**COMPANY LOGO**

**Report on Controlcase INC's Description of its Example of a System Name’s system, and on the Suitability of the Design and Operating Effectiveness of its Controls Relevant to Security, Availability, and Confidentiality**

**System and Organization Controls – SOC 2 Type 2**

**Throughout the Period**

**January 1, 1999 to December 31, 1999**

A blue circle with black text

Description automatically generated

**TABLE OF CONTENTS**

[1. DESCRIPTION OF Controlcase INC CONTROL OBJECTIVES AND RELATED CONTROLS, AND INDEPENDENT SERVICE AUDITOR’S DESCRIPTION OF TEST OF CONTROLS AND RESULTS 4](#_Toc173247546)

[INTRODUCTION 4](#_Toc173247547)

[TRUST SERVICES CRITERIA FOR SECURITY-RELATED CONTROLS, AND TESTS OF CONTROLS 4](#_Toc173247548)

[DESCRIPTION OF CONTROL OBJECTIVES 4](#_Toc173247549)

[CC1.0 CONTROL ENVIRONMENT 4](#_Toc173247550)

[CC2.0 COMMUNICATION AND INFORMATION 9](#_Toc173247551)

[C1.0 ADDITIONAL CRITERIA FOR CONFIDENTIALITY 12](#_Toc173247552)

[A1.0 ADDITIONAL CRITERIA FOR AVAILABILITY 14](#_Toc173247553)

[ADDITIONAL CRITERIA FOR PRIVACY 16](#_Toc173247554)

|  |
| --- |
|  |

**SECTION 1**

**INDEPENDENT SERVICE AUDITOR’S REPORT**

**CPA LOGO**

# DESCRIPTION OF Controlcase INC CONTROL OBJECTIVES AND RELATED CONTROLS, AND INDEPENDENT SERVICE AUDITOR’S DESCRIPTION OF TEST OF CONTROLS AND RESULTS

## INTRODUCTION

FILLED1

## TRUST SERVICES CRITERIA FOR SECURITY-RELATED CONTROLS, AND TESTS OF CONTROLS

FILLED2

## DESCRIPTION OF CONTROL OBJECTIVES

### CC1.0 CONTROL ENVIRONMENT

| Criteria # | Description of Controlcase INC’s Controls | Tests Performed by Service Auditor | Results of Tests of Controls |
| --- | --- | --- | --- |
| CC1.1 COSO Principle 1 The entity demonstrates a commitment to integrity and ethical values. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| CC1.1.1 | Controlcase INC has an Organizational chart and job responsibilities that identifies reporting lines and indicates management levels within the hierarchy. This is NA. Controlcase INC has detailed job descriptions for all levels within their reporting lines. | Inspected the organizational chart from the Company to determine whether it describes functional areas and reporting structures within functional areas and whether reporting hierarchies were defined.  Inspected a sample of position descriptions from the Company and obtained job descriptions for the selected roles to confirm all criteria are defined. | No exceptions noted. |
| CC1.1.2 | Personnel must pass a background check before they may be hired. Background checks are performed for employees as a component of the hiring process and cleared before gaining access to any portions of the PHI/PII environment. | Inspected sample background checks to confirm personnel must pass a background check before they may be hired. | No exceptions noted. |
| CC1.1.3 | Sample has documented an Employee Handbook, which is reviewed, updated as-needed basis, and approved by Information Security Officer.  An employee handbook describes the minimum expected behavior of everyone. | Inspected the Employee Handbook to determine it included guidance regarding employee ethics and code of business conduct and was reviewed and communicated during the evaluation period.  Inspected a copy of the Employee Handbook to determine if it is provided to employees as part of the hiring process. | No exceptions noted. |
| CC1.1.4 | Controlcase INC has documented an Employee Handbook, which is reviewed, updated if applicable, and approved by Senior Management. | Controlcase INC has documented an Employee Handbook, which is reviewed, updated if applicable, and approved by Senior Management. | No exceptions noted. |
| CC1.1.5 | Personnel is required to read and accept the code of conduct. Policies and procedures require that employees sign an acknowledgment form, upon hire and at least annually, indicating that they have been given access to the employee manual and understand their responsibility for adhering to the code of conduct. | Inspected a sample of new hires employees to determine if they have read and accepted the Employee Handbook and signed the acknowledgment form upon hire, indicating that they have had access to the employee handbook and understand their responsibility to adhere to the code of conduct.  For a sample of employee records, inspected the annual signoff of the Controlcase INC Information Security Handbook to determine whether the criterion was met | No exceptions noted. |
| CC1.1.6 | Policies and procedures include disciplinary actions, which may result in termination for employees who are found to violate the Company's standards. Inspected the Employee Handbook to determine that a disciplinary process was in place. | Policies and procedures include disciplinary actions, which may result in termination for employees who are found to violate the Company's standards. Inspected the Employee Handbook to determine that a disciplinary process was in place. | No exceptions noted. |

