bswift®

BSWIFT LLC

bswift Software-as-a-Service Platform

SOC 3 + HIPAA

System and Organization Controls (SOC) for Service Organizations Report
for the period of October 1, 2022 to September 30, 2023

Aprio®
Passionate for what's next®

Report of Independent Service Auditors issued by Aprio LLP

Table of Contents

I. Report of Independent Service Auditor

We have examined bswift LLC's (the "Company" or "bswift") accompanying assertion titled *bswift LLC's Assertion* (the "Assertion") indicating that the controls within the bswift Software-as-a-Service Platform (the "System") were effective for the period of October 1, 2022 to September 30, 2023 (the "Specified Period"), to provide reasonable assurance that bswift LLC's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*) and the applicable portions of the HIPAA Security Rule as defined in 45 CFR Part 160 and subparts A and C of Part 164 (the "HIPAA Criteria") for the Specified Period.

As of August 19, 2023, the Company uses Amazon Web Services ("AWS"), a subservice organization, for its cloud computing services in an Infrastructure-as-a-Service environment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. The Company also uses AWS' Elastic Compute Cloud (Amazon EC2) services and AWS' Simple Storage services. For the period October 1, 2022 to August 18, 2023, the Company used CVS Health Corporation ("CVS"), a subservice organization, for its data center services and hosting of servers and equipment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. The Company also used CVS for its infrastructure support, server patch management, storage management, network security management, workstation and laptop management, human resources management, and backup management services. The Company uses Microsoft Azure's ("Azure"), a subservice organization, Platform-as-a-Service for its hosting of workforce technology and identity solutions, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. This includes the use of Office 365, OneDrive, Azure Active Directory Domain, and Microsoft Defender. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at the Company, to achieve the Company's service commitments and system requirements based on the applicable trust services criteria and the HIPAA criteria. The description presents the Company's controls, the applicable trust services criteria, the HIPAA criteria, and the types of complementary subservice organization controls assumed in the design of the Company's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The Assertion indicates that certain AICPA Applicable Trust Services Criteria and the HIPAA criteria specified in the section titled *bswift LLC's Description of the Boundaries of its System*, under the section *User Entity Controls*, can be achieved only if complementary user entity controls contemplated in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the Company. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's responsibilities

The Company is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that the Company's service commitments and system requirements were achieved. The Company has provided the accompanying assertion titled *bswift LLC's Assertion* about the suitability of design and operating effectiveness of controls. When preparing its assertion, the Company is responsible for selecting, and identifying in its assertion, the Applicable Trust Services Criteria and the HIPAA criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that the controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the Applicable Trust Services Criteria and the HIPAA Criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements;
- Assessing the risks that the controls were not effective to achieve the Company's service commitments and system requirements based on the Applicable Trust Services criteria and the HIPAA criteria; and
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve the Company's service commitments and system requirements based on the Applicable Trust Services Criteria and the HIPAA criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

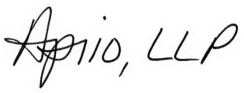
Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the Applicable Trust Services Criteria and the HIPAA criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Other matters

We did not perform any procedures regarding the fairness of presentation as it relates to the description criteria of the description in Section III titled *bswift LLC's Description of the Boundaries of its System*, and, accordingly, do not express an opinion thereon.

Opinion
In our opinion, bswift LLC's assertion that the controls within the Company's System were effective throughout the Specified Period to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the Applicable Trust Services Criteria and the HIPAA criteria, in all material respects, is fairly stated.

Aprio, LLP



Atlanta, Georgia
December 14, 2023

II. bswift LLC's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls over bswift LLC's (the "Company" or "bswift") bswift Software-as-a-Service Platform (the "System") for the period of October 1, 2022 to September 30, 2023 (the "Specified Period"), to provide reasonable assurance that the Company's service commitments and system requirements relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy were achieved. We have performed an evaluation of the effectiveness of the controls within the System throughout the Specified Period to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy (the "Applicable Trust Services Criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*) and the applicable portions of the HIPAA Security Rule as defined in 45 CFR Part 160 and subparts A and C of Part 164 (the "HIPAA Criteria") for the Specified Period. The Company's objectives for the system in applying the Applicable Trust Services Criteria are embodied in its service commitments and system requirements relevant to the Applicable Trust Services Criteria. The principal service commitments and system requirements related to the Applicable Trust Services Criteria and the HIPAA criteria are specified in the section titled *bswift LLC's Description of the Boundaries of its System*.

