bswift®

BSWIFT LLC

bswift Benefits Administration Platform

SOC 3 + HIPAA

System and Organization Controls (SOC) for Service Organizations Report
for the period of October 1, 2023 to September 30, 2024

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 Benefits Administration Platform (the "System" or "bswift Platform") were effective for the period of October 1, 2023 to September 30, 2024 (the "Specified Period") to provide reasonable assurance that bswift'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* (With Revised Points of Focus – 2022) (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 uses various subservice organizations to support the bswift Platform as described in the *Subservice Organizations* section of Section III of this report. Certain AICPA applicable trust services criteria HIPAA 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. The Assertion 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.

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.

We are required to be independent and to meet our ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

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.

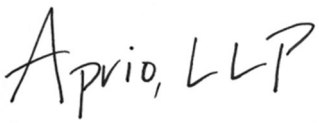
Other matters

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'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 11, 2024

The SOC Logo is a proprietary trademark and service mark of the American Institute of Certified Public Accountants, which reserves all rights.

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 Benefits Administration Platform (the "System") for the period of October 1, 2023 to September 30, 2024 (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* (With Revised Points of Focus – 2022) (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"). The Company's objectives for the system in applying the applicable trust services criteria and the HIPAA criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria and the HIPAA 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*.

The Company uses various subservice organizations to support the bswift Platform as described in the *Subservice Organizations* section of Section III of this report. 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 *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.

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 and the HIPAA 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 Benefits Administration Platform (the "System") for the period of October 1, 2023 to September 30, 2024 (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* (With Revised Points of Focus – 2022) (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 is a leading provider of benefits administration technology, offering comprehensive, cloud-based solutions that simplify and streamline the complexities of employee benefits. The bswift platform empowersemployers, brokers, and health plans to efficiently manage the full spectrum of benefits administration, from open enrollment through ongoing management and compliance.

The Platform provides a seamless experience, enabling users to easily navigate health and wellness plans and various employee benefits and point solutions. The Platform integrates advanced technology with a user-friendly interface to make benefits enrollment, education, and management more accessible for all stakeholders. By automating administrative tasks, reducing errors, and offering real-time data analytics, bswift helps to enhance decision making, improve employee engagement, and control an organization's costs.

Key Services:

1. **Benefits Enrollment**: A streamlined, intuitive platform that simplifies the open enrollment process, allowing employees to easily select and manage health, dental, vision, and other insurance benefits.
2. **Eligibility and Compliance Management**: Robust tools to track employee eligibility for benefits and support compliance with federal regulations such as the Affordable Care Act (ACA).
3. **Data Analytics and Reporting**: Access to real-time data insights, allowing Human Resources (HR) professionals and administrators to make informed decisions regarding employee benefits and overall organizational health.
4. **Employee Self-Service**: A user-friendly interface where employees can access information, review their benefit options, and manage selections all in one place.
5. **Carrier Connectivity**: Secure and efficient data exchange with insurance carriers to provide seamless communication and accurate administration of benefits.

With a commitment to innovation and customer service, bswift helps support organizations in delivering comprehensive benefits experiences that drive employee satisfaction while optimizing administrative processes.

C. System Overview

1. bswift Platform

The scope of this report is limited to the bswift Platform, which streamlines human resources and benefits administration for customers.

2. Infrastructure and Databases

The bswift Platform is hosted on Amazon Web Services (AWS), utilizing a combination of both server-based and serverless infrastructure to provide scalability, flexibility, and high availability. AWS provides comprehensive physical security and environmental controls, as detailed in the *Subservice Organizations* section.

This hybrid approach of server and serverless technologies ensures bswift's platform remains resilient, cost-effective, and adaptable to evolving business needs while maintaining the highest security standards.

Systems Overview	Purpose
AWS EC2	Virtual machines
AWS S3	Scalable cloud storage
AWS WAF	Web Application Firewall
Microsoft SQL Database	Core server operating system and relational database management for production databases
Azure Entra ID	Identity access management and Single Sign-On (SSO) for infrastructure and related supporting software tools
Microsoft Azure	Platform-as-a-Service 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
Company-owned devices (Laptops)	WindowsOS

D. Principal Service Commitments and System Requirements

bswift has implemented comprehensive processes and procedures for its Platform to help ensure fulfillment of its operational objectives. Those objectives are grounded in the service commitments made to user entities, as well as the laws and regulations that govern the provision of the services. Additionally, the objectives are shaped by the operational and compliance requirements that bswift has established to support its services.

The Company's commitments to security, availability, processing integrity, confidentiality, and privacy are clearly documented and communicated through executed contracts and service descriptions. These commitments are standardized and include, but are not limited to, the following principles:

- **Security**: The system is designed with security at the core, ensuring that users can access the information necessary, while restricting access to only the information needed.
- **Availability**: bswift ensures the uptime and availability of production systems to meet service level agreements.

- **Processing Integrity**: Data is processed accurately, completely, and in a timely manner, maintaining the integrity of critical operations.
- **Confidentiality**: Encryption technologies are used to protect confidential data, both at rest and in transit, safeguarding sensitive information.
- **Privacy**: Personal information is protected throughout its lifecycle, covering its collection, use, retention, disclosure, and disposal in compliance with applicable laws and regulations.

bswift also has operational requirements that align with the Company's commitments to security, availability, processing integrity, confidentiality, and privacy. These requirements are designed to support service level agreements (SLAs), comply with relevant legal frameworks, and meet other system requirements. These commitments are communicated through the Company's policies, procedures, system design documentation, and customer contracts.

The Company's information security policies outline an organization-wide strategy for safeguarding systems and data. These policies cover key areas such as service design and development, system operations, the management of internal business systems and networks, and employee onboarding and training. bswift's management remains proactive in monitoring regulatory and market changes that may impact the services.

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 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.
P 2.1	The entity communicates choices available regarding the collection, use, retention, disclosure, and disposal of personal information to the data subjects and the consequences, if any, of each choice. Explicit consent for the collection, use, retention, disclosure, and disposal of personal information is obtained from data subjects or other authorized persons, if required. Such consent is obtained only for the intended purpose of the information to meet the entity's objectives related to privacy. The entity's basis for determining implicit consent for