| Criteria # | Description of Controlcase INC’s Controls | Tests Performed by Service Auditor | Results of Tests of Controls |
| --- | --- | --- | --- |
| CC1.2 COSO Principle 2 The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| CC1.2.1 | Controlcase INC has an Organizational chart and job responsibilities that identifies reporting lines and indicates management levels within the hierarchy.   Controlcase INC has detailed job descriptions for all levels within their reporting lines. | Inspected the organizational chart from the Company to determine whether it describes functional areas and reporting structures within functional areas and whether reporting hierarchies were defined.  Inspected a sample of position descriptions from the Company and obtained job descriptions for the selected roles to confirm all criteria are defined. | No exceptions noted. |
| CC1.2.2 | Employees must acknowledge its adherence to Policies and Procedures and Employee Handbook at least annually. | Employees must acknowledge its adherence to Policies and Procedures and Employee Handbook at least annually. | No exceptions noted. |
| CC1.2.3 | Policies and procedures have been prepared and available to employees via the Intranet. | Inspect all information security policies and procedures, and the evidence that demonstrates their periodic review. Policies are available to all users. | No exceptions noted. |
| CC1.2.4 | The Director of IT is responsible and accountable for developing and maintaining the Information Security Program, and changes and updates to the policies. | Inquired of Management to determine that the Director of IT is responsible and accountable for developing and maintaining the Information Security Program, and changes and updates to the policies. | No exceptions noted. |
| CC1.2.5 | Client agreements and statements of work that describe Controlcase INC's systems and its boundaries and responsibilities are provided to customers during the onboarding process. | Inspected Master Service Agreement to determine that Controlcase INC's systems and its boundaries and responsibilities are provided to customers during the onboarding process. | No exceptions noted. |
| CC1.2.6 | The Compliance department is responsible for implementing, documenting, and updating privacy policies. | Inquired of Management to Determine that the Compliance Specialist/ISMS Manager is responsible for documenting and updating Controlcase INC’s Privacy policies. | No exceptions noted. |

| Criteria # | Description of Controlcase INC’s Controls | Tests Performed by Service Auditor | Results of Tests of Controls |
| --- | --- | --- | --- |
| CC1.3 COSO Principle 3 Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in pursuit of objectives. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| CC1.3.1 | Controlcase INC has an Organizational chart and job responsibilities that identifies reporting lines and indicates management levels within the hierarchy.   Controlcase INC has detailed job descriptions for all levels within their reporting lines. | Inspected the organizational chart from the Company to determine whether it describes functional areas and reporting structures within functional areas and whether reporting hierarchies were defined.  Inspected a sample of position descriptions from the Company and obtained job descriptions for the selected roles to confirm all criteria are defined. | No exceptions noted. |
| CC1.3.2 | Management has established requirements for third-party vendors and service providers.  Agreements are established with third-party vendors and service providers, relevant to the System, that include clearly defined terms, conditions, and responsibilities. Responsibilities include confidentiality and privacy commitments as applicable. Agreements include clauses to terminate relationships when necessary. | Inspected agreements with third-party vendors and service providers to confirm the definition of terms, conditions, and responsibilities. A sample of contracts between Controlcase INC and some of its customers was inspected to determine that service level agreements are in place. | No exceptions noted. |

| Criteria # | Description of Controlcase INC’s Controls | Tests Performed by Service Auditor | Results of Tests of Controls |
| --- | --- | --- | --- |
| CC1.4 COSO Principle 4 The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| CC1.4.1 | Controlcase INC human resource policies and practices are written and communicated. Policies and procedures that are listed in the Employee Handbook include hiring, training, disciplinary actions, and termination procedures. | Inspected the policies and procedures to determine that they are written, and the employee handbook includes recruitment, hiring, employment, training, promotion, demotion, transfer, leaves of absence, compensation, and termination procedures. The procedures are supported by the Employee Handbook. | No exceptions noted. |
| CC1.4.2 | Each employee involved in the screening process is required to complete mandatory Security Training. | Inspected the training records of a sample of employees to determine whether the employees who participated in the screening process had received safety training. | No exceptions noted. |
| CC1.4.3 | Employees are required to complete security awareness training on an annual basis to understand their obligations and responsibilities to comply with the corporate and business unit security policies. | Inspected a sample of employee training records to determine that the annual training requirements were met. | No exceptions noted. |
| CC1.4.4 | Personnel must pass a background check before they may be hired. Background checks are performed for employees as a component of the hiring process and cleared before gaining access to any portions of the PHI/PII environment. | Inspected sample background checks to confirm personnel must pass a background check before they may be hired. | No exceptions noted. |
| CC1.4.5 | Management establishes personnel goals and encourages continued training as part of Controlcase INC's commitment to employees. Management monitors compliance with training requirements yearly. | Inspected the performance reviews to verify that Controlcase INC has established personnel goals and encourages continuous training and monitors compliance with training requirements annually. | No exceptions noted. |