As of August 19, 2023, the Company uses Amazon Web Services ("AWS"), a subservice organization, for its cloud computing services in an Infrastructure-as-a-Service environment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. The Company also uses AWS' Elastic Compute Cloud (Amazon EC2) services and AWS' Simple Storage services. For the period October 1, 2022 to August 18, 2023, the Company used CVS Health Corporation ("CVS"), a subservice organization, for its data center services and hosting of servers and equipment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. The Company also used CVS for its infrastructure support, server patch management, storage management, network security management, workstation and laptop management, human resources management, and backup management services. The Company uses Microsoft Azure's ("Azure"), a subservice organization, Platform-as-a-Service for its hosting of workforce technology and identity solutions, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. This includes the use of Office 365, OneDrive, Azure Active Directory Domain, and Microsoft Defender. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at bswift, to achieve bswift's service commitments and system requirements based on the applicable trust services criteria and the HIPAA criteria. The description presents the bswift's controls, the applicable trust services criteria, the HIPAA criteria, and the types of complementary subservice organization controls assumed in the design of the bswift's controls. The description does not disclose the actual controls at the subservice organizations.

Certain AICPA Applicable Trust Services Criteria specified in the section titled *bswift LLC's Description of the Boundaries of its System*, under the section *Subservice Organizations*, can be achieved only if complementary subservice organization controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the Company. Management's assertion includes only the controls of the Company and excludes the controls performed by the subservice organizations. Certain AICPA Applicable Trust Services Criteria and the HIPAA criteria, specified in Section III, *bswift LLC's Description of the Boundaries of its System*, under the section *User Entity Controls* can be achieved only if complementary user entity controls contemplated in the design of the Company's controls are suitably designed and operating effectively, along with related controls at the Company. Management's assertion includes only the controls of the Company and excludes the controls performed by User Entities.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the System were effective throughout the Specified Period to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the Applicable Trust Services Criteria.

III. bswift LLC's Description of the Boundaries of its System

A. Scope and Purpose of the Report

This report describes the control structure of bswift LLC (the "Company" or "bswift") as it relates to its bswift Software-as-a-Service Platform (the "System") for the period of October 1, 2022 to September 30, 2023 (the "Specified Period"), for the trust services criteria relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy (the "Applicable Trust Services Criteria") as set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*) and the applicable portions of the HIPAA Security Rule as defined in 45 CFR Part 160 and subparts A and C of Part 164 (the "HIPAA Criteria").

It is the responsibility of each specified party to evaluate this information in relation to the control structure in place at the user organization to assess the total internal control environment. The internal control structures at the Company are not designed to compensate for any weaknesses that may exist if the internal control structure at a user organization is ineffective.

B. Company Overview and Background

bswift offers software and services that streamline human resources (HR) and benefits administration.

Effective November 7, 2022, bswift was acquired by Francisco Partners, a global investment firm that specializes in partnering with technology businesses. Prior to the acquisition, bswift was wholly owned by CVS Health Corporation. As a part of the acquisition, bswift may elect to utilize certain CVS Health services for a period of up to 18 months, concluding May 7, 2024.

C. System Overview

1. Infrastructure

The bswift SaaS Platform's infrastructure was located at the Phoenix Data Center (PDC), a subservice organization owned by CVS until August 18, 2023. Effective August 19, 2023, the bswift SaaS Platform's infrastructure was transitioned to Amazon Web Services (AWS). AWS provides the physical security and environmental protection controls – refer to *Subservice Organizations* section below.

2. Software

The system is implemented using Windows, MSSQL, IIS, and Microsoft technology with known performance, scalability, and security properties.

3. People

bswift has a staff of approximately 1,100 employees organized in the following functional areas:

- *Chief Executive Officer* – responsible for bswift's strategic vision, growth, and culture.
- *Chief Operating Officer* – responsible for service operations and delivery.
- *Chief Information Security Officer* – responsible for enhancement and maintenance of IT security program, infrastructure, and workplace technology.
- *Chief Legal Officer* – responsible for leading bswift's corporate legal and compliance department.
- *Chief Financial Officer* – responsible for leading Finance and Accounting.
- *Chief People Officer* – responsible for leading the People team that provides all human resource functional needs including learning and development.
- *Chief Growth Officer* – responsible for leading sales, client relationship management, marketing, and growth strategy.
- *Executive Vice President (EVP) Strategic Product Management* – responsible for developing the product roadmap and driving innovation.
- *EVP Operational Excellence* – responsible for consistent, high-quality delivery of service to clients and partners, and efficient deployment of the technology roadmap.
- *EVP Engineering* – responsible for delivery of product enhancements and other technology commitments.

4. Data

Information takes many forms and may be stored on computers, transmitted across networks, printed or written on paper, or spoken in conversations. bswift personnel are obligated to respect and, in all cases, to protect confidential and private data. Customer information, employment-related records, and other intellectual property-related records are, subject to limited exceptions, confidential as a matter of law. Many other categories of records, including Company and other personnel records, and records relating to bswift's business and finances are treated as confidential as a matter of bswift policy. Responsibility for maintaining appropriate security for data, systems, and networks is shared by the Client Services and IT Departments. IT is responsible for designing, implementing, and maintaining security protection and retains responsibility for compliance with the policy. In addition to management and the technology staff, individual users are responsible for the equipment and resources under users control.

