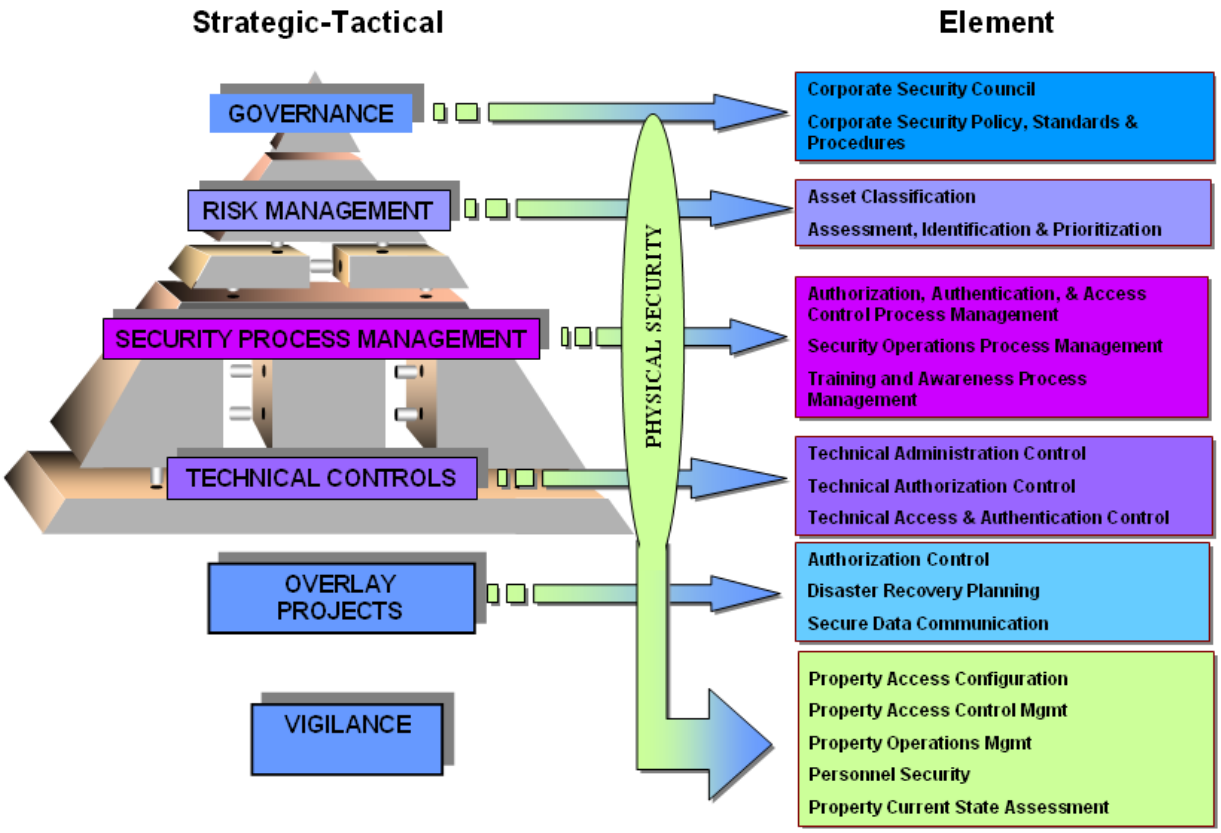
The Privacy Rule establishes regulations for the use and disclosure of Protected Health Information (PHI). PHI is discussed in this report and definitions are provided. Broadly interpreted, PHI includes any part of a patient's medical record or information regarding payment for health care. Because this report discusses Security Rule compliance, it does not analyze the requirements or compliance with the HIPAA Privacy Rule.

The Security Rule

The Security Rule complements the Privacy Rule. While the Privacy Rule pertains to all PHI including paper and electronic, the Security Rule deals specifically with ePHI.

The Security Rule specifies three types of security safeguards required for compliance: administrative, physical, and technical. For each of these types, the Rule identifies various security standards, and for each standard, it names both required **[R]** and addressable **[A]** implementation specifications.

An illustration of the HIPAA Security rule structure and its key attributes is as follows:



HIPAA Security Rule Illustration

Required specifications must be adopted and administered as specifically dictated by the Rule.

Addressable specifications are more flexible. Individual covered entities and business associates can evaluate their own situation and determine the best way to implement addressable specifications.

The standards and specifications are as follows:

Administrative Safeguards

This consists of policies and procedures designed to clearly show how the entity will comply with the Act. Covered entities (entities that must comply with the HIPAA requirements), must adopt a written set of privacy procedures and designate a privacy officer to be responsible for developing and implementing all required policies and procedures. The policies and procedures must reference management oversight and demonstrate organizational buy-in to compliance with the documented security controls.

Procedures should clearly identify employees or classes of employees who will have access to ePHI. Access to ePHI must be restricted to only those employees who have a need for it to complete their designated job function. The procedures must address access authorization, establishment, modification, and termination. Entities must show that an appropriate ongoing training program regarding the handling of ePHI is provided to employees performing health plan administrative functions.

Covered entities that out-source some of their business processes to a third party must ensure that their vendors also have a framework in place to comply with HIPAA requirements. Companies typically gain this assurance through clauses in the contracts stating that the vendor will meet the same data protection requirements that apply to the covered entity. Care must be taken to determine if the vendor further out-

sources any data handling functions to other vendors and monitor whether appropriate contracts and controls are in place.

A contingency plan needs to be in place for responding to emergencies. Covered entities are responsible for backing up their data and having disaster recovery procedures in place. The plan should document data priority and failure analysis, testing activities, and change control procedures.

Internal audits play a key role in HIPAA compliance by reviewing operations with the goal of identifying potential security violations. Policies and procedures should specifically document the scope, frequency, and procedures of audits. Audits should be both routine and event-based.

Procedures should document instructions for addressing and responding to security breaches that are identified either during the audit or the normal course of operations.

Physical Safeguards

Controlling physical access to protect against inappropriate access to protected data is required.

Controls must govern the introduction and removal of hardware and software from the network. (When equipment is retired it must be disposed of properly to ensure that PHI is not compromised.) Access to equipment containing health information should be carefully controlled and monitored. Access to hardware and software must be limited to properly authorized individuals. Required access controls consist of facility security plans, maintenance records, and visitor sign-in and escorts.

Policies are required to address proper workstation use. Workstations should be removed from high traffic areas and monitor screens should not be in direct view of the public. If the covered entities utilize contractors or agents, they too must be fully trained on their physical access responsibilities.

Technical Safeguards

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

Information systems housing PHI must be protected from intrusion. When information flows over open networks, some form of encryption must be utilized. If closed systems / networks are utilized, existing access controls are considered sufficient and encryption is optional.

Each covered entity is responsible for ensuring that the data within its systems has not been changed or erased in an unauthorized manner.

Data corroboration, including the use of check sum, double-keying, message authentication, and digital signature may be used to ensure data integrity.

Covered entities must also authenticate entities with whom it communicates. Authentication consists of corroborating that an entity is who it claims to be. Examples of corroboration include: password systems, two or three-way handshakes, telephone callback, and token systems.

Covered entities must make documentation of their HIPAA practices available to the government to determine compliance. In addition to policies and procedures and access records, information technology documentation should also include a written record of all configuration settings on the components of the network because these components are complex, configurable, and always changing.

Documented risk analysis and risk management programs are required. Covered entities must carefully consider the risks of their operations as they implement systems to comply with the regulations. (The requirement of risk analysis and risk management implies that the act's security requirements are a minimum standard and places responsibility on covered entities to take all reasonable precautions necessary to prevent PHI from being used for non-health purposes.)

Approach to Addressability for this Assessment

The tests of controls included in Section 6 of this report are based on a review of the applicable safeguards to protecting ePHI at Shapco's facility. The scope of the project undertaken did not include final determinations of addressability for each requirement / rule.

SECTION 6:

CONTROL DESCRIPTIONS AND TEST OF CONTROLS

Information Provided by the Assessor

Introduction

The purpose of this section is to identify controls implemented by Shapco to address the HIPAA requirements / rules as they relate to the services provided to entities by Shapco. It is not the intention of this assessment to determine if the controls implemented by Shapco management satisfy the requirement / rule. Each recipient of this assessment must determine if the controls implemented by Shapco are satisfactory to meet their own unique requirements as they relate to compliance with the HIPAA Security Final Rule.

360 Advanced recommends that each covered entity confer with its Senior Management, HIPAA Compliance Officer, and Legal Council on a regular basis to review and discuss HIPAA compliance and how to apply and interpret the HITECH Act's relevance and application to its business operations as they continue to change from the introduction of new services, hardware, software or the creation of new functional business units within the enterprise.