| Criteria # | Description of Controlcase INC’s Controls | Tests Performed by Service Auditor | Results of Tests of Controls |
| --- | --- | --- | --- |
| CC1.5 COSO Principle 5 The entity holds individuals accountable for their internal control responsibilities in pursuit of objectives. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| CC1.5.1 | The responsibilities of individual process owners, as well as senior management, are described in the organization’s Policies and Procedures. | Inspected the Policies and Procedures to determine that responsibilities for individual process owners, as well as senior management, are described. | No exceptions noted. |
| CC1.5.2 | Policies and procedures include disciplinary actions, which may result in termination for employees who are found to violate the Company's standards. Inspected the Employee Handbook to determine that a disciplinary process was in place. | Policies and procedures include disciplinary actions, which may result in termination for employees who are found to violate the Company's standards. Inspected the Employee Handbook to determine that a disciplinary process was in place. | No exceptions noted. |
| CC1.5.3 | The Director of IT is responsible and accountable for developing and maintaining the Information Security Program, and changes and updates to the policies. | Inquired of Management to determine that the Director of IT is responsible and accountable for developing and maintaining the Information Security Program, and changes and updates to the policies. | No exceptions noted. |
| CC1.5.4 | Performance evaluations are in place to communicate and hold individuals accountable for the performance of internal control responsibilities. | For a sample of employees’ records inspected performance evaluations were performed. The reviews include appraisal, Company culture, performance metrics, goals, and core values review.  Performance reviews are conducted annually. | No exceptions noted. |

### CC2.0 COMMUNICATION AND INFORMATION

| Criteria # | Description of Controlcase INC’s Controls | Tests Performed by Service Auditor | Results of Tests of Controls |
| --- | --- | --- | --- |
| CC2.1 COSO Principle 13 The entity obtains or generates and uses relevant, quality information to support the functioning of internal control | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| CC2.1.1 | Dataflow diagrams are prepared and reviewed, identifying critical systems and sensitive information that explain the storage, processing, and transmission of covered information. | Inspected dataflow diagrams to determine that they identify critical systems and sensitive information relevant to the company's compliance with service commitments and system requirements. Data flows were updated annually. | No exceptions noted. |
| CC2.1.2 | Sample Management is responsible for monitoring vulnerabilities and vendors’ releases of patches and fixes and installing operational software updates, patches, and fixes on the operational systems. | Approved Vulnerability reports were inspected to confirm the execution of the scans as well as the remediation of the found vulnerabilities. | No exceptions noted. |
| CC2.1.3 | A third-party security specialist performs annual penetration tests of the production environment.  The Security Operations team reviews a penetration test report. | Inspected the annual penetration test report completed by a third-party security specialist and remediation of the found vulnerabilities. | No exceptions noted. |

| Criteria # | Description of Controlcase INC’s Controls | Tests Performed by Service Auditor | Results of Tests of Controls |
| --- | --- | --- | --- |
| CC2.2 COSO Principle 14 The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| CC2.2.1 | A system description is documented that includes the services provided, data, people, software, infrastructure, procedures, control environment, risk assessment, monitoring, and information and communication systems. The system description is communicated to authorized internal and external users. | Inspected network descriptions, process flow diagrams, and Information Security policies and procedures to determine whether they were made available to users of the system and the description addresses infrastructure, software, people, procedures, and data for the in-scope technology and locations. Determined that those were prepared and communicated to internal and external users to understand their responsibilities to comply with security and availability commitments. | No exceptions noted. |
| CC2.2.2 | Employees must acknowledge its adherence to Policies and Procedures and Employee Handbook at least annually. | Employees must acknowledge its adherence to Policies and Procedures and Employee Handbook at least annually. | No exceptions noted. |
| CC2.2.3 | Employees are required to complete security awareness training on an annual basis to understand their obligations and responsibilities to comply with the corporate and business unit security policies. | Inspected a sample of employee training records to determine that the annual training requirements were met. | No exceptions noted. |
| CC2.2.4 | Documented policies and procedures are in place to guide personnel in the entity's security, confidentiality, and privacy commitments and the associated system requirements. The policies and procedures are communicated to internal personnel via the Company's Intranet. | Inspected the list of Information Security policies, procedures, guidelines, and standards to determine whether those were prepared and communicated to internal and external users to understand their responsibilities to comply with security and availability commitments. | No exceptions noted |
| CC2.2.5 | Sample has a Security Breach Plan in place that includes an escalation plan based on the nature and severity of the incident to management, as necessary. | Inspected the Security Breach Plan to determine that a plan includes an incident response process and different levels of escalation per event category. | No exceptions noted. |
| CC2.2.6 | The entity's confidentiality commitments and requirements are documented in customer contracts. The contracts are updated, and a signature is obtained should the confidentiality practice change. | Inquired of Management to obtain an understanding of the management approval process for updates to confidentiality commitments and requirements. | No exceptions noted. |
| CC2.2.7 | Management has established requirements for third-party vendors and service providers.  Agreements are established with third-party vendors and service providers, relevant to the System, that include clearly defined terms, conditions, and responsibilities. Responsibilities include confidentiality and privacy commitments as applicable. Agreements include clauses to terminate relationships when necessary. | Inspected agreements with third-party vendors and service providers to confirm the definition of terms, conditions, and responsibilities.  A sample of contracts between Controlcase INC and some of its customers was inspected to determine that service level agreements are in place. | No exceptions noted. |