Policies and procedures are in place regarding proper retention and disposal of confidential and private data. The Data Classification and Handling Policy outlines the handling, communication, destruction, maintenance, storage, back-up, distribution, identification, and classification of confidential information as well as the identification of related processes, systems, and third parties involved in the handling of such information. This policy is reviewed, updated, and approved on an annual basis by management. Formal data retention and destruction standards have been developed to provide guidelines for the retention of data for required periods of time. The Company disposes of confidential data when requested by the client upon end of a contract unless regulatory requirements dictate a longer retention period. bswift maintains security policies and communicates with staff to inform individuals utilizing Company resources of the employee's responsibilities in reducing the risk of compromise and exercise appropriate security measures to protect systems and data.

Electronic communications are treated with the same level of confidentiality and security as physical documents. All transmissions of electronic information from/to the production environment is encrypted as the default setting over public networks via secure transmission protocols (e.g., HTTPS and TLS). The Company maintains a system log of all carrier file transmissions, including to whom, and when the files were transmitted.

The Company has operationalized its commitments to maintaining confidentiality and integrity for processing customer data, using reasonably available in force measures within the information technology industry. System requirements are documented in customer contracts including definitions of data processed and product and service specifications to support the use of the products and services. A member of the Legal Department is responsible for reviewing and approving the customer contract for each new customer.

All confidential data related to the production environment is de-identified prior to use in non-production environments. Data within the in-scope databases is encrypted while at rest. Laptops are configured to enforce hard drive encryption to access the Company's network. Encryption keys are maintained in a secured location, and access is limited to appropriate personnel based on job function.

5. Policies and Procedures

Management has developed and communicated to bswift employees the defined policies and procedures to restrict logical access to the systems. The Company has implemented a formal written Information Security Policy, Incident Response Policy, Data Classification Policy, and Privacy Policy which collectively address the security, availability, confidentiality, and privacy of the system and cover the escalation process for security breaches and other incidents. These policies are reviewed and approved by management on an annual basis and are posted on the Company's intranet.

The Company has implemented formal documented privacy notice which addresses the following:

- The purpose for collecting personal information;
- Choice and consent;
- Types of personal information collected;
- Methods of collection (e.g., use of cookies, etc.);
- Uses, retention, and disposal;
- Access;
- Disclosure to third parties;
- Security for privacy;
- Quality, including Data Subjects' responsibilities for quality; and
- Monitoring and enforcement.

Changes to these policies and procedures are performed annually and authorized by senior management. These procedures cover the following key security life cycle areas:

- Acceptable Use
- Access Management
- Asset Management
- AI Utilities Usage
- Backup and Data Restoration
- Business Continuity
- Change Management
- Data Classification and Handling
- Device Management
- Encryption and Key Management
- HR and Personnel Security
- Incident Response
- Information Security

- Network Security
- Physical Security
- Risk Management
- Third-party Risk Management
- Vulnerability Management

D. Principal Service Commitments and System Requirements

bswift has designed processes and procedures related to the SaaS Platform to meet its objectives. Those objectives are based on the service commitments that bswift makes to user entities, the laws and regulations that govern the provision of the services, and the operational and compliance requirements that bswift has established for the services.

Security, availability, processing integrity, availability, and privacy commitments to user entities are documented and communicated via the executed contracts, as well as in the description of the services offered. Security, availability, confidentiality, processing integrity, and privacy commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental design of the System permits system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role;
- Uptime availability of production systems;
- Processing information completely, accurately, and in a timely manner;
- Use of encryption technologies to protect confidential data at rest and in transit; and
- Protection of personal information regarding the collection, use, retention, disclosure, and disposal, as applicable.

The Company establishes operational requirements that support the achievement of security, availability, processing integrity, confidentiality, and privacy commitments; service level commitments; relevant laws and regulations; and other system requirements. Such requirements are communicated in bswift's policies, procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. They include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. Management is committed to being aware of regulatory and economic changes that impact lines of business and monitoring the customer base for trends, changes, and anomalies.

E. Non-Applicable Trust Services Criteria

Security, Availability, Processing Integrity, Confidentiality, and Privacy Trust Services Categories		
Non-Applicable Trust Services Criteria		**bswift's Rationale**
CC 6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	N/A – The Company's third-party providers, AWS, CVS, and Azure, are responsible for physical security controls, including environmental safeguards such as UPS, backup generators, and fire suppression. The Company does not maintain any hard copy data or store any customer information physically.