Types of Tests Performed

The table below describes the nature of our examination procedures and detailed in the matrices that follow:

Test Types	Description of Tests
Inquiry / Interview	Inquired of appropriate personnel seeking relevant information or representation to obtain the following information about the control: ➢ Knowledge and additional information regarding the policy or procedure ➢ Corroborating evidence of the policy or procedure
Inspection	Inspected documents and records indicating performance of the control. This includes, but is not limited to, the following: ➢ Examination / Inspection of source documentation and authorizations to verify transactions processed ➢ Examination / Inspection of documents or records for evidence of performance, such as existence of initials or signatures ➢ Examination / Inspection of systems documentation, configurations and settings ➢ Examination / Inspection of procedural documentation such as operations manuals, flow charts and job descriptions
Observation	Observed the implementation, application or existence of specific controls as represented

Testing Matrices

#	Control Identified / In Place	Testing Steps	Results of Testing
§164.308 Administrative Safeguards			
§164.308(a)(1)(i) Security Management Process: Implement policies and procedures to prevent, detect, contain, and correct security violations.			
§164.308(a)(1)(ii)(A) Risk Analysis [R]: Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.			
RA-1	Vulnerability scans of the Shapco network are performed at minimum quarterly. Results are reviewed by management and risks identified are mitigated as determined appropriate.	Inquired of the VP of Technologies to verify that vulnerability scans of the Shapco network were performed at minimum quarterly and results were reviewed by management and risks identified were mitigated as determined appropriate.	No relevant exceptions noted.
		Inspected the vulnerability scan results for a sample of quarters within the past 12 months to verify that vulnerability scans of the Shapco network were performed at minimum quarterly and results were reviewed by management and risks identified were mitigated as determined appropriate.	No relevant exceptions noted.
RA-2	Management maintains an inventory of the Shapco system components.	Inquired of the VP of Technologies to verify that management maintained an inventory the Shapco system components.	No relevant exceptions noted.
		Inspected the inventory listing to verify that management maintained an inventory of the Shapco system components.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
§164.308(a)(1)(ii)(B) Risk Management [R]: Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).			
RM-1	Policies and procedures regarding Security, Availability, and Confidentiality are documented and available to guide personnel.	Inquired of the Controller and VP of Technologies to verify that policies and procedures regarding Security, Availability, and Confidentiality were documented and available to guide personnel.	No relevant exceptions noted.
		Inspected the policies and procedures and their location on the company intranet to verify that policies and procedures regarding Security, Availability, and Confidentiality were documented and available to guide personnel.	No relevant exceptions noted.
RM-2	On a quarterly basis, security reminders are sent out and ongoing training is performed.	Inquired of the VP of Technologies to verify that on a quarterly basis, security reminders were sent out and ongoing training was performed.	No relevant exceptions noted.
		Inspected the security reminder emails sent out to employees for a sample of quarters within the past 12 months to verify that on a quarterly basis, security reminders were sent out and ongoing training was performed.	No relevant exceptions noted.
RM-3	Employees with credentials that allow access to systems are required to complete the company security training annually.	Inquired of the Controller to verify that employees with credentials that allowed access to systems were required to complete the company security training annually.	No relevant exceptions noted.
		Inspected the training completion results for a sample of active employees within the past 12 months to verify that employees with credentials that allowed access to systems were required to complete the company security training within the past 12 months.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
RM-4	Vulnerability scans of the Shapco network are performed at minimum quarterly. Results are reviewed by management and risks identified are mitigated as determined appropriate.	Inquired of the VP of Technologies to verify that vulnerability scans of the Shapco network were performed at minimum quarterly and results were reviewed by management and risks identified were mitigated as determined appropriate.	No relevant exceptions noted.
		Inspected the vulnerability scan results for a sample of quarters within the past 12 months to verify that vulnerability scans of the Shapco network were performed at minimum quarterly and results were reviewed by management and risks identified were mitigated as determined appropriate.	No relevant exceptions noted.
§164.308(a)(1)(ii)(C) Sanction Policy [R]: Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.			
SP-1	As part of the on-boarding process, new employees are required to sign to a statement indicating that they have read, understand, and will follow the Employee Handbook and the company policy and procedures.	Inquired of the Controller to verify that as part of the on-boarding process, new employees were required to sign to a statement indicating that they had read, understood, and would follow the Employee Handbook and the company policy and procedures.	No relevant exceptions noted.
		Inspected the signed employee handbook receipt / acknowledgment forms for a sample of employees on-boarded during the past 12 months to verify that as part of the on-boarding process, new employees were required to sign to a statement indicating that they had read, understood, and would follow the Employee Handbook and the company policy and procedures.	No relevant exceptions noted.
SP-2	Policies include suspension, restriction of access, and termination as potential sanctions for employee misconduct.	Inquired of the Controller to verify that policies included suspension, restriction of access, and termination as potential sanctions for employee misconduct.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
		Inspected the Shapco policies and procedures to verify that policies included suspension, restriction of access, and termination as potential sanctions for employee misconduct.	No relevant exceptions noted.
SP-3	Management obtains signatures from contractors indicating they have read and will adhere to Shapco Security Policies prior to access being provided.	Inquired of the Controller to verify that management obtained signatures from contractors indicating they had read and would adhere to Shapco Security Policies prior to access being provided.	No relevant exceptions noted.
		No tests of the control were performed because the circumstances that warranted the operation of the control did not occur during the past 12 months.	N/A
§164.308(a)(1)(ii)(D) Information System Activity Review [R]: Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.			
AR-1	IT management meets at minimum twice per month to discuss results of security events, scanning results, as well as to approve changes to the production network.	Inquired of the VP of Technologies to verify that IT management met at minimum twice per month to discuss results of security events, scanning results, as well as to approve changes to the production network.	No relevant exceptions noted.
		Inspected the Shapco Risk Assessment and Review Agenda and Minutes documentation for a sample of months within the past 12 months to verify that IT management met at minimum twice per month to discuss results of security events, scanning results, as well as to approve changes to the production network.	No relevant exceptions noted.
AR-2	Management has documented and maintains an Incident Response Policy on the company Intranet.	Inquired of the Controller to verify that management had documented and maintained an Incident Response Policy on the company Intranet.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
		Inspected the Incident Response Policy and its location on the company intranet to verify that management had documented and maintained an Incident Response Policy on the company intranet.	No relevant exceptions noted.
AR-3	Vulnerability scans of the Shapco network are performed at minimum quarterly. Results are reviewed by management and risks identified are mitigated as determined appropriate.	Inquired of the VP of Technologies to verify that vulnerability scans of the Shapco network were performed at minimum quarterly and results were reviewed by management and risks identified were mitigated as determined appropriate.	No relevant exceptions noted.
		Inspected the vulnerability scan results for a sample of quarters within the past 12 months to verify that vulnerability scans of the Shapco network were performed at minimum quarterly and results were reviewed by management and risks identified were mitigated as determined appropriate.	No relevant exceptions noted.
AR-4	Active Directory (AD) and Monarch are configured to log successful and unsuccessful login attempts.	Inquired of the VP of Technologies to verify that AD and Monarch were configured to log successful and unsuccessful login attempts.	No relevant exceptions noted.
		Inspected the Eventlog Analyzer to verify that AD and Monarch were configured to log successful and unsuccessful login attempts.	No relevant exceptions noted.
§164.308(a)(2) Assigned Security Responsibility [R]: Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the entity or business associate.			
SR-1	Management has assigned ownership of the policies and procedures to the various department leaders.	Inquired of the Controller to verify that management had assigned ownership of the policies and procedures to the various department leaders.	No relevant exceptions noted.
		Inspected the Shapco policies ownership document to verify that management had assigned ownership of the policies and procedures to the various department leaders.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
SR-2	Roles and responsibilities are defined in written job descriptions.	Inquired of the Controller to verify that roles and responsibilities were defined in written job descriptions.	No relevant exceptions noted.
		Inspected the documented job descriptions to verify that roles and responsibilities for key positions were defined in written job descriptions.	No relevant exceptions noted.
§164.308(a)(3)(i) Workforce Security: Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.			
§164.308(a)(3)(ii)(A) Authorization and / or Supervision [A]: Implement procedures for the authorization and / or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.			
AS-1	Access to the network requires a unique ID and password.	Inquired of the VP of Technologies to verify that access to the network required a unique ID and password.	No relevant exceptions noted.
		Inspected the AD user listing and network password policy to verify that access to the network required a unique ID and password.	No relevant exceptions noted.
AS-2	Logical and physical access privileges are approved by management during new hire employee on-boarding.	Inquired of the VP of Technologies to verify that logical and physical access privileges were approved by management during new hire employee on-boarding.	No relevant exceptions noted.
		Inspected the access forms for a sample of employees that were on-boarded during the past 12 months to verify that logical and physical access privileges were approved by management during new hire employee on-boarding.	No relevant exceptions noted.
AS-3	Administrative access to the network is restricted to members of the IT department.	Inquired of the VP of Technologies to verify that Administrative access to the network was restricted to members of the IT department.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
		Inspected the AD Domain Administrators user listing to verify that Administrative access to the network was restricted to members of the IT department.	No relevant exceptions noted.
AS-4	Access to the operating systems is restricted to the following users: ➢ VP of Technologies ➢ Contractor (2)	Inquired of the VP of Technologies to verify that access to the operating systems was restricted to the following personnel: ➢ VP of Technologies ➢ Contractor (2)	No relevant exceptions noted.
		Inspected the domain administrator user listing to verify that access to the operating systems was restricted to the following users: ➢ VP of Technologies ➢ Contractor (2)	No relevant exceptions noted.
AS-5	Access to the Monarch application requires a unique ID and password.	Inquired of the VP of Technologies to verify that access to the Monarch application required a unique ID and password.	No relevant exceptions noted.
		Inspected the Monarch user listing and password policy to verify that access to the Monarch application required a unique ID and password.	No relevant exceptions noted.
AS-6	Administrative access to the Monarch application is restricted to the following personnel: ➢ VP of Technologies ➢ Contractor (2)	Inquired of the VP of Technologies to verify that Administrative access to the Monarch application was restricted to the following personnel: ➢ VP of Technologies ➢ Contractor (2)	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
		Inspected the administrator user listing within the application to verify that administrative access to the Monarch application was restricted to the following personnel: ➢ VP of Technologies ➢ Contractor (2)	No relevant exceptions noted.
AS-7	Management has configured groups with role-based privileges within AD, Monarch, and the physical badge access system.	Inquired of the VP of Technologies to verify that Management had configured groups with role-based privileges within AD, Monarch, and the physical badge access system.	No relevant exceptions noted.
		Inspected AD, Monarch, and badge access systems to verify that Management had configured groups with role-based privileges within AD, Monarch, and the physical badge access system.	No relevant exceptions noted.
AS-8	Access to the production database is restricted to the Domain Administrators and requires the use of a unique ID and password.	Inquired of the VP of Technologies to verify that access to the production database was restricted to the Domain Administrators and required the use of a unique ID and password.	No relevant exceptions noted.
		Inspected the SQL user listing to verify that access to the production database was restricted to the Domain Administrators and required the use of a unique ID and password.	No relevant exceptions noted.
AS-9	Access to the internal network from outside of the facility is limited through VPN protocols configured to authenticate with the AD.	Inquired of the VP of Technologies to verify that access to the internal network from outside of the facility was limited through VPN protocols configured to authenticate with the AD.	No relevant exceptions noted.
		Inspected the VPN user access group within AD to verify that access to the internal network from outside of the facility was limited through VPN protocols configured to authenticate with the AD.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
§164.308(a)(3)(ii)(B) Workforce Clearance Procedure [A]: Implement procedures that determine that the access of a workforce member to electronic protected health information is appropriate.			
CP-1	Logical and physical access privileges are approved by management during new hire employee on-boarding.	Inquired of the VP of Technologies to verify that logical and physical access privileges were approved by management during new hire employee on-boarding.	No relevant exceptions noted.
		Inspected the access forms for a sample of employees that were on-boarded during the past 12 months to verify that logical and physical access privileges were approved by management during new hire employee on-boarding.	No relevant exceptions noted.
CP-2	Management performs criminal background checks on new employees prior to on-boarding.	Inquired of the Controller to verify that management performed criminal background checks on new employees prior to on-boarding.	No relevant exceptions noted.
		Inspected the results of background screenings performed for a sample of employees on-boarded during the past 12 months to verify that management performed criminal background checks on new employees prior to on-boarding.	No relevant exceptions noted.
CP-3	Administrative access to the network is restricted to members of the IT department.	Inquired of the VP of Technologies to verify that Administrative access to the network was restricted to members of the IT department.	No relevant exceptions noted.
		Inspected the AD Domain Administrators user listing to verify that Administrative access to the network was restricted to members of the IT department.	No relevant exceptions noted.