| Criteria # | Description of Controlcase INC’s Controls | Tests Performed by Service Auditor | Results of Tests of Controls |
| --- | --- | --- | --- |
| CC2.3 COSO Principle 15 The entity communicates with external parties regarding matters affecting the functioning of internal controls. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| CC2.3.1 | Client agreements and statements of work that describe Sample’s responsibilities are provided to customers during the onboarding process and acknowledge their confidentiality, access security, and security breach notification requirements. | A sample of customer agreements was inspected to determine whether customers are provided with responsibilities during the onboarding process and whether their requirements for confidentiality, access security, and security breach notification are recognized. | No exceptions noted. |
| CC2.3.2 | A system description is documented that includes the services provided, data, people, software, infrastructure, procedures, control environment, risk assessment, monitoring, and information and communication systems. The system description is communicated to authorized internal and external users. | Inspected network descriptions, process flow diagrams, and Information Security policies and procedures to determine whether they were made available to users of the system and the description addresses infrastructure, software, people, procedures, and data for the in-scope technology and locations. Determined that those were prepared and communicated to internal and external users to understand their responsibilities to comply with security and availability commitments. | No exceptions noted. |
| CC2.3.3 | External users are notified via email and news items on the Web portal. | Inquired of management to determine that Sample uses email alerts to communicate to internal and external users the changes and priority notifications and relevant information of systems. | No exceptions noted. |
| CC2.3.4 | Documented escalation procedures are in place to guide employees in reporting, acting upon, and resolving reported events. | Inspected the Security Breach Plan to determine whether security and availability commitments, as well as, significant processes, which include responsibility for reporting information security events and security weaknesses, incidents, system problems, concerns, and user complaints (and the process for doing so), are published and available to interested parties. | No exceptions noted. |
| CC2.3.5 | Controlcase INC management monitors compliance with training requirements. | Inspected a sample of employee training records to determine that the annual training requirements were met. | No exceptions noted. |

### C1.0 ADDITIONAL CRITERIA FOR CONFIDENTIALITY

| Criteria # | Description of Controlcase INC’s Controls | Tests Performed by Service Auditor | Results of Tests of Controls |
| --- | --- | --- | --- |
| C1.1 The entity identifies and maintains confidential information to meet the entity’s objectives related to confidentiality. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| C1.1.1 | Controlcase INC has a documented data retention policy and has processes in place to retain and dispose of information per those policies. | Inspected the Document and Records Control Policy (Document and Record Retention/ Document and Record Destruction) and inquired of Management to confirm that policies are in place to protect confidential information.    Inquired of Management to obtain an understanding of the data retention policies and procedures.    Inspected the Computer, Hardware, and Media Destruction Policy to confirm that guidelines are in place for the systematic destruction of computers, hardware, and media containing PII owned by Controlcase INC.    Inspected a sample of media destruction records to confirm the correct application of the defined policies. | No exceptions noted. |
| C1.1.2 | Remote access to the production systems is authenticated through VPN utilizing two-factor authentication. | two-factor authentication is performed using the DUO mobile application. Sample VPN must be set up with the preshared key for authentication on the at-home computer. | No exceptions noted |
| C1.1.3 | SAMPLE has established Data Classification and Asset Management policies to outline procedures for the protection of information assets. | Inspected the Information Security Policy to confirm that Data Classification and Asset Management procedures are in place for the protection of information assets. | No exceptions noted |
| C1.1.4 | Employees are required to sign the Eden Health Acceptable Use Agreement | Inspected attestation records for a sample of employees to confirm that employees are required to sign an Eden Health Acceptable Use Agreement upon being hired. | No exceptions noted. |

| Criteria # | Description of Controlcase INC’s Controls | Tests Performed by Service Auditor | Results of Tests of Controls |
| --- | --- | --- | --- |
| C1.2 The entity disposes of confidential information to meet the entity’s objectives related to confidentiality. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| C1.2.1 | Controlcase INC has a documented data retention policy and has processes in place to retain and dispose of information per those policies. | Inspected the Document and Records Control Policy (Document and Record Retention/ Document and Record Destruction) and inquired of Management to confirm that policies are in place to protect confidential information.    Inquired of Management to obtain an understanding of the data retention policies and procedures.    Inspected the Computer, Hardware, and Media Destruction Policy to confirm that guidelines are in place for the systematic destruction of computers, hardware, and media containing PII owned by Sample.    Inspected a sample of media destruction records to confirm the correct application of the defined policies. | No exceptions noted |