Security, Availability, Processing Integrity, Confidentiality, and Privacy Trust Services Categories		
Non-Applicable Trust Services Criteria		**bswift's Rationale**
P 5.1	The entity grants identified and authenticated data subjects the ability to access their stored personal information for review and, upon request, provides physical or electronic copies of that information to data subjects to meet the entity's objectives related to privacy. If access is denied, data subjects are informed of the denial and reason for such denial, as required, to meet the entity's objectives related to privacy.	N/A – The Company is not a Data Controller. The relationship with the data subjects is with the client; therefore, any requests for personal information from the data subjects would be directed to the client. Therefore, these criteria are not applicable.
P 5.2	The entity corrects, amends, or appends personal information based on information provided by data subjects and communicates such information to third parties, as committed or required, to meet the entity's objectives related to privacy. If a request for correction is denied, data subjects are informed of the denial and reason for such denial to meet the entity's objectives related to privacy.	
P 6.7	The entity provides data subjects with an accounting of the personal information held and disclosure of the data subjects' personal information, upon the data subjects' request, to meet the entity's objectives related to privacy.	
P 7.1	The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet the entity's objectives related to privacy.	

F. Subservice Organizations

The Company utilizes subservice organizations to perform certain functions. The description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at the third-party subservice organizations described below. The examination by the Independent Service Auditor did not extend to the policies and procedures at these subservice organizations.

Complementary subservice organization controls, controls that management of the service organization assumes will be implemented by the subservice organizations and are necessary to achieve the service organization's service commitments and system requirements based on the applicable trust services criteria, along with the associated subservice organizations, are included within the table below. Management also describes the activities performed to monitor the effectiveness of controls at the subservice organizations. Each user entity's internal control must be evaluated in conjunction with the Company's controls and taking into account the related complementary subservice organization controls expected to be implemented at the subservice organizations as described below.

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
Amazon Web Services (AWS)	As of August 19, 2023, the Company uses AWS for its cloud computing services in an Infrastructure-as-a-Service environment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. The Company also uses AWS' Elastic Compute Cloud (Amazon EC2) services and AWS' Simple Storage services. The following control activities are critical to achieving the Applicable Trust Services Criteria: • Controls over the underlying infrastructure and Data Centers supporting the in-scope production environment including environmental safeguards such as UPS, backup generators, and fire suppression; • Controls over managing infrastructure security such as physical servers and physical access to backups and facilities; • Controls over the change management processes for the physical servers supporting the Infrastructure-as-a-Service Platform; • Controls over the configuration settings within the EC2 instance to ensure that data is encrypted and stored as per the configuration settings selected with AWS; • Controls over incident monitoring, response, and follow up; • Controls over managing the Platform-as-a-Service components for Amazon S3 such as physical servers and operating systems including applying critical patching for this infrastructure; • Controls over Amazon S3 including operating system installation and patches; database software installation and patches; and routers/firewalls monitoring and maintenances; • Controls over AWS S3 redundancy, including controls over data replication; and • Controls over the change management processes for the AWS Infrastructure-as-a-Service Platform and the Platform-as-a-Service S3 Platform components as applicable.	CC 5.2* CC 6.1* CC 6.2* CC 6.3* CC 6.4 CC 6.5* CC 6.6* CC 6.7* CC 6.8* CC 7.1* CC 7.2* CC 7.3* CC 7.4* CC 7.5* CC 8.1* CC 9.1* CC 9.2* A 1.1* A 1.2* A 1.3* C 1.1* C 1.2* PI 1.2* PI 1.3* PI 1.4* PI 1.5* P 4.2* P 4.3*

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
	In addition, the Company has identified the following control activity to help monitor the subservice organization: • On at least an annual basis, management evaluates the third parties who have access to confidential data and/or who perform a managed service related to the operation of the system and determines their risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations. Based on this risk rating, management either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 reports, or the third party is subjected to continuous monitoring controls. Corrective actions are taken, if necessary; and • Data restore testing is performed on at least a quarterly basis to verify the integrity of the backup data.	P 6.6*
CVS Health Corporation (CVS)	For the period October 1, 2022 to August 18, 2023, the Company used CVS for its data center services and hosting of servers and equipment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. The Company also used CVS for its infrastructure support, server patch management, storage management, network security management, workstation and laptop management, human resources management, and backup management services. The following control activities are critical to achieving the Applicable Trust Services Criteria: • Controls over the underlying infrastructure and Data Centers supporting the in-scope production environment including environmental safeguards such as UPS, backup generators, and fire suppression; • Controls over managing infrastructure security such as physical servers and physical access to backups and facilities; • Controls over the change management processes for the physical servers supporting the Infrastructure-as-a-Service environment, including design, build, implementation, maintenance; • Controls over infrastructure support, including availability monitoring and day-to-day support; • Controls over the configuration settings within the in-scope production environment to ensure that data is encrypted and stored as per the configuration settings selected; • Controls over the management of stored data related to the in-scope production environment, including redundancy; • Controls over incident monitoring, response, and follow up for the network, Company-owned laptops and workstations, firewalls, IDS, and VPN; • Controls over the underlying infrastructure and Data Centers supporting the in-scope production environment including operating systems installation including applying critical patching for this infrastructure;	CC 1.1* CC 1.2* CC 1.3* CC 1.4* CC 1.5* CC 2.1* CC 2.2* CC 3.1* CC 3.4* CC 4.1* CC 4.2* CC 5.1* CC 5.2* CC 5.3* CC 6.1* CC 6.2* CC 6.3* CC 6.4 CC 6.5* CC 6.6* CC 6.7* CC 6.8* CC 7.1* CC 7.2* CC 7.3* CC 7.4* CC 7.5*