CP-4	Management has configured groups with role-based privileges within AD, Monarch, and the physical badge access system.	Inquired of the VP of Technologies to verify that Management had configured groups with role-based privileges within AD, Monarch, and the physical badge access system.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
		Inspected AD, Monarch, and badge access systems to verify that Management had configured groups with role-based privileges within AD, Monarch, and the physical badge access system.	No relevant exceptions noted.
§164.308(a)(3)(ii)(C) Termination Procedures [A]: Implement procedures for terminating access to electronic protected health information when the employment of a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.			
TP-1	Logical and physical access privileges are approved by management during new hire employee on-boarding.	Inquired of the VP of Technologies to verify that logical and physical access privileges were approved by management during new hire employee on-boarding.	No relevant exceptions noted.
		Inspected the access forms for a sample of employees that were on-boarded during the past 12 months to verify that logical and physical access privileges were approved by management during new hire employee on-boarding.	No relevant exceptions noted.
§164.308(a)(4)(i) Information Access Management: Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.			
§164.308(a)(4)(ii)(A) Isolating Health Care Clearinghouse Functions [R]: If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.			
N/A – Shapco is not a clearinghouse.			
§164.308(a)(4)(ii)(B) Access Authorization [A]: Implement policies and procedures for granting access to electronic protected health information, for example, through access to a work station, transaction, program, process, or other mechanism.			
AA-1	Access to the network requires a unique ID and password.	Inquired of the VP of Technologies to verify that access to the network required a unique ID and password.	No relevant exceptions noted.
		Inspected the AD user listing and network password policy to verify that access to the network required a unique ID and password.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
AA-2	Network authentication settings enforce password policies including: ➢ six character minimum passwords ➢ maximum password age 60 ➢ minimum password age 45 ➢ password history two ➢ complexity enabled ➢ storing passwords using reversible encryption is disabled ➢ five invalid logon attempts before lockout ➢ lockout duration 15 min	Inquired of the VP of Technologies to verify that network authentication settings enforced password policies including: ➢ six character minimum passwords ➢ maximum password age 60 ➢ minimum password age 45 ➢ password history two ➢ complexity enabled ➢ storing passwords using reversible encryption was disabled ➢ five invalid logon attempts before lockout ➢ lockout duration 15 min	No relevant exceptions noted.
		Inspected the AD policies to verify that network authentication settings enforced password policies including: ➢ six character minimum passwords ➢ maximum password age 60 ➢ minimum password age 45 ➢ password history two ➢ complexity enabled ➢ storing passwords using reversible encryption was disabled ➢ five invalid logon attempts before lockout ➢ lockout duration 15 min	No relevant exceptions noted.
AA-3	Logical and physical access privileges are approved by management during new hire employee on-boarding.	Inquired of the VP of Technologies to verify that logical and physical access privileges were approved by management during new hire employee on-boarding.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
		Inspected the access forms for a sample of employees that were on-boarded during the past 12 months to verify that logical and physical access privileges were approved by management during new hire employee on-boarding.	No relevant exceptions noted.
AA-4	Administrative access to the network is restricted to members of the IT department.	Inquired of the VP of Technologies to verify that Administrative access to the network was restricted to members of the IT department.	No relevant exceptions noted.
		Inspected the AD Domain Administrators user listing to verify that Administrative access to the network was restricted to members of the IT department.	No relevant exceptions noted.
AA-5	Logical and physical access assigned to terminated employees is deactivated, disabled, or assigned a new password at the time of termination.	Inquired of the VP of Technologies to verify that logical and physical access assigned to terminated employees was deactivated, disabled, or assigned a new password at the time of termination.	No relevant exceptions noted.
		Inspected the access forms and termination checklists for a sample of employees terminated within the past 12 months to verify that logical and physical access assigned to terminated employees was deactivated, disabled, or assigned a new password at the time of termination.	No relevant exceptions noted.
§164.308(a)(4)(ii)(C) Access Establishment and Modification [A]: Implement policies and procedures that, based upon the 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.			
AE-1	Access to the network requires a unique ID and password.	Inquired of the VP of Technologies to verify that access to the network required a unique ID and password.	No relevant exceptions noted.
		Inspected the AD user listing and network password policy to verify that access to the network required a unique ID and password.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
AE-2	Administrative access to the network is restricted to members of the IT department.	Inquired of the VP of Technologies to verify that Administrative access to the network was restricted to members of the IT department.	No relevant exceptions noted.
		Inspected the AD Domain Administrators user listing to verify that Administrative access to the network was restricted to members of the IT department.	No relevant exceptions noted.
AE-3	Logical and physical access assigned to terminated employees is deactivated, disabled, or assigned a new password at the time of termination.	Inquired of the VP of Technologies to verify that logical and physical access assigned to terminated employees was deactivated, disabled, or assigned a new password at the time of termination.	No relevant exceptions noted.
		Inspected the access forms and termination checklists for a sample of employees terminated within the past 12 months to verify that logical and physical access assigned to terminated employees was deactivated, disabled, or assigned a new password at the time of termination.	No relevant exceptions noted.
AE-4	Logical and physical access privileges are approved by management during new hire employee on-boarding.	Inquired of the VP of Technologies to verify that logical and physical access privileges were approved by management during new hire employee on-boarding.	No relevant exceptions noted.
		Inspected the access forms for a sample of employees that were on-boarded during the past 12 months to verify that logical and physical access privileges were approved by management during new hire employee on-boarding.	No relevant exceptions noted.
AE-5	Management has configured groups with role-based privileges within AD, Monarch, and the physical badge access system.	Inquired of the VP of Technologies to verify that Management had configured groups with role-based privileges within AD, Monarch, and the physical badge access system.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
		Inspected AD, Monarch, and badge access systems to verify that Management had configured groups with role-based privileges within AD, Monarch, and the physical badge access system.	No relevant exceptions noted.
§164.308(a)(5)(i) Security Awareness and Training: Implement a security awareness and training program for all members of its workforce (including management).			
§164.308(a)(5)(ii)(A) Security Reminders [A]: Periodic security updates.			
RM-1	Employees with credentials that allow access to systems are required to complete the company security training annually.	Inquired of the Controller to verify that employees with credentials that allowed access to systems were required to complete the company security training annually.	No relevant exceptions noted.
		Inspected the training completion results for a sample of active employees within the past 12 months to verify that employees with credentials that allowed access to systems were required to complete the company security training within the past 12 months.	No relevant exceptions noted.
RM-2	On a quarterly basis, security reminders are sent out and ongoing training is performed.	Inquired of the VP of Technologies to verify that on a quarterly basis, security reminders were sent out and ongoing training was performed.	No relevant exceptions noted.
		Inspected the security reminder emails sent out to employees for a sample of quarters within the past 12 months to verify that on a quarterly basis, security reminders were sent out and ongoing training was performed.	No relevant exceptions noted.
RM-3	A centralized anti-virus system is in place to monitor anti-virus installations and configurations on the production workstations and servers.	Inquired of the VP of Technologies to verify that a centralized anti-virus system was in place to monitor anti-virus installations and configurations on the production workstations and servers.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
		Inspected the Symantec Endpoint Protection Manager system and Cisco AMP system to verify that a centralized anti-virus system was in place to monitor anti-virus installations and configurations on the production workstations and servers.	No relevant exceptions noted.
§164.308(a)(5)(ii)(B) Protection from Malicious Software [A]: Procedures for guarding against, detecting, and reporting malicious software.			
MS-1	Vulnerability scans of the Shapco network are performed at minimum quarterly. Results are reviewed by management and risks identified are mitigated as determined appropriate.	Inquired of the VP of Technologies to verify that vulnerability scans of the Shapco network were performed at minimum quarterly and results were reviewed by management and risks identified were mitigated as determined appropriate.	No relevant exceptions noted.
		Inspected the vulnerability scan results for a sample of quarters within the past 12 months to verify that vulnerability scans of the Shapco network were performed at minimum quarterly and results were reviewed by management and risks identified were mitigated as determined appropriate.	No relevant exceptions noted.
MS-2	A centralized anti-virus system is in place to monitor anti-virus installations and configurations on the production workstations and servers.	Inquired of the VP of Technologies to verify that a centralized anti-virus system was in place to monitor anti-virus installations and configurations on the production workstations and servers.	No relevant exceptions noted.
		Inspected the Symantec Endpoint Protection Manager system and Cisco AMP system to verify that a centralized anti-virus system was in place to monitor anti-virus installations and configurations on the production workstations and servers.	No relevant exceptions noted.
MS-3	Firewalls are in place and configured to limit traffic to the internal network.	Inquired of the VP of Technologies to verify that firewalls were in place and configured to limit traffic to the internal network.	No relevant exceptions noted.
		Inspected the firewall access rules to verify that firewalls were in place and configured to limit traffic to the internal network.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
MS-4	Cisco AMP is installed and configured on production servers to mitigate damage of a successful penetration of the network.	Inquired of the VP of Technologies to verify that Cisco AMP was installed and configured on production servers to mitigate damage of a successful penetration of the network.	No relevant exceptions noted.
		Inspected Cisco AMP running on a production server to verify that Cisco AMP was installed and configured on production servers to mitigate damage of a successful penetration of the network.	No relevant exceptions noted.
MS-5	An Intrusion Protection System (IPS) is in place and is configured to block suspected intrusion attempts and send alerts to IT management.	Inquired of the VP of Technologies to verify that an IPS was in place and was configured to block suspected intrusion attempts and send alerts to IT management.	No relevant exceptions noted.
		Inspected the IPS configurations and an example alert sent to IT management to verify that an IPS was in place and was configured to block suspected intrusion attempts and send alerts to IT management.	No relevant exceptions noted.
MS-6	The monitoring tool is configured to monitor the health of the network and provide IT management with alerts when predefined thresholds are reached.	Inquired of the VP of Technologies to verify that the monitoring tool was configured to monitor the health of the network and provide IT management with alerts when predefined thresholds were reached.	No relevant exceptions noted.
		Inspected the monitoring dashboard, alert configurations, and an example of an alert notification email to verify that the monitoring tool was configured to monitor the health of the network and provide IT management with alerts when predefined thresholds were reached.	No relevant exceptions noted.
MS-7	Administrative access to the network is restricted to members of the IT department.	Inquired of the VP of Technologies to verify that Administrative access to the network was restricted to members of the IT department.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
		Inspected the AD Domain Administrators user listing to verify that Administrative access to the network was restricted to members of the IT department.	No relevant exceptions noted.
§164.308(a)(5)(ii)(C) Log-in Monitoring [A]: Procedures for monitoring log-in attempts and reporting discrepancies.			
LM-1	AD and Monarch are configured to log successful and unsuccessful login attempts.	Inquired of the VP of Technologies to verify that AD and Monarch were configured to log successful and unsuccessful login attempts.	No relevant exceptions noted.
		Inspected the Eventlog Analyzer to verify that AD and Monarch were configured to log successful and unsuccessful login attempts.	No relevant exceptions noted.
LM-2	A ticketing system is utilized to document and track incidents and systems change requests.	Inquired of the VP of Technologies to verify that a ticketing system was utilized to document and track incidents and systems change requests.	No relevant exceptions noted.
		Inspected the ticketing system to verify that a ticketing system utilized to document and track incidents and systems change requests.	No relevant exceptions noted.
§164.308(a)(5)(ii)(D) Password Management [A]: Procedures for creating, changing, and safeguarding passwords.			
PW-1	Access to the network requires a unique ID and password.	Inquired of the VP of Technologies to verify that access to the network required a unique ID and password.	No relevant exceptions noted.
		Inspected the AD user listing and network password policy to verify that access to the network required a unique ID and password.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
PW-2	Network authentication settings enforce password policies including: ➢ six character minimum passwords ➢ maximum password age 60 ➢ minimum password age 45 ➢ password history two ➢ complexity enabled ➢ storing passwords using reversible encryption is disabled ➢ five invalid logon attempts before lockout ➢ lockout duration 15 min	Inquired of the VP of Technologies to verify that network authentication settings enforced password policies including: ➢ six character minimum passwords ➢ maximum password age 60 ➢ minimum password age 45 ➢ password history two ➢ complexity enabled ➢ storing passwords using reversible encryption was disabled ➢ five invalid logon attempts before lockout ➢ lockout duration 15 min	No relevant exceptions noted.
		Inspected the AD policies to verify that network authentication settings enforced password policies including: ➢ six character minimum passwords ➢ maximum password age 60 ➢ minimum password age 45 ➢ password history two ➢ complexity enabled ➢ storing passwords using reversible encryption was disabled ➢ five invalid logon attempts before lockout ➢ lockout duration 15 min	No relevant exceptions noted.
§164.308(a)(6)(i) Security Incident Procedures: Implement policies and procedures to address security incidents.			
§164.308(a)(6)(ii) Response and Reporting [R]: 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.			
RR-1	Management has documented and maintains an Incident Response Policy on the company Intranet.	Inquired of the Controller to verify that management had documented and maintained an Incident Response Policy on the company Intranet.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