### A1.0 ADDITIONAL CRITERIA FOR AVAILABILITY

| Criteria # | Description of Controlcase INC’s Controls | Tests Performed by Service Auditor | Results of Tests of Controls |
| --- | --- | --- | --- |
| A1.1 The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| A1.1.1 | All critical systems, including servers, firewalls, routers, and network switches, have logging enabled. When a warning, error, or critical state occurs, the monitoring and logging server or system sends a notification to the appropriate personnel. Corrective action takes place based on the contents of the notification and the event is logged as an incident. | Inquired of management to confirm that all critical systems, including servers, firewalls, routers, and network switches, are verified to be logged in. Notifications sent to the appropriate personnel are verified. Corrective action is taken based on the contents of the notification.    Inquired of management to confirm that Sample is still using systems including Third-party (Intrusion Detection), Industry standard (antivirus), Logger (logic monitor/processing errors or issues) | No exceptions noted. |
| A1.1.2 | Monitoring software tools are used by the Technical Operations Team to monitor the security, availability, and performance of the Controlcase INC network | Logging and monitoring software capability was observed used to collect data from Controlcase INC system infrastructure components. The log management system checks performance, unauthorized software installation, potential security threats and vulnerabilities, resource utilization, and detects unusual system activity or service requests. | No exceptions noted. |
| A1.1.3 | A Capacity Management Plan is defined to ensure the proper operation of all systems within the environment. | Inspected drive space reports to confirm the organization monitors the use of resources (capacity) and makes changes to the environment as needed | No exceptions noted. |

| Criteria # | Description of Controlcase INC’s Controls | Tests Performed by Service Auditor | Results of Tests of Controls |
| --- | --- | --- | --- |
| A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| A1.2.1 | Backups of systems, applications, and network files are performed daily. | Inquired of management and inspected the screenshots to determine that the Backup of servers at Sample is performed using XYZ Recovery. Each server is backed up at least once per day. Each server has a base image of the entire system performed and then incremental until a new base image is required.    Separately, inquired of management to determine that Data is then replicated offsite daily. In both locations data is stored at rest in the data repository as well as a cold spare virtual machine. | No exceptions noted. |
| A1.2.2 | Servers and networking equipment are stored in a hosting facility that complies with security and availability requirements. | Inquired of management to confirm that environmental controls are in place and periodic maintenance is performed.    Invoice and reports of HVAC equipment, safety systems fire and alarm, server room, and generator report were observed. | No exceptions noted. |

| Criteria # | Description of Controlcase INC’s Controls | Tests Performed by Service Auditor | Results of Tests of Controls |
| --- | --- | --- | --- |
| A1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| A1.3.1 | Business continuity and disaster recovery plans, including restoration of backups, are tested annually. Test results are reviewed, and the contingency plan is adjusted. | Inspected Controlcase INC Disaster Recovery Plan to confirm that has been designed to address the following areas of Controlcase INC. 1. Facility 2. Technology 3. Documentation and Records 4. Crisis Communication Plan 5. Staffing This plan works congruently with Controlcase INC’s Information Security Management System (ISMS), ensuring the security and recovery of all data systems and PII maintained by Controlcase INC.    The plan is reviewed at least once a year and changes will be made as needed at that time.    Also, the Tabletop exercise was observed to confirm that Controlcase INC’s Disaster Recovery Plan is reviewed as part of its ISO 27001 certifications. The checklist guide through steps and suggestions to plan and facilitate a successful Mock Disaster Exercise. | No exceptions noted. |

### P1.0 ADDITIONAL CRITERIA FOR PRIVACY

| Criteria # | Description of Controlcase INC’s Controls | Tests Performed by Service Auditor | Results of Tests of Controls |
| --- | --- | --- | --- |
| P1.1 The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| P1.1 .1 | Controlcase INC provides notice to data subjects on the purpose, choice, and consent; types of information collected; methods of collection; use, retention, and disposal; access, complaints, and disputes; disclosure to third parties; security; quality, including data subjects' responsibilities; and monitoring and enforcement of personal information. | Inspected the Privacy Policy and HIPAA Privacy Policy to confirm that they clearly provide notice on the purpose; choice and consent; types of information collected; methods of collection; use, retention, and disposal; access, complaints, and disputes; disclosure to third parties; security; quality, including data subjects' responsibilities; and monitoring and enforcement of personal information. | No exceptions noted. |

| Criteria # | Description of Controlcase INC’s Controls | Tests Performed by Service Auditor | Results of Tests of Controls |
| --- | --- | --- | --- |
| P2.1 The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| P2.1 .1 | Controlcase INC has published policies on its website that provide notice on the purpose, choice and consent, collection, use and retention, access to, disclosure, security, and monitoring of personal information and PHI. | Inspected the Privacy Policy and HIPAA Privacy Policy to confirm that it provides notice on the purpose, choice and consent, collection, use and retention, access to, disclosure, security, and monitoring of personal information and PHI.    Inquired of management confirms that during the registration process, users must consent to the policies that govern data collection, retention, and the user’s options to obtain this information. | No exceptions noted. |
| P2.1 .2 | Controlcase INC obtains explicit consent directly from the data subject when collecting, using, or disclosing sensitive personal information unless a law or regulation specifically requires otherwise. | Inquired of Management to confirm that consent is obtained directly from the data subject when collecting, using, or disclosing sensitive personal information unless a law or regulation specifically requires otherwise.    Inspected a sample to the records to confirm that explicit consent is taken from individuals as the last step of registration (prior to data submission) with the three data usage and privacy policies.    • HIPAA Statement  • Privacy Policy  • Terms of service | No exceptions noted. |