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
	• Controls over the monitoring of backup performance and the backup settings within the in-scope system, including redundancy and data replication; • Controls over security awareness training, including performance and the security policies and procedures; and • Controls over logical access to in-scope systems, Company assets, and client data. In addition, the Company has identified the following control activity to help monitor the subservice organization: • On at least an annual basis, management evaluates the third parties who have access to confidential data and/or who perform a managed service related to the operation of the system and determines their risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations. Based on this risk rating, management either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 reports, or the third party is subjected to continuous monitoring controls. Corrective actions are taken, if necessary; and • Data restore testing is performed on at least a quarterly basis to verify the integrity of the backup data.	CC 8.1* CC 9.1* CC 9.2* A 1.1* A 1.2* A 1.3* C 1.1* C 1.2* PI 1.1* PI 1.2* PI 1.3* PI 1.4* PI 1.5* P 4.2* P 4.3* P 6.3* P 6.6* P 8.1*
Microsoft Azure (Azure)	The Company uses Azure's Platform-as-a-Service for its hosting of workforce technology and identity solutions, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. This includes the use of Office 365, OneDrive, Azure Active Directory Domain, and Microsoft Defender. The following control activities are critical to achieving the Applicable Trust Services Criteria: • Controls over the underlying infrastructure and Data Centers supporting the in-scope production environment including environmental safeguards such as UPS, backup generators, and fire suppression; • Controls over managing the security of infrastructure and software including Azure SQL Database service such as physical servers and physical access to backups and facilities; • Controls over the change management processes for the software and infrastructure supporting the platform including Azure SQL Database service; • Controls over incident monitoring, response, and follow up; • Controls over the prevention, detection, and follow up upon the introduction of malicious software; • Controls over Azure Storage redundancy, including controls over data replication; • Controls over the monitoring of the Office 365, OneDrive, and Azure AD, and MS Defender Software-as-a-Service components	CC 5.2* CC 6.1* CC 6.2* CC 6.3* CC 6.4 CC 6.5* CC 6.6* CC 6.7* CC 6.8* CC 7.1* CC 7.2* CC 7.3* CC 7.4* CC 7.5* CC 8.1* CC 9.1* CC 9.2* A 1.1* A 1.2* A 1.3* C 1.1*

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
	including backups, anti-virus, and incidents related to security and availability including responding to items identified; • Controls over the encryption of transmitted and stored data within the platform including Azure SQL Database service; and • Controls over managing patching for the software and infrastructure supporting the platform, including Azure SQL Database service. In addition, the Company has identified the following control activity to help monitor the subservice organization: • On at least an annual basis, management evaluates the third parties who have access to confidential data and/or who perform a managed service related to the operation of the system and determines their risk-rating based on their level of access, the sensitivity of the related data, and the impact to operations. Based on this risk rating, management either performs a vendor security assessment of the third party, reviews the third party's System and Organization Control reports such as SOC 2 reports, or the third party is subjected to continuous monitoring controls. Corrective actions are taken, if necessary; and • Data restore testing is performed on at least a quarterly basis to verify the integrity of the backup data.	C 1.2* PI 1.4* PI 1.5* P 4.2* P 4.3* P 6.6*

** The achievement of design and operating effectiveness related to this criterion assumes that the complementary controls at this subservice organization that support the service organization's service commitments and system requirements are in place and are operating effectively.*

G. User Entity Controls

bswift LLC's controls relating to the system cover only a portion of the overall internal control structure of each user entity of the Company. It is not feasible for the Company's service commitments and system requirements to be achieved based on the applicable trust services criteria solely by the Company. Therefore, each user entity's internal control must be evaluated in conjunction with the Company's controls and taking into account the related complementary user entity controls identified within the table below, where applicable. As applicable, suggested control considerations and/or complementary user entity controls and their associated criteria have been included within the table below.

Management has highlighted criterion in which complementary user entity controls were assumed in the design of the Company's system with an asterisk. In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal control environment to determine if the identified complementary user entity controls have been implemented and are operating effectively.

Furthermore, the table below includes suggested control considerations that the Company believes each user organization should consider in developing their internal controls or planning their audits that are relevant to the Company's controls detailed in this report, however, such control considerations are not required to achieve design or operating effectiveness for the Company's service commitments and system requirements based on the applicable trust services criteria. The following list of suggested control activities is intended to address only those policies and procedures surrounding the interface and communication between the Company and each user entity. Accordingly, this list does not allege to be, and is not, a complete listing of all the control activities which provide a basis for the assertions underlying the control environments for the Company's user entities.