		Inspected the Incident Response Policy and its location on the company intranet to verify that management had documented and maintained an Incident Response Policy on the company intranet.	No relevant exceptions noted.
RR-2	Employees with credentials that allow access to systems are required to complete the company security training annually.	Inquired of the Controller to verify that employees with credentials that allowed access to systems were required to complete the company security training annually.	No relevant exceptions noted.
		Inspected the training completion results for a sample of active employees within the past 12 months to verify that employees with credentials that allowed access to systems were required to complete the company security training within the past 12 months.	No relevant exceptions noted.
RR-3	On a quarterly basis, security reminders are sent out and ongoing training is performed.	Inquired of the VP of Technologies to verify that on a quarterly basis, security reminders were sent out and ongoing training was performed.	No relevant exceptions noted.
		Inspected the security reminder emails sent out to employees for a sample of quarters within the past 12 months to verify that on a quarterly basis, security reminders were sent out and ongoing training was performed.	No relevant exceptions noted.
RR-4	A ticketing system is utilized to document and track incidents and systems change requests.	Inquired of the VP of Technologies to verify that a ticketing system was utilized to document and track incidents and systems change requests.	No relevant exceptions noted.
		Inspected the ticketing system to verify that a ticketing system utilized to document and track incidents and systems change requests.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
§164.308(a)(7)(i) Contingency Plan: Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example: fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.			
§164.308(a)(7)(ii)(A) Data Backup Plan [R]: Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.			
BU-1	Backup policies and procedures are documented and available to guide personnel in the backup process.	Inquired of the VP of Technologies to verify that backup policies and procedures were documented and available to guide personnel in the backup process.	No relevant exceptions noted.
		Inspected the backup policy and the Shapco intranet to verify that backup policies and procedures were documented and available to guide personnel in the backup process.	No relevant exceptions noted.
BU-2	The backup job schedulers are configured to perform daily backups.	Inquired of the VP of Technologies to verify that the backup job schedulers were configured to perform daily backups.	No relevant exceptions noted.
		Inspected the backup job scheduler to verify that the backup job schedulers were configured to perform daily backups.	No relevant exceptions noted.
BU-3	The backup system provides notification of success, failure, or warning as a result of the backups performed.	Inquired of the VP of Technologies to verify that the backup system provided notification of success, failure, or warning as a result of the backups performed.	No relevant exceptions noted.
		Inspected the backup notification configurations and an example backup notification email to verify that the backup system provided notification of success, failure, or warning as a result of the backups performed.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
BU-4	On an annual basis, IT management performs a full restoration test of a virtual environment.	Inquired of the VP of Technologies to verify that within the past 12 months, IT management performed a full restoration test of a virtual environment.	No relevant exceptions noted.
		Inspected an example of a backup restoration test to verify that within the past 12 months, IT management performed a full restoration test of a virtual environment.	No relevant exceptions noted.
§164.308(a)(7)(ii)(B) Disaster Recovery Plan [R]: Establish (and implement as needed) procedures to restore any loss of data.			
DP-1	On an annual basis, IT management performs a full restoration test of a virtual environment.	Inquired of the VP of Technologies to verify that within the past 12 months, IT management performed a full restoration test of a virtual environment.	No relevant exceptions noted.
		Inspected an example of a backup restoration test to verify that within the past 12 months, IT management performed a full restoration test of a virtual environment.	No relevant exceptions noted.
DP-2	A business continuity plan has been documented and is in place.	Inquired of the VP of Technologies to verify that a business continuity plan had been documented and was in place.	No relevant exceptions noted.
		Inspected the business continuity plan to verify that a business continuity plan had been documented and was in place.	No relevant exceptions noted.
DP-3	On an annual basis, Shapco management reviews and updates the business continuity plans.	Inquired of the VP of Technologies to verify that, on an annual basis, Shapco management reviewed and updated the business continuity plans.	No relevant exceptions noted.
		Inspected the Shapco business continuity plan to verify that within the past 12 months, Shapco management reviewed and updated the business continuity plans.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
§164.308(a)(7)(ii)(C) Emergency Mode Operation Plan [R]: Establish (and implement as needed) Procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.			
EP-1	On an annual basis, Shapco management reviews and updates the business continuity plans.	Inquired of the VP of Technologies to verify that, on an annual basis, Shapco management reviewed and updated the business continuity plans.	No relevant exceptions noted.
		Inspected the Shapco business continuity plan to verify that within the past 12 months, Shapco management reviewed and updated the business continuity plans.	No relevant exceptions noted.
EP-2	A business continuity plan has been documented and is in place.	Inquired of the VP of Technologies to verify that a business continuity plan had been documented and was in place.	No relevant exceptions noted.
		Inspected the business continuity plan to verify that a business continuity plan had been documented and was in place.	No relevant exceptions noted.
EP-3	A third-party vendor inspects the fire detection and suppression systems annually to verify that the fire detection and suppression systems are in proper working order.	Inquired of the VP of Technologies to verify that a third-party vendor inspected the fire detection and suppression systems annually to verify that the fire detection and suppression systems were in proper working order.	No relevant exceptions noted.
		Inspected the most recent third-party suppression system and fire extinguisher invoice to verify that a third-party vendor inspected the fire detection and suppression systems within the past 12 months to verify that the fire detection and suppression systems were in proper working order.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
EP-4	The data center is equipped with the following environmental protection systems: ➢ Dedicated / secondary cooling system ➢ Battery backup ➢ Smoke detectors ➢ Inergen fire suppression system	Inquired of the VP of Technologies to verify that the data center was equipped with the following environmental protection systems: ➢ Dedicated / secondary cooling system ➢ Battery backup ➢ Smoke detectors ➢ Inergen fire suppression system	No relevant exceptions noted.
		Observed the environmental systems identified within the control activity within the Shapco data center to verify that the data center was equipped with the following environmental protection systems: ➢ Dedicated / secondary cooling system ➢ Battery backup ➢ Smoke detectors ➢ Inergen fire suppression system	No relevant exceptions noted.
§164.308(a)(7)(ii)(D) Testing and Revision Procedures [A]: Implement procedures for periodic testing and revision of the contingency plans.			
RP-1	A business continuity plan has been documented and is in place.	Inquired of the VP of Technologies to verify that a business continuity plan had been documented and was in place.	No relevant exceptions noted.
		Inspected the business continuity plan to verify that a business continuity plan had been documented and was in place.	No relevant exceptions noted.
RP-2	On an annual basis, Shapco management reviews and updates the business continuity plans.	Inquired of the VP of Technologies to verify that, on an annual basis, Shapco management reviewed and updated the business continuity plans.	No relevant exceptions noted.
		Inspected the Shapco business continuity plan to verify that within the past 12 months, Shapco management reviewed and updated the business continuity plans.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
RP-3	On an annual basis, IT management performs a full restoration test of a virtual environment.	Inquired of the VP of Technologies to verify that within the past 12 months, IT management performed a full restoration test of a virtual environment.	No relevant exceptions noted.
		Inspected an example of a backup restoration test to verify that within the past 12 months, IT management performed a full restoration test of a virtual environment.	No relevant exceptions noted.
164.308(a)(7)(ii)(E) Applications and Data Criticality Analysis [A]: Assess the relative criticality of specific applications and data in support of other contingency plan components.			
AD-1	IT management meets at minimum twice per month to discuss results of security events, scanning results, as well as to approve changes to the production network.	Inquired of the VP of Technologies to verify that IT management met at minimum twice per month to discuss results of security events, scanning results, as well as to approve changes to the production network.	No relevant exceptions noted.
		Inspected the Shapco Risk Assessment and Review Agenda and Minutes documentation for a sample of months within the past 12 months to verify that IT management met at minimum twice per month to discuss results of security events, scanning results, as well as to approve changes to the production network.	No relevant exceptions noted.
§164.308(a)(8) Evaluation [R]: Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.			
EV-1	IT management meets at minimum twice per month to discuss results of security events, scanning results, as well as to approve changes to the production network.	Inquired of the VP of Technologies to verify that IT management met at minimum twice per month to discuss results of security events, scanning results, as well as to approve changes to the production network.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
		Inspected the Shapco Risk Assessment and Review Agenda and Minutes documentation for a sample of months within the past 12 months to verify that IT management met at minimum twice per month to discuss results of security events, scanning results, as well as to approve changes to the production network.	No relevant exceptions noted.
EV-2	Vulnerability scans of the Shapco network are performed at minimum quarterly. Results are reviewed by management and risks identified are mitigated as determined appropriate.	Inquired of the VP of Technologies to verify that vulnerability scans of the Shapco network were performed at minimum quarterly and results were reviewed by management and risks identified were mitigated as determined appropriate.	No relevant exceptions noted.
		Inspected the vulnerability scan results for a sample of quarters within the past 12 months to verify that vulnerability scans of the Shapco network were performed at minimum quarterly and results were reviewed by management and risks identified were mitigated as determined appropriate.	No relevant exceptions noted.
EV-3	Policies and procedures regarding Security, Availability, and Confidentiality are documented and available to guide personnel.	Inquired of the Controller and VP of Technologies to verify that policies and procedures regarding Security, Availability, and Confidentiality were documented and available to guide personnel.	No relevant exceptions noted.
		Inspected the policies and procedures and their location on the company intranet to verify that policies and procedures regarding Security, Availability, and Confidentiality were documented and available to guide personnel.	No relevant exceptions noted.
EV-4	Management maintains an inventory of the Shapco system components.	Inquired of the VP of Technologies to verify that management maintained an inventory the Shapco system components.	No relevant exceptions noted.
		Inspected the inventory listing to verify that management maintained an inventory of the Shapco system components.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
§164.308(b)(1) Business Associate Contracts and Other Arrangements [R]: A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with § 164.314(a) that the business associate will appropriately safeguard the information.			
§164.308(b)(3) Written Contract or Other Arrangement [R]: Document the satisfactory assurances required by paragraph (b)(1) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a).			
Shapco is not currently conducting business that would require BAAs. This will be required should Shapco begin conducting business involving HIPAA data.			
§164.310 Physical Safeguards			
§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.			
§164.310(a)(2)(i) Contingency Operations [A]: 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.			
CO-1	Access to the data center is restricted to the following personnel: ➢ VP of Technologies ➢ Pre-press Manager ➢ Pre-press Tech (2)	Inquired of the VP of Technologies to verify that access to the data center was restricted to the following personnel: ➢ VP of Technologies ➢ Pre-press Manager ➢ Pre-press Tech (2)	No relevant exceptions noted.
		Inspected badge system showing users with access to the data center to verify that access to the data center was restricted to the following personnel: ➢ VP of Technologies ➢ Pre-press Manager ➢ Pre-press Tech (2)	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
CO-2	Administrative access to the badge system is limited through a generic administrator account ID and password. Knowledge of the account credentials is limited to members of the IT team.	Inquired of the VP of Technologies to verify that administrative access to the badge system was limited through a generic administrator account ID and password and knowledge of the account credentials was limited to members of the IT team.	No relevant exceptions noted.
		Inspected physical badge access system listing the users with administrative access to verify that administrative access to the badge system was limited through a generic administrator account ID and password and knowledge of the account credentials was limited to members of the IT team.	No relevant exceptions noted.
CO-3	A business continuity plan has been documented and is in place.	Inquired of the VP of Technologies to verify that a business continuity plan had been documented and was in place.	No relevant exceptions noted.
		Inspected the business continuity plan to verify that a business continuity plan had been documented and was in place.	No relevant exceptions noted.
CO-4	On an annual basis, Shapco management reviews and updates the business continuity plans.	Inquired of the VP of Technologies to verify that, on an annual basis, Shapco management reviewed and updated the business continuity plans.	No relevant exceptions noted.
		Inspected the Shapco business continuity plan to verify that within the past 12 months, Shapco management reviewed and updated the business continuity plans.	No relevant exceptions noted.
§164.310(a)(2)(ii) Facility Security Plan [A]: Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.			
FS-1	Visitors are required to sign into a guest log, wear a visitor ID, and be escorted during onsite.	Inquired of the VP of Technologies and of the receptionist to verify that visitors were required to sign into a guest log, wear a visitor ID, and be escorted during onsite.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
		Observed the requirements to sign into a guest log, wear a badge, and be escorted during the onsite walk-throughs of the facility to verify that visitors were required to sign into a guest log, wear a visitor ID, and be escorted during onsite.	No relevant exceptions noted.
		Inspected the visitor logs for the past 12 months to verify that visitors were required to sign into a guest log.	No relevant exceptions noted.
FS-2	Perimeter doors are locked with the exception of the main entrance which is staffed during office hours. After hours, the main entrance is also locked.	Inquired of the VP of Technologies to verify that perimeter doors were locked with the exception of the main entrance which was staffed during office hours and after hours, the main entrance was also locked.	No relevant exceptions noted.
		Observed the perimeter doors during onsite walk-throughs to verify that perimeter doors were locked with the exception of the main entrance which was staffed during office hours and after hours, the main entrance was also locked.	No relevant exceptions noted.