| Criteria # | Description of Controlcase INC’s Controls | Tests Performed by Service Auditor | Results of Tests of Controls |
| --- | --- | --- | --- |
| P3.1 The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| P3.1.1 | Controlcase INC methods of collecting personal information are reviewed by management before they are implemented to confirm that personal information is obtained (a) fairly, without intimidation or deception, and (b) lawfully, adhering to all relevant rules of law, whether derived from statute or common law, relating to the collection of personal information. | Inquired of Management regarding Eden Health’s methods of collecting personal information and confirmed that personal information is obtained.    (a) fairly, without intimidation or deception, and (b) lawfully, adhering to all relevant law rules, whether derived from statute or common law, relating to collecting personal information.    Inspected the Privacy Policy to determine the collection process was in place.    Inquired with Technical Operations Manager confirms Eden Health collects personal information through their mobile patient app, Athena EHR, and customer data files. The data loads from customers are not modified in any way. The data owners enter the EHR data and the patient mobile app data directly. | No exceptions noted |
| P3.1.2 | Controlcase INC policy is that only the personal information required to provide the service is collected. | Inspected the privacy notices and privacy policies on the Eden Health public websites to confirm they specify that only the personal information required to complete the service is collected. | No exceptions noted |
| P3.1.3 | Controlcase INC provides notice to data subjects on the purpose, choice, and consent; types of information collected; methods of collection; use, retention, and disposal; access, complaints, and disputes; disclosure to third parties; security; quality, including data subjects' responsibilities; and monitoring and enforcement of personal information.    If personal information is collected from sources other than the individual, such sources are described in the privacy notice. | Inspected the Privacy Policy and HIPAA Privacy Policy to confirm that they clearly provide notice on the purpose; choice and consent; types of information collected; methods of collection; use, retention, and disposal; access, complaints, and disputes; disclosure to third parties; security; quality, including data subjects' responsibilities; and monitoring and enforcement of personal information.    Verified that if personal information is collected from sources other than the individual, such sources are described in the privacy notice. | No exceptions noted |

| Criteria # | Description of Controlcase INC’s Controls | Tests Performed by Service Auditor | Results of Tests of Controls |
| --- | --- | --- | --- |
| P3.2 The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| P3.2.1 | Controlcase INC obtains explicit consent directly from the data subject when collecting, using, or disclosing sensitive personal information unless a law or regulation specifically requires otherwise. | Inquired of Management to confirm that consent is obtained directly from the data subject when collecting, using, or disclosing sensitive personal information unless a law or regulation specifically requires otherwise.    Inspected a sample to the records to confirm that explicit consent is taken from individuals as the last step of registration (prior to data submission) with the three data usage and privacy policies.    • HIPAA Statement  • Privacy Policy  • Terms of service | No exceptions noted |
| P3.2.2 | Controlcase INC retains documentation of explicit consent in accordance with privacy-related purposes. | Inquired of Technical Operation Lead to confirm that Eden Health retains documentation of explicit consent in accordance with privacy-related purposes. | No exceptions noted |

| Criteria # | Description of Controlcase INC’s Controls | Tests Performed by Service Auditor | Results of Tests of Controls |
| --- | --- | --- | --- |
| P4.1 The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| P4.1.1 | Controlcase INC limits the use of personal information to the purposes identified in the privacy notice. | Inspected the privacy notices and privacy policies on the Eden Health public websites to confirm they specify the uses of personal information.    Inspected examples of how Eden Health uses personal information to generate customer alerts. | No exceptions noted |

| Criteria # | Description of Controlcase INC’s Controls | Tests Performed by Service Auditor | Results of Tests of Controls |
| --- | --- | --- | --- |
| P4.2 The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| P4.2.1 | Controlcase INC retains personal information and PHI for no longer than is necessary to fulfill the stated purposes unless a law or regulation specifically requires otherwise. | Inspected the Privacy Policy and HIPAA Security Manual confirmed that it provides notice on the purpose, choice, consent, collection, use and retention, access to, disclosure, security, and monitoring of personal information. The company will retain the required documentation of policies, procedures, actions, activities, or assessments required by the HIPAA Security Rule for six years from the date of its creation or the date when it last was in effect. | No exceptions noted |
| P4.2.2 | Policies and procedures have been implemented to protect personal information and PHI from erasure or destruction during the specified retention period of the information. | Inquired of Management to confirm that Eden Health has implemented policies and procedures to protect personal information and PHI from erasure or destruction during the specified retention period of the information. | No exceptions noted |
| P4.2.3 | Databases housing sensitive customer data are encrypted at rest. | Inspected the cryptography guidelines to determine requirements that have been defined regarding encryption and use of cryptographic keys.    Inspected database configurations to confirm that databases are encrypted at rest. | No exceptions noted |