User Entity Control	Associated Criteria
User Entities are responsible for ensuring that the authentication of the bswift SaaS Platform meets the User Entities' logical access standards, including configurable password and authentication standards.	CC 5.2* CC 6.1* CC 6.7*
User Entities are responsible for periodically reviewing access to the bswift SaaS Platform to ensure that User Entities' users' access is appropriate and for notifying the Company of any changes that need to be made.	CC 6.1* CC 6.2* CC 6.3*
User Entities are responsible for requesting access provisioning and de-provisioning for their users. In addition, User Entities are responsible for notifying the Company in a timely manner when access must be removed due to events such as the termination of a user.	CC 6.2* CC 6.3*
User Entities are responsible for defining data retention and destruction policies and for ensuring that the User Entities' bswift SaaS Platform instance meets those standards, including requesting of bswift when User Entities' data should be deleted.	CC 6.5* PI 1.5* C 1.1* C 1.2* P 4.2* P 4.3*
User Entities are responsible for immediately notifying the Company of any actual or suspected information security breaches, including compromised user accounts.	CC 7.1 CC 7.2 CC 7.3 CC 7.4 CC 7.5
User Entities are responsible for ensuring data is complete and accurate when providing information to bswift to input into the SaaS Platform.	PI 1.2*

** The achievement of design and operating effectiveness related to this criterion assumes that the complementary user entity controls that support the service organization's service commitments and system requirements are in place and are operating effectively.*

H. Cross-referencing of the SOC 2 Criteria to the HIPAA Criteria

Safeguard / Area	HIPAA Security Rule 45 CFR Standard	SOC 2 Criteria Mapping
Administrative Safeguards	§164.308 Administrative safeguards.	
Administrative Safeguards	§164.308(a) A covered entity or business associate must, in accordance with §164.306:	
Administrative Safeguards	§164.308(a)(1)(i) **Standard: Security management process.** Implement policies and procedures to prevent, detect, contain, and correct security violations.	CC 1.1
Administrative Safeguards	§164.308(a)(1)(ii) **Implementation specifications:**	

Safeguard / Area	HIPAA Security Rule 45 CFR Standard	SOC 2 Criteria Mapping
Administrative Safeguards	§164.308(a)(1)(ii)(A) **Risk analysis (Required).** 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.	CC 2.1
Administrative Safeguards	§164.308(a)(1)(ii)(B) **Risk management (Required).** Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).	CC 2.1
Administrative Safeguards	§164.308(a)(1)(ii)(C) **Sanction policy (Required).** Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.	CC 1.1
Administrative Safeguards	§164.308(a)(1)(ii)(D) **Information system activity review (Required).** Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	CC 2.1 CC 4.2
Administrative Safeguards	§164.308(a)(2) **Standard: Assigned security responsibility.** Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.	CC 1.3
Administrative Safeguards	§164.308(a)(3)(i) **Standard: 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.	CC 1.1
Administrative Safeguards	§164.308(a)(3)(ii) **Implementation specifications:**	
Administrative Safeguards	§164.308(a)(3)(ii)(A) **Authorization and/or supervision (Addressable).** 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.	CC 6.2
Administrative Safeguards	§164.308(a)(3)(ii)(B) **Workforce clearance procedure (Addressable).** Implement procedures to determine that the access of a workforce member to electronic protected health information **is appropriate.**	CC 6.2

Safeguard / Area	HIPAA Security Rule 45 CFR Standard	SOC 2 Criteria Mapping
Administrative Safeguards	§164.308(a)(3)(ii)(C) **Termination procedures (Addressable).** Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.	CC 6.1
Administrative Safeguards	§164.308(a)(4)(i) **Standard: 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.	CC 1.1
Administrative Safeguards	§164.308(a)(4)(ii) **Implementation specifications:**	
Administrative Safeguards	§164.308(a)(4)(ii)(A) **Isolating health care clearinghouse functions (Required).** 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, bswift is not a healthcare clearinghouse.
Administrative Safeguards	§164.308(a)(4)(ii)(B) **Access authorization (Addressable).** Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.	CC 6.2
Administrative Safeguards	§164.308(a)(4)(ii)(C) **Access establishment and modification (Addressable).** Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	CC 6.1 CC 6.2
Administrative Safeguards	§164.308(a)(5)(i) **Standard: Security awareness and training.** Implement a security awareness and training program for all members of its workforce (including management).	CC 1.1 CC 1.4
Administrative Safeguards	§164.308(a)(5)(ii) **Implementation specifications. Implement:**	
Administrative Safeguards	§164.308(a)(5)(ii)(A) **Security reminders (Addressable).** Periodic security updates.	CC 5.2
Administrative Safeguards	§164.308(a)(5)(ii)(B) **Protection from malicious software (Addressable).** Procedures for guarding against, detecting, and reporting malicious software.	CC 2.1 CC 6.8
Administrative Safeguards	§164.308(a)(5)(ii)(C) **Log-in monitoring (Addressable).** Procedures for monitoring log-in attempts and reporting discrepancies.	CC 2.1 CC 6.6