FS-3	Video surveillance systems are in place throughout the facility, including the data center, and are configured to record and maintain footage for a minimum of 30 days.	Inquired of the VP of Technologies to verify that video surveillance systems were in place throughout the facility, including the data center, and were configured to record and maintain footage for a minimum of 30 days.	No relevant exceptions noted.
		Inspected the video surveillance system and footage to verify that video surveillance systems were in place throughout the facility, including the data center, and were configured to record and maintain footage for a minimum of 30 days.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
FS-4	Access to the data center is restricted to the following personnel: ➢ VP of Technologies ➢ Pre-press Manager ➢ Pre-press Tech (2)	Inquired of the VP of Technologies to verify that access to the data center was restricted to the following personnel: ➢ VP of Technologies ➢ Pre-press Manager ➢ Pre-press Tech (2)	No relevant exceptions noted.
		Inspected badge system showing users with access to the data center to verify that access to the data center was restricted to the following personnel: ➢ VP of Technologies ➢ Pre-press Manager ➢ Pre-press Tech (2)	No relevant exceptions noted.
FS-5	Administrative access to the badge system is limited through a generic administrator account ID and password. Knowledge of the account credentials is limited to members of the IT team.	Inquired of the VP of Technologies to verify that administrative access to the badge system was limited through a generic administrator account ID and password and knowledge of the account credentials was limited to members of the IT team.	No relevant exceptions noted.
		Inspected physical badge access system listing the users with administrative access to verify that administrative access to the badge system was limited through a generic administrator account ID and password and knowledge of the account credentials was limited to members of the IT team.	No relevant exceptions noted.
FS-6	The badge access system logs and maintains activity for 30 days prior to being backed up.	Inquired of the VP of Technologies to verify that the badge access system logged and maintained activity for 30 days prior to being backed up.	No relevant exceptions noted.
		Inspected the badge access system and example logs to verify that the badge access system logged and maintained activity for activity for 30 days prior to being backed up.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
§164.310(a)(2)(iii) Access Control and Validation Procedures [A]: 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.			
AC-1	Access to the network requires a unique ID and password.	Inquired of the VP of Technologies to verify that access to the network required a unique ID and password.	No relevant exceptions noted.
		Inspected the AD user listing and network password policy to verify that access to the network required a unique ID and password.	No relevant exceptions noted.
AC-2	Logical and physical access privileges are approved by management during new hire employee on-boarding.	Inquired of the VP of Technologies to verify that logical and physical access privileges were approved by management during new hire employee on-boarding.	No relevant exceptions noted.
		Inspected the access forms for a sample of employees that were on-boarded during the past 12 months to verify that logical and physical access privileges were approved by management during new hire employee on-boarding.	No relevant exceptions noted.
AC-3	Access to the data center is restricted to the following personnel: ➢ VP of Technologies ➢ Pre-press Manager ➢ Pre-press Tech (2)	Inquired of the VP of Technologies to verify that access to the data center was restricted to the following personnel: ➢ VP of Technologies ➢ Pre-press Manager ➢ Pre-press Tech (2)	No relevant exceptions noted.
		Inspected badge system showing users with access to the data center to verify that access to the data center was restricted to the following personnel: ➢ VP of Technologies ➢ Pre-press Manager ➢ Pre-press Tech (2)	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
AC-4	Visitors are required to sign into a guest log, wear a visitor ID, and be escorted during onsite.	Inquired of the VP of Technologies and of the receptionist to verify that visitors were required to sign into a guest log, wear a visitor ID, and be escorted during onsite.	No relevant exceptions noted.
		Observed the requirements to sign into a guest log, wear a badge, and be escorted during the onsite walk-throughs of the facility to verify that visitors were required to sign into a guest log, wear a visitor ID, and be escorted during onsite.	No relevant exceptions noted.
		Inspected the visitor logs for the past 12 months to verify that visitors were required to sign into a guest log.	No relevant exceptions noted.
AC-5	Administrative access to the badge system is limited through a generic administrator account ID and password. Knowledge of the account credentials is limited to members of the IT team.	Inquired of the VP of Technologies to verify that administrative access to the badge system was limited through a generic administrator account ID and password and knowledge of the account credentials was limited to members of the IT team.	No relevant exceptions noted.
		Inspected physical badge access system listing the users with administrative access to verify that administrative access to the badge system was limited through a generic administrator account ID and password and knowledge of the account credentials was limited to members of the IT team.	No relevant exceptions noted.
AC-6	Video surveillance systems are in place throughout the facility, including the data center, and are configured to record and maintain footage for a minimum of 30 days.	Inquired of the VP of Technologies to verify that video surveillance systems were in place throughout the facility, including the data center, and were configured to record and maintain footage for a minimum of 30 days.	No relevant exceptions noted.
		Inspected the video surveillance system and footage to verify that video surveillance systems were in place throughout the facility, including the data center, and were configured to record and maintain footage for a minimum of 30 days.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
AC-7	The badge access system logs and maintains activity for 30 days prior to being backed up.	Inquired of the VP of Technologies to verify that the badge access system logged and maintained activity for 30 days prior to being backed up.	No relevant exceptions noted.
		Inspected the badge access system and example logs to verify that the badge access system logged and maintained activity for activity for 30 days prior to being backed up.	No relevant exceptions noted.
§164.310(a)(2)(iv) Maintenance Records [A]: 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).			
MR-1	The data center is equipped with the following environmental protection systems: ➢ Dedicated / secondary cooling system ➢ Battery backup ➢ Smoke detectors ➢ Inergen fire suppression system	Inquired of the VP of Technologies to verify that the data center was equipped with the following environmental protection systems: ➢ Dedicated / secondary cooling system ➢ Battery backup ➢ Smoke detectors ➢ Inergen fire suppression system	No relevant exceptions noted.
		Observed the environmental systems identified within the control activity within the Shapco data center to verify that the data center was equipped with the following environmental protection systems: ➢ Dedicated / secondary cooling system ➢ Battery backup ➢ Smoke detectors ➢ Inergen fire suppression system	No relevant exceptions noted.
MR-2	A third-party vendor inspects the fire detection and suppression systems annually to verify that the fire detection and suppression systems are in proper working order.	Inquired of the VP of Technologies to verify that a third-party vendor inspected the fire detection and suppression systems annually to verify that the fire detection and suppression systems were in proper working order.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
		Inspected the most recent third-party suppression system and fire extinguisher invoice to verify that a third-party vendor inspected the fire detection and suppression systems within the past 12 months to verify that the fire detection and suppression systems were in proper working order.	No relevant exceptions noted.
MR-3	Management maintains an inventory of the Shapco system components.	Inquired of the VP of Technologies to verify that management maintained an inventory the Shapco system components.	No relevant exceptions noted.
		Inspected the inventory listing to verify that management maintained an inventory of the Shapco system components.	No relevant exceptions noted.
§164.310(b) Workstation Use [R]: Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.			
WU-1	Shapco maintains its Terms of Use and Privacy statements on the company website for external users.	Inquired of the Controller to verify that Shapco maintained its Terms of Use and Privacy statements on the company website for external users.	No relevant exceptions noted.
		Inspected the Terms of Use and Privacy statements on the company website to verify that Shapco maintained its Terms of Use and Privacy statements on the company website for external users.	No relevant exceptions noted.
WU-2	Access to the network requires a unique ID and password.	Inquired of the VP of Technologies to verify that access to the network required a unique ID and password.	No relevant exceptions noted.
		Inspected the AD user listing and network password policy to verify that access to the network required a unique ID and password.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
§164.310(c) Workstation Security [R]: Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.			
WS-1	The Windows screensaver is configured to be enabled after 15 minutes of inactivity.	Inquired of the VP of Technologies to verify that the windows screensaver was configured to be enabled after 15 minutes of inactivity.	No relevant exceptions noted.
		Inspected the screensaver configurations to verify that the windows screensaver was configured to be enabled after 15 minutes of inactivity.	No relevant exceptions noted.
WS-2	Visitors are required to sign into a guest log, wear a visitor ID, and be escorted during onsite.	Inquired of the VP of Technologies and of the receptionist to verify that visitors were required to sign into a guest log, wear a visitor ID, and be escorted during onsite.	No relevant exceptions noted.
		Observed the requirements to sign into a guest log, wear a badge, and be escorted during the onsite walk-throughs of the facility to verify that visitors were required to sign into a guest log, wear a visitor ID, and be escorted during onsite.	No relevant exceptions noted.
		Inspected the visitor logs for the past 12 months to verify that visitors were required to sign into a guest log.	No relevant exceptions noted.
WS-3	Perimeter doors are locked with the exception of the main entrance which is staffed during office hours. After hours, the main entrance is also locked.	Inquired of the VP of Technologies to verify that perimeter doors were locked with the exception of the main entrance which was staffed during office hours and after hours, the main entrance was also locked.	No relevant exceptions noted.
		Observed the perimeter doors during onsite walk-throughs to verify that perimeter doors were locked with the exception of the main entrance which was staffed during office hours and after hours, the main entrance was also locked.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
WS-4	Video surveillance systems are in place throughout the facility, including the data center, and are configured to record and maintain footage for a minimum of 30 days.	Inquired of the VP of Technologies to verify that video surveillance systems were in place throughout the facility, including the data center, and were configured to record and maintain footage for a minimum of 30 days.	No relevant exceptions noted.
		Inspected the video surveillance system and footage to verify that video surveillance systems were in place throughout the facility, including the data center, and were configured to record and maintain footage for a minimum of 30 days.	No relevant exceptions noted.
§164.310(d)(1) Device and Media Controls: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.			
§164.310(d)(2)(i) Disposal [R]: Implement policies and procedures to address the final disposition of electronic protected health information, and / or the hardware or electronic media on which it is stored.			
DS-1	The data retention policy outlines the retention periods and procedures for the protection of assets and covered information.	Inquired of the VP of Technologies to verify that the data retention policy outlined the retention periods and procedures for the protection of assets and covered information.	No relevant exceptions noted.
		Inspected the Retention Policy to verify that to verify that the data retention policy outlined the retention periods and procedures for the protection of assets and covered information.	No relevant exceptions noted.
DS-2	A third-party vendor is utilized to perform onsite shredding of documentation designated as confidential data after the retention period has expired.	Inquired of the VP of Technologies to verify that a third-party vendor was utilized to perform onsite shredding of documentation designated as confidential data after that retention period had expired.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
		Observed the shred bin located within the Shapco facility during onsite walkthroughs to verify that a third-party vendor was utilized to perform onsite shredding of documentation designated as confidential data after that retention period had expired.	No relevant exceptions noted.
DS-3	A Destruction Declaration is retained as evidence of the destruction of documentation.	Inquired of the VP of Technologies to verify that a destruction declaration was retained as evidence of the destruction of documentation.	No relevant exceptions noted.
		Inspected an example of a recent destruction declaration to verify that a destruction declaration was retained as evidence of the destruction of documentation.	No relevant exceptions noted.
§164.310(d)(2)(ii) Media Re-Use [R]: Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.			
RU-1	The data retention policy outlines the retention periods and procedures for the protection of assets and covered information.	Inquired of the VP of Technologies to verify that the data retention policy outlined the retention periods and procedures for the protection of assets and covered information.	No relevant exceptions noted.
		Inspected the Retention Policy to verify that to verify that the data retention policy outlined the retention periods and procedures for the protection of assets and covered information.	No relevant exceptions noted.
RU-2	A third-party vendor is utilized to perform onsite shredding of documentation designated as confidential data after the retention period has expired.	Inquired of the VP of Technologies to verify that a third-party vendor was utilized to perform onsite shredding of documentation designated as confidential data after that retention period had expired.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
		Observed the shred bin located within the Shapco facility during onsite walkthroughs to verify that a third-party vendor was utilized to perform onsite shredding of documentation designated as confidential data after that retention period had expired.	No relevant exceptions noted.
RU-3	A Destruction Declaration is retained as evidence of the destruction of documentation.	Inquired of the VP of Technologies to verify that a destruction declaration was retained as evidence of the destruction of documentation.	No relevant exceptions noted.
		Inspected an example of a recent destruction declaration to verify that a destruction declaration was retained as evidence of the destruction of documentation.	No relevant exceptions noted.
§164.310(d)(2)(iii) Accountability [A]: Maintain a record of the movements of hardware and electronic media and any person responsible therefore.			
AT-1	A third-party vendor is utilized to perform onsite shredding of documentation designated as confidential data after the retention period has expired.	Inquired of the VP of Technologies to verify that a third-party vendor was utilized to perform onsite shredding of documentation designated as confidential data after that retention period had expired.	No relevant exceptions noted.
		Observed the shred bin located within the Shapco facility during onsite walkthroughs to verify that a third-party vendor was utilized to perform onsite shredding of documentation designated as confidential data after that retention period had expired.	No relevant exceptions noted.