| Criteria # | Description of Controlcase INC’s Controls | Tests Performed by Service Auditor | Results of Tests of Controls |
| --- | --- | --- | --- |
| P4.3 The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| P4.3.1 | Requests for deletion of PII and PHI are captured, and information related to the requests is identified and flagged for destruction to meet the entity’s privacy objectives. | Inspected evidence shows the requests to change or delete personal information, including evidence of how the requests were resolved. The request could be approved or denied via email. | No exceptions noted |
| P4.3.2 | Personal information and PHI no longer retained are anonymized, disposed of, or destroyed to prevent loss, theft, misuse, or unauthorized access. | Inquired of Management to confirm that Personal information no longer retained is anonymized, disposed of, or destroyed to prevent the loss, theft, misuse, or unauthorized access. Eden Health has not yet reached the retention/destruction period for any identifiable PHI as outlined in its data retention and destruction policy, but the process is in place. | No exceptions noted |

| Criteria # | Description of Controlcase INC’s Controls | Tests Performed by Service Auditor | Results of Tests of Controls |
| --- | --- | --- | --- |
| P5.1 The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| P5.1.1 | Identified and authenticated data subjects are given access to their personal information. Data subjects are also provided with information regarding the processes, systems, and third parties involved in the handling of such information. | Inspected the privacy notices and privacy policies on the Eden Health public websites to confirm they specify how data subjects are granted access to their personal information and information regarding the processes, systems, and third parties involved in the handling of their personal information.    Inspected evidence of member login pages used for members to log in to their accounts to access their personal information. | No exceptions noted |

| Criteria # | Description of Controlcase INC’s Controls | Tests Performed by Service Auditor | Results of Tests of Controls |
| --- | --- | --- | --- |
| P5.2 The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| P5.2.1 | Controlcase INC provides identified and authenticated data subjects with the ability to access their accounts online to correct, amend, or append their personal information. The Company communicates such information to third parties as committed or required. | Inspected the privacy notices and privacy policies on the company and public websites to confirm they specify how individuals can correct or amend their personal information within the member dashboards.    Inspected a sample of requests to change or delete personal information, including evidence of how the requests were resolved. The request could be approved or denied via email. | No exceptions noted |

| Criteria # | Description of Controlcase INC’s Controls | Tests Performed by Service Auditor | Results of Tests of Controls |
| --- | --- | --- | --- |
| P6.1 The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| P6.1.1 | Personal information is disclosed to third parties only for the purposes for which it was collected or created and only when implicit or explicit consent has been obtained from the data subject unless a law or regulation specifically requires otherwise. | Inspected the Privacy Policy and HIPAA Privacy Policy to confirm that they indicate disclosure to third parties for the purposes it was collected/created and only when consent has been obtained by the data subject unless a law or regulation specifically requires otherwise. | No exceptions noted |

| Criteria # | Description of Controlcase INC’s Controls | Tests Performed by Service Auditor | Results of Tests of Controls |
| --- | --- | --- | --- |
| P6.2 The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| P6.2.1 | Controlcase INC has published policies on its website that provide notice on the purpose, choice and consent, collection, use and retention, access to, disclosure, security, and monitoring of personal information and PHI. | Inspected the Privacy Policy and HIPAA Privacy Policy to confirm that it provides notice on the purpose, choice and consent, collection, use and retention, access to, disclosure, security, and monitoring of personal information and PHI.    Inquired of management confirms that during the registration process, users must consent to the policies that govern data collection, retention, and the user’s options to obtain this information. | No exceptions noted |
| P6.2.2 | Controlcase INC creates and maintains a complete, accurate, and timely record of authorized disclosures of personal information. | Inquired of management and inspected the privacy notice to determine that Eden Health maintains records of authorized disclosures of personal information that are complete, accurate and timely. Also, PII is not shared outside of the Companies without permission. | No exceptions noted |

| Criteria # | Description of Controlcase INC’s Controls | Tests Performed by Service Auditor | Results of Tests of Controls |
| --- | --- | --- | --- |
| P6.3 The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| P6.3.1 | Controlcase INC creates and maintains a record of detected or reported unauthorized disclosures of personal information. | Inspected the HIPAA policy and confirmed that Eden Health creates and maintains a record of detected or reported unauthorized disclosures of personal information PII and PHI. | No exceptions noted |

| Criteria # | Description of Controlcase INC’s Controls | Tests Performed by Service Auditor | Results of Tests of Controls |
| --- | --- | --- | --- |
| P6.4 The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| P6.4.1 | Personal information is disclosed only to third parties who have agreements with the entity to protect personal information in a manner consistent with the relevant aspects of Eden Health's Privacy Policy. | Inquired of management confirms Eden Health does not collect, alter, or dispose of the data; the patients make these decisions (Accepting Security Policy, terms and conditions, and HIPAA statement). Eden Health, at the time, entered data and did not receive PHI from third-party medical records. Eden Health does not share any personal information. Also, Eden Health does not utilize subcontractors. | No exceptions noted |