Safeguard / Area	HIPAA Security Rule 45 CFR Standard	SOC 2 Criteria Mapping
Administrative Safeguards	§164.308(a)(5)(ii)(D) **Password management (Addressable).** Procedures for creating, changing, and safeguarding passwords.	CC 6.1
Administrative Safeguards	§164.308(a)(6) (i) **Standard: Security incident procedures.** Implement policies and procedures to address security incidents.	CC 1.1 CC 4.2
Administrative Safeguards	§164.308(a)(6)(ii) **Implementation specification: Response and reporting (Required).** 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.	CC 1.1 CC 4.2
Administrative Safeguards	§164.308(a)(7)(i) **Standard: 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.	CC 7.4 CC 7.5
Administrative Safeguards	§164.308(a)(7)(ii) **Implementation specifications:**	
Administrative Safeguards	§164.308(a)(7)(ii)(A) **Data backup plan (Required).** Establish and implement procedures to create and maintain retrievable exact copies of electronic protected health information.	CC 7.4
Administrative Safeguards	§164.308(a)(7)(ii)(B) **Disaster recovery plan (Required).** Establish (and implement as needed) procedures to restore any loss of data.	CC 7.4 CC 7.5
Administrative Safeguards	§164.308(a)(7)(ii)(C) **Emergency mode operation plan (Required).** 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.	CC 7.5
Administrative Safeguards	§164.308(a)(7)(ii)(D) **Testing and revision procedures (Addressable).** Implement procedures for periodic testing and revision of contingency plans.	CC 7.5
Administrative Safeguards	§164.308(a)(7)(ii)(E) **Applications and data criticality analysis (Addressable).** Assess the relative criticality of specific applications and data in support of other contingency plan components.	CC 7.5
Administrative Safeguards	§164.308(a)(8) **Standard: Evaluation.** 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.	CC 1.1 CC 1.3

Safeguard / Area	HIPAA Security Rule 45 CFR Standard	SOC 2 Criteria Mapping
Administrative Safeguards	§164.308(b)(1) **Business associate contracts and other arrangements.** 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. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.	CC 1.3
Administrative Safeguards	§164.308(b)(2) A business associate may permit a business associate that is a subcontractor to create, receive, maintain, or transmit electronic protected health information on its behalf only if the business associate obtains satisfactory assurances, in accordance with §164.314(a), that the subcontractor will appropriately safeguard the information.	CC 1.3
Administrative Safeguards	§164.308(b)(3) **Implementation specifications: Written contract or other arrangement (Required).** Document the satisfactory assurances required by paragraph (b)(1) or (b)(2) of this section through a written contract or other arrangement with the business associate that meets the applicable requirements of §164.314(a).	CC 1.3
Physical Safeguards	§164.310 Physical safeguards.	
Physical Safeguards	§164.310 A covered entity or business associate must, in accordance with §164.306	
Physical Safeguards	§164.310(a)(1) **Standard: 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.	N/A - Physical Security is managed by a subservice organization.
Physical Safeguards	§164.310(a)(2) **Implementation specifications:**	
Physical Safeguards	§164.310(a)(2)(i) **Contingency operations (Addressable).** 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.	CC 7.5
Physical Safeguards	§164.310(a)(2)(ii) **Facility security plan (Addressable).** Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	N/A - Physical Security is managed by a subservice organization.

Safeguard / Area	HIPAA Security Rule 45 CFR Standard	SOC 2 Criteria Mapping
Physical Safeguards	§164.310(a)(2)(iii) **Access control and validation procedures (Addressable).** 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.	N/A - Physical Security is managed by a subservice organization.
Physical Safeguards	§164.310(a)(2)(iv) **Maintenance records (Addressable).** 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).	N/A - Physical Security is managed by a subservice organization.
Physical Safeguards	§164.310(b) **Standard: Workstation use.** Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.	CC 1.1
Physical Safeguards	§164.310(c) **Standard: Workstation security.** Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users.	N/A - Management of hardware and electronic media is managed by a subservice organization.
Physical Safeguards	§164.310(d)(1) **Standard: 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.	N/A - Management of hardware and electronic media is managed by a subservice organization.
Physical Safeguards	§164.310(d)(2) **Implementation specifications:**	
Physical Safeguards	§164.310(d)(2)(i) **Disposal (Required).** 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.	CC 6.5
Physical Safeguards	§164.310(d)(2)(ii) **Media re-use (Required).** Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.	N/A - Management of hardware and electronic media is managed by a subservice organization.
Physical Safeguards	§164.310(d)(2)(iii) **Accountability (Addressable).** Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	N/A - Management of hardware and electronic media is managed by a subservice organization.
Physical Safeguards	§164.310(d)(2)(iv) **Data backup and storage (Addressable).** Create a retrievable, exact copy of electronic protected health information, when needed, before movement of equipment.	N/A - Management of hardware and electronic media is managed by a subservice organization.
Technical Safeguards	§164.312 Technical safeguards.	