AT-2	A Destruction Declaration is retained as evidence of the destruction of documentation.	Inquired of the VP of Technologies to verify that a destruction declaration was retained as evidence of the destruction of documentation.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
		Inspected an example of a recent destruction declaration to verify that a destruction declaration was retained as evidence of the destruction of documentation.	No relevant exceptions noted.
AT-3	Access to the production database is restricted to the Domain Administrators and requires the use of a unique ID and password.	Inquired of the VP of Technologies to verify that access to the production database was restricted to the Domain Administrators and required the use of a unique ID and password.	No relevant exceptions noted.
		Inspected the SQL user listing to verify that access to the production database was restricted to the Domain Administrators and required the use of a unique ID and password.	No relevant exceptions noted.
§164.310(d)(2)(iv) Data Backup and Storage [A]: Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.			
DB-1	The backup job schedulers are configured to perform daily backups.	Inquired of the VP of Technologies to verify that the backup job schedulers were configured to perform daily backups.	No relevant exceptions noted.
		Inspected the backup job scheduler to verify that the backup job schedulers were configured to perform daily backups.	No relevant exceptions noted.
DB-2	The backup system provides notification of success, failure, or warning as a result of the backups performed.	Inquired of the VP of Technologies to verify that the backup system provided notification of success, failure, or warning as a result of the backups performed.	No relevant exceptions noted.
		Inspected the backup notification configurations and an example backup notification email to verify that the backup system provided notification of success, failure, or warning as a result of the backups performed.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
§164.312 Technical Safeguards			
§164.312(a)(1) Access Control: Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).			
§164.312(a)(2)(i) Unique User Identification [R]: Assign a unique name and / or number for identifying and tracking user identity.			
UI-1	Access to the network requires a unique ID and password.	Inquired of the VP of Technologies to verify that access to the network required a unique ID and password.	No relevant exceptions noted.
		Inspected the AD user listing and network password policy to verify that access to the network required a unique ID and password.	No relevant exceptions noted.
UI-2	AD and Monarch are configured to log successful and unsuccessful login attempts.	Inquired of the VP of Technologies to verify that AD and Monarch were configured to log successful and unsuccessful login attempts.	No relevant exceptions noted.
		Inspected the Eventlog Analyzer to verify that AD and Monarch were configured to log successful and unsuccessful login attempts.	No relevant exceptions noted.
UI-3	Access to the internal network from outside of the facility is limited through VPN protocols configured to authenticate with the AD.	Inquired of the VP of Technologies to verify that access to the internal network from outside of the facility was limited through VPN protocols configured to authenticate with the AD.	No relevant exceptions noted.
		Inspected the VPN user access group within AD to verify that access to the internal network from outside of the facility was limited through VPN protocols configured to authenticate with the AD.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
§164.312(a)(2)(ii) Emergency Access Procedure [R]: Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.			
EA-1	Policies related to change management practices are documented and maintained to ensure that security, availability, and confidentiality are considered when changes to the network are made.	Inquired of the VP of Technologies to verify that policies related to change management practices were documented and maintained to ensure that security, availability, and confidentiality were considered when changes to the network were made.	No relevant exceptions noted.
		Inspected the Network Hardening, Patch Management, and Software Installation policies to verify that policies related to change management practices were documented and maintained to ensure that security, availability, and confidentiality were considered when changes to the network were made.	No relevant exceptions noted.
EA-2	On an annual basis, IT management performs a full restoration test of a virtual environment.	Inquired of the VP of Technologies to verify that within the past 12 months, IT management performed a full restoration test of a virtual environment.	No relevant exceptions noted.
		Inspected an example of a backup restoration test to verify that within the past 12 months, IT management performed a full restoration test of a virtual environment.	No relevant exceptions noted.
EA-3	On an annual basis, Shapco management reviews and updates the business continuity plans.	Inquired of the VP of Technologies to verify that, on an annual basis, Shapco management reviewed and updated the business continuity plans.	No relevant exceptions noted.
		Inspected the Shapco business continuity plan to verify that within the past 12 months, Shapco management reviewed and updated the business continuity plans.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
§164.312(a)(2)(iii) Automatic Logoff [A]: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.			
AL-1	The Windows screensaver is configured to be enabled after 15 minutes of inactivity.	Inquired of the VP of Technologies to verify that the windows screensaver was configured to be enabled after 15 minutes of inactivity.	No relevant exceptions noted.
		Inspected the screensaver configurations to verify that the windows screensaver was configured to be enabled after 15 minutes of inactivity.	No relevant exceptions noted.
§164.312(a)(2)(iv) Encryption and Decryption [A]: Implement a mechanism to encrypt and decrypt electronic protected health information.			
ED-1	Access to the internal network from outside of the facility is limited through VPN protocols configured to authenticate with the AD.	Inquired of the VP of Technologies to verify that access to the internal network from outside of the facility was limited through VPN protocols configured to authenticate with the AD.	No relevant exceptions noted.
		Inspected the VPN user access group within AD to verify that access to the internal network from outside of the facility was limited through VPN protocols configured to authenticate with the AD.	No relevant exceptions noted.
ED-2	An SFTP site is configured and utilized by Shapco to provide options for secure uploading of customer information directly to Shapco.	Inquired of the VP of Technologies to verify that an SFTP site was configured and utilized by Shapco to provide options for secure uploading of customer information directly to Shapco.	No relevant exceptions noted.
		Inspected the configurations of the Secure FTP to verify that an SFTP site was configured and utilized by Shapco to provide options for secure uploading of customer information directly to Shapco.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
§164.312(b) Audit Controls [R]: Implement hardware, software, and / or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.			
AU-1	AD and Monarch are configured to log successful and unsuccessful login attempts.	Inquired of the VP of Technologies to verify that AD and Monarch were configured to log successful and unsuccessful login attempts.	No relevant exceptions noted.
		Inspected the Eventlog Analyzer to verify that AD and Monarch were configured to log successful and unsuccessful login attempts.	No relevant exceptions noted.
AU-2	The monitoring tool is configured to monitor the health of the network and provide IT management with alerts when predefined thresholds are reached.	Inquired of the VP of Technologies to verify that the monitoring tool was configured to monitor the health of the network and provide IT management with alerts when predefined thresholds were reached.	No relevant exceptions noted.
		Inspected the monitoring dashboard, alert configurations, and an example of an alert notification email to verify that the monitoring tool was configured to monitor the health of the network and provide IT management with alerts when predefined thresholds were reached.	No relevant exceptions noted.
§164.312(c)(1) Integrity: Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.			
§164.312(c)(2) Mechanism to Authenticate Electronic Protected Health Information [A]: Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.			
MA-1	Access to the production database is restricted to the Domain Administrators and requires the use of a unique ID and password.	Inquired of the VP of Technologies to verify that access to the production database was restricted to the Domain Administrators and required the use of a unique ID and password.	No relevant exceptions noted.
		Inspected the SQL user listing to verify that access to the production database was restricted to the Domain Administrators and required the use of a unique ID and password.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
MA-2	AD and Monarch are configured to log successful and unsuccessful login attempts.	Inquired of the VP of Technologies to verify that AD and Monarch were configured to log successful and unsuccessful login attempts.	No relevant exceptions noted.
		Inspected the Eventlog Analyzer to verify that AD and Monarch were configured to log successful and unsuccessful login attempts.	No relevant exceptions noted.
MA-3	The monitoring tool is configured to monitor the health of the network and provide IT management with alerts when predefined thresholds are reached.	Inquired of the VP of Technologies to verify that the monitoring tool was configured to monitor the health of the network and provide IT management with alerts when predefined thresholds were reached.	No relevant exceptions noted.
		Inspected the monitoring dashboard, alert configurations, and an example of an alert notification email to verify that the monitoring tool was configured to monitor the health of the network and provide IT management with alerts when predefined thresholds were reached.	No relevant exceptions noted.
§164.312(d) Person or Entity Authentication [R]: Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.			
PA-1	Access to the Monarch application requires a unique ID and password.	Inquired of the VP of Technologies to verify that access to the Monarch application required a unique ID and password.	No relevant exceptions noted.
		Inspected the Monarch user listing and password policy to verify that access to the Monarch application required a unique ID and password.	No relevant exceptions noted.
PA-2	Management has configured groups with role-based privileges within AD, Monarch, and the physical badge access system.	Inquired of the VP of Technologies to verify that Management had configured groups with role-based privileges within AD, Monarch, and the physical badge access system.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
		Inspected AD, Monarch, and badge access systems to verify that Management had configured groups with role-based privileges within AD, Monarch, and the physical badge access system.	No relevant exceptions noted.
PA-3	Access to the internal network from outside of the facility is limited through VPN protocols configured to authenticate with the AD.	Inquired of the VP of Technologies to verify that access to the internal network from outside of the facility was limited through VPN protocols configured to authenticate with the AD.	No relevant exceptions noted.
		Inspected the VPN user access group within AD to verify that access to the internal network from outside of the facility was limited through VPN protocols configured to authenticate with the AD.	No relevant exceptions noted.
§164.312(e)(1) Transmission Security: Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.			
§164.312(e)(2)(i) Integrity Controls [A]: Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.			
IC-1	An SFTP site is configured and utilized by Shapco to provide options for secure uploading of customer information directly to Shapco.	Inquired of the VP of Technologies to verify that an SFTP site was configured and utilized by Shapco to provide options for secure uploading of customer information directly to Shapco.	No relevant exceptions noted.
		Inspected the configurations of the Secure FTP to verify that an SFTP site was configured and utilized by Shapco to provide options for secure uploading of customer information directly to Shapco.	No relevant exceptions noted.
IC-2	Firewalls are in place and configured to limit traffic to the internal network.	Inquired of the VP of Technologies to verify that firewalls were in place and configured to limit traffic to the internal network.	No relevant exceptions noted.
		Inspected the firewall access rules to verify that firewalls were in place and configured to limit traffic to the internal network.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
IC-3	An IPS is in place and is configured to block suspected intrusion attempts and send alerts to IT management.	Inquired of the VP of Technologies to verify that an IPS was in place and was configured to block suspected intrusion attempts and send alerts to IT management.	No relevant exceptions noted.
		Inspected the IPS configurations and an example alert sent to IT management to verify that an IPS was in place and was configured to block suspected intrusion attempts and send alerts to IT management.	No relevant exceptions noted.
IC-4	Cisco AMP is installed and configured on production servers to mitigate damage of a successful penetration of the network.	Inquired of the VP of Technologies to verify that Cisco AMP was installed and configured on production servers to mitigate damage of a successful penetration of the network.	No relevant exceptions noted.
		Inspected Cisco AMP running on a production server to verify that Cisco AMP was installed and configured on production servers to mitigate damage of a successful penetration of the network.	No relevant exceptions noted.
§164.312(e)(2)(ii) Encryption [A]: Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.			
EN-1	On an annual basis, management reviews and updates the Software Installation Policy, the Data Classification Policy, and the Data Transmission Policy. These policies are maintained on the company intranet.	Inquired of the VP of Technologies to verify that within the past 12 months, management reviewed and updated the Software Installation Policy, the Data Classification Policy, and the Data Transmission Policy and these policies were maintained on the company intranet.	No relevant exceptions noted.
		Inspected the Software Installation Policy, the Data Classification Policy, and the Data Transmission Policy and their location on the intranet to verify that within the past 12 months, management reviewed and updated the Software Installation Policy, the Data Classification Policy, and the Data Transmission Policy and these policies were maintained on the company intranet.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
EN-2	Access to the internal network from outside of the facility is limited through VPN protocols configured to authenticate with the AD.	Inquired of the VP of Technologies to verify that access to the internal network from outside of the facility was limited through VPN protocols configured to authenticate with the AD.	No relevant exceptions noted.
		Inspected the VPN user access group within AD to verify that access to the internal network from outside of the facility was limited through VPN protocols configured to authenticate with the AD.	No relevant exceptions noted.
EN-3	An SFTP site is configured and utilized by Shapco to provide options for secure uploading of customer information directly to Shapco.	Inquired of the VP of Technologies to verify that an SFTP site was configured and utilized by Shapco to provide options for secure uploading of customer information directly to Shapco.	No relevant exceptions noted.
		Inspected the configurations of the Secure FTP to verify that an SFTP site was configured and utilized by Shapco to provide options for secure uploading of customer information directly to Shapco.	No relevant exceptions noted.
§164.314 Organizational Requirements			
§164.314(a)(1) Business Associate Contracts or Other Arrangements: The contract or other arrangement required by §164.308(b)(3) must meet the requirements of paragraph (a)(2)(i), (a)(2)(ii), or (a)(2)(iii) of this section, as applicable.			
§164.314(a)(2)(i) Business Associate Contracts [R]: The contract must provide that the business associate will: (A) Comply with the applicable requirements of this subpart (B) In accordance with §164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section (C) Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410			
N/A - Shapco is not currently conducting business that would require BAAs. This will be required should Shapco begin conducting business involving HIPAA data.			