| Criteria # | Description of Controlcase INC’s Controls | Tests Performed by Service Auditor | Results of Tests of Controls |
| --- | --- | --- | --- |
| P6.5 The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| P6.5.1 | Arrangements involving Vendor and Third-Party access to organizational information processing facilities must be based on a formal contract containing all necessary security requirements accompanied with appropriate responsibility and confidentiality undertaking. Any violations thereto must be dealt with accordingly. | Inspected the Vendor Risk Management Policy to determine vendors are required to sign the agreements stating that they agree with the guidelines prior to the receipt of any confidential information.    For a selection of third-party vendors and service providers, including existing and new providers, it determined that external service provider performance and risks were assessed against established policies and practices as part of a periodic evaluation process, including action items for any shortcomings as well as follow-up on prior year’s action items as necessary. | No exceptions noted |
| P6.5.2 | Personal information is disclosed only to third parties who have agreements with the entity to protect personal information in a manner consistent with the relevant aspects of Eden Health's Privacy Policy. | Inquired of management confirms Eden Health does not collect, alter, or dispose of the data; the patients make these decisions (Accepting Security Policy, terms and conditions, and HIPAA statement). Eden Health, at the time to enter data, did not receive PHI from third-party medical records. Eden Health does not share any personal information. Also, Eden Health does not utilize subcontractors. | No exceptions noted |

| Criteria # | Description of Controlcase INC’s Controls | Tests Performed by Service Auditor | Results of Tests of Controls |
| --- | --- | --- | --- |
| P6.6 The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| P6.6.1 | Controlcase INC has a process for providing notice of breaches and incidents to affected data subjects, regulators, and others to meet the entity’s objectives related to privacy. | Inspected the HIPAA Security Manual and Incident Reporting Policy and confirmed that Eden Health has a model to respond to and mitigate personal data breaches. | No exceptions noted |
| P6.6.2 | Issues with system availability, confidentiality, and other security incidents are promptly addressed according to the company’s Security Incident Reporting Policy. | Inquired Management to determine that security incidents are promptly addressed according to the company's Security Incident Reporting Policy.    Inspected policies and procedures to determine procedures are in place in the event of a security incident resulting in unauthorized disclosure of personal information. | No exceptions noted |

| Criteria # | Description of Controlcase INC’s Controls | Tests Performed by Service Auditor | Results of Tests of Controls |
| --- | --- | --- | --- |
| P6.7 The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| P6.7.1 | Controlcase INC creates and maintains a complete, accurate, and timely record of authorized disclosures of personal information. | Inquired of management and inspected the privacy notice to determine that Eden Health maintains records of authorized disclosures of personal information that are complete, accurate, and timely. Also, PII is not shared outside of the Companies without permission. | No exceptions noted |

| Criteria # | Description of Controlcase INC’s Controls | Tests Performed by Service Auditor | Results of Tests of Controls |
| --- | --- | --- | --- |
| P7.1 The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| P7.1.1 | Personal information is accurate and complete for the purposes for which it is to be used. | Inspected Eden Health's Privacy Policy and confirmed that it provides notice that if any of the data is inaccurate or outdated, it can be requested to be corrected. Eden Health has backend validation on registration to confirm that patient demographic data is legitimate. | No exceptions noted |
| P7.1.2 | Controlcase INC policy is that only the personal information required to provide the service is collected. | Inspected the privacy notices and privacy policies on the Eden Health public websites to confirm they specify that only the personal information required to complete the service is collected. | No exceptions noted |

| Criteria # | Description of Controlcase INC’s Controls | Tests Performed by Service Auditor | Results of Tests of Controls |
| --- | --- | --- | --- |
| P8.1 The entity provides notice to data subjects about its privacy practices to meet the entity's objectives related to privacy. The notice is updated and communicated to data subjects in a timely manner for changes to the entity's privacy practices, including changes in the use of personal information, to meet the entity's objectives related to privacy. | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| P8.1.1 | Controlcase INC has published policies on its website that provide notice on the purpose, choice and consent, collection, use and retention, access to, disclosure, security, and monitoring of personal information and PHI. | Inspected the Privacy Policy and HIPAA Privacy Policy to confirm that it provides notice on the purpose, choice and consent, collection, use and retention, access to, disclosure, security, and monitoring of personal information and PHI.    Inquired of management confirms that during the registration process, users must consent to the policies that govern data collection, retention, and the user’s options to obtain this information. | No exceptions noted |
| P8.1.2 | Controlcase INC has implemented a process for receiving, addressing, resolving, documenting, and communicating the resolution of inquiries, complaints, and disputes from data subjects and others and periodically monitors compliance. | Inspected the Eden Health Security Incident Reporting Policy to confirm that there is a process for receiving, addressing, resolving, documenting, and communicating the resolution of inquiries, complaints and disputes from data subjects. | No exceptions noted |
| P8.1.3 | Controlcase INC performs ongoing monitoring of the effectiveness of controls over personal information and takes timely corrective actions when necessary. | Inspected evidence of ongoing monitoring of the effectiveness of controls over personal information, including quarterly internal assessments, annual policy reviews, and the use of ticketing systems to track and monitor the status of compliance reviews. | No exceptions noted |