Safeguard / Area	HIPAA Security Rule 45 CFR Standard	SOC 2 Criteria Mapping
Technical Safeguards	§164.312 A covered entity or business associate must, in accordance with §164.306:	
Technical Safeguards	§164.312(a)(1) **Standard: 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).	CC 1.1 CC 6.1 CC 6.2
Technical Safeguards	§164.312(a)(2) **Implementation specifications:**	
Technical Safeguards	§164.312(a)(2)(i) **Unique user identification (Required).** Assign a unique name and/or number for identifying and tracking user identity.	CC 5.2
Technical Safeguards	§164.312(a)(2)(ii) **Emergency access procedure (Required).** Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	CC 7.5
Technical Safeguards	§164.312(a)(2)(iii) **Automatic logoff (Addressable).** Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	CC 6.1
Technical Safeguards	§164.312(a)(2)(iv) **Encryption and decryption (Addressable).** Implement a mechanism to encrypt and decrypt electronic protected health information.	CC 6.1 CC 6.7
Technical Safeguards	§164.312(b) **Standard: Audit controls.** Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	CC 2.1
Technical Safeguards	§164.312(c)(1) **Standard: Integrity.** Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	CC 1.1 CC 6.1 CC 6.2 CC 6.5
Technical Safeguards	§164.312(c)(2) **Implementation specification: Mechanism to authenticate electronic protected health information (Addressable).** Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	CC 2.1 CC 5.2
Technical Safeguards	§164.312(d) **Standard: Person or entity authentication.** Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	N/A - bswift is not responsible for providing access to electronic protected health information to data subjects.

Safeguard / Area	HIPAA Security Rule 45 CFR Standard	SOC 2 Criteria Mapping
Technical Safeguards	§164.312(e)(1) **Standard: 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.	CC 5.2 CC 6.6 CC 6.7
Technical Safeguards	§164.312(e)(2) **Implementation specifications:**	
Technical Safeguards	§164.312(e)(2)(i) **Integrity controls (Addressable).** Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	CC 5.2 CC 6.6 CC 6.7
Technical Safeguards	§164.312(e)(2)(ii) **Encryption (Addressable).** Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	CC 6.1 CC 6.7
Organizational Safeguards	§164.314 Organizational requirements.	
Organizational Safeguards	§164.314(a)(1) **Standard: 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.	CC 1.3
Organizational Safeguards	§164.314(a)(2) **Implementation specifications (Required).**	
Organizational Safeguards	§164.314(a)(2)(i) **Business associate contracts.** The contract must provide that the business associate will adhere to the requirements of the subparts below.	
Organizational Safeguards	§164.314(a)(2)(i)(A/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; and	CC 1.3
Organizational Safeguards	§164.314(a)(2)(i)(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.	CC 1.3
Organizational Safeguards	§164.314(a)(2)(ii) **Other arrangements.** 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).	CC 1.3
Organizational Safeguards	§164.314(a)(2)(iii) **Business associate contracts with subcontractors.** 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.	CC 1.3

Safeguard / Area	HIPAA Security Rule 45 CFR Standard	SOC 2 Criteria Mapping
Organizational Safeguards	§164.314(b) (1) **Standard: 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.	N/A - bswift is not a group health plan.
Organizational Safeguards	§164.314(b)(2) **Implementation specifications (Required).** The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to—	N/A - bswift is not a group health plan.
Organizational Safeguards	§164.314(b)(2)(i) 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 - bswift is not a group health plan.
Organizational Safeguards	§164.314(b)(2)(ii) Ensure that the adequate separation required by §164.504(f)(2)(iii) is supported by reasonable and appropriate security measures;	N/A - bswift is not a group health plan.
Organizational Safeguards	§164.314(b)(2)(iii) Ensure that any agent to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and	N/A - bswift is not a group health plan.
Organizational Safeguards	§164.314(b)(2)(iv) Report to the group health plan any security incident of which it becomes aware.	N/A - bswift is not a group health plan.
Organizational Safeguards	§164.316 Policies and procedures and documentation requirements.	
Organizational Safeguards	§164.316 A covered entity or business associate must, in accordance with §164.306:	
Organizational Safeguards	§164.316(a) **Standard: 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.	CC 1.1 CC 1.3
Documentation Safeguards	§164.316(b)(1) **Standard: Documentation.**	
Documentation Safeguards	§164.316(b)(1)(i) Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and	CC 1.1 CC 1.3

Safeguard / Area	HIPAA Security Rule 45 CFR Standard	SOC 2 Criteria Mapping
Documentation Safeguards	§164.316(b)(1)(ii) If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.	CC 1.1 CC 1.3
Documentation Safeguards	§164.316(b)(2) **Implementation specifications:**	
Documentation Safeguards	§164.316(b)(2)(i) **Time limit (Required).** 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.	CC 6.5
Documentation Safeguards	§164.316(b)(2)(ii) **Availability (Required).** Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	CC 1.1 CC 1.3
Documentation Safeguards	§164.316(b)(2)(iii) **Updates (Required).** Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.	CC 1.3 CC 2.1


Aprio