#	Control Identified / In Place	Testing Steps	Results of Testing
§164.314(a)(2)(ii) Other Arrangements [R]: The covered entity is in compliance with paragraph (a)(1) of this section if it has another arrangement in place that meets the requirements of §164.504(e)(3).			
N/A - Shapco is not currently conducting business that would require BAAs. This will be required should Shapco begin conducting business involving HIPAA data.			
§164.314(a)(2)(iii) Business Associate Contracts with Subcontractors [R]: The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by §164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.			
N/A - Shapco is not currently conducting business that would require BAAs. This will be required should Shapco begin conducting business involving HIPAA data.			
§164.314(b)(1) Requirements for Group Health Plans: Except when the only electronic protected health information disclosed to a plan sponsor is disclosed pursuant to §164.504(f)(1)(ii) or (iii), or as authorized under §164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard electronic protected health information created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.			
§164.314(b)(2)(i) Plan Sponsor to Implement Safeguards [R]: The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits on behalf of the group health plan.			
N/A – Shapco does not maintain group health plans.			
§164.314(b)(2)(ii) Adequate Separation Between Group Health Plan and Plan Sponsor [R]: The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to ensure that the adequate separation required by §164.504(f)(2)(iii) is supported by reasonable and appropriate security measures.			
N/A – Shapco does not maintain group health plans.			
§164.314(b)(2)(iii) Security Measures for Plan Sponsor Agents [R]: The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information.			
N/A – Shapco does not maintain group health plans.			

#	Control Identified / In Place	Testing Steps	Results of Testing
§164.314(b)(2)(iv) Plan Sponsor to Report Security Incidents [R]: The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to report to the group health plan any security incident of which it becomes aware.			
N/A – Shapco does not maintain group health plans.			
§164.316 Policies and Procedures and Documentation Requirements			
§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). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.			
§164.316(b) Documentation: Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form.			
§164.316(b)(1)(i) Maintenance of Documentation [R]: Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form.			
MD-1	Shapco maintains its Terms of Use and Privacy statements on the company website for external users.	Inquired of the Controller to verify that Shapco maintained its Terms of Use and Privacy statements on the company website for external users.	No relevant exceptions noted.
		Inspected the Terms of Use and Privacy statements on the company website to verify that Shapco maintained its Terms of Use and Privacy statements on the company website for external users.	No relevant exceptions noted.
MD-2	Management maintains policy and procedure documents on the company intranet.	Inquired of the Controller to verify that management maintained policy and procedure documents on the company intranet.	No relevant exceptions noted.
		Inspected the policies and procedures and their location on the company intranet to verify that management maintained policy and procedure documents on the company intranet.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
MD-3	The data retention policy outlines the retention periods and procedures for the protection of assets and covered information.	Inquired of the VP of Technologies to verify that the data retention policy outlined the retention periods and procedures for the protection of assets and covered information.	No relevant exceptions noted.
		Inspected the Retention Policy to verify that to verify that the data retention policy outlined the retention periods and procedures for the protection of assets and covered information.	No relevant exceptions noted.
§164.316(b)(1)(ii) Documentation of Activities [R]: 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.			
DA-1	Visitors are required to sign into a guest log, wear a visitor ID, and be escorted during onsite.	Inquired of the VP of Technologies and of the receptionist to verify that visitors were required to sign into a guest log, wear a visitor ID, and be escorted during onsite.	No relevant exceptions noted.
		Observed the requirements to sign into a guest log, wear a badge, and be escorted during the onsite walk-throughs of the facility to verify that visitors were required to sign into a guest log, wear a visitor ID, and be escorted during onsite.	No relevant exceptions noted.
		Inspected the visitor logs for the past 12 months to verify that visitors were required to sign into a guest log.	No relevant exceptions noted.
DA-2	A third-party vendor is utilized to perform onsite shredding of documentation designated as confidential data after the retention period has expired.	Inquired of the VP of Technologies to verify that a third-party vendor was utilized to perform onsite shredding of documentation designated as confidential data after that retention period had expired.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
		Observed the shred bin located within the Shapco facility during onsite walkthroughs to verify that a third-party vendor was utilized to perform onsite shredding of documentation designated as confidential data after that retention period had expired.	No relevant exceptions noted.
DA-3	A Destruction Declaration is retained as evidence of the destruction of documentation.	Inquired of the VP of Technologies to verify that a destruction declaration was retained as evidence of the destruction of documentation.	No relevant exceptions noted.
		Inspected an example of a recent destruction declaration to verify that a destruction declaration was retained as evidence of the destruction of documentation.	No relevant exceptions noted.
§164.316(b)(2)(i) Time Limit of Documentation [R]: Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.			
TL-1	The data retention policy outlines the retention periods and procedures for the protection of assets and covered information.	Inquired of the VP of Technologies to verify that the data retention policy outlined the retention periods and procedures for the protection of assets and covered information.	No relevant exceptions noted.
		Inspected the Retention Policy to verify that to verify that the data retention policy outlined the retention periods and procedures for the protection of assets and covered information.	No relevant exceptions noted.
§164.316(b)(2)(ii) Availability of Documentation [R]: Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.			
DO-1	Management maintains policy and procedure documents on the company intranet.	Inquired of the Controller to verify that management maintained policy and procedure documents on the company intranet.	No relevant exceptions noted.

#	Control Identified / In Place	Testing Steps	Results of Testing
		Inspected the policies and procedures and their location on the company intranet to verify that management maintained policy and procedure documents on the company intranet.	No relevant exceptions noted.
§164.316(b)(2)(iii) Updates of Documentation [R]: Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.			
UP-1	IT management meets at minimum twice per month to discuss results of security events, scanning results, as well as to approve changes to the production network.	Inquired of the VP of Technologies to verify that IT management met at minimum twice per month to discuss results of security events, scanning results, as well as to approve changes to the production network.	No relevant exceptions noted.
		Inspected the Shapco Risk Assessment and Review Agenda and Minutes documentation for a sample of months within the past 12 months to verify that IT management met at minimum twice per month to discuss results of security events, scanning results, as well as to approve changes to the production network.	No relevant exceptions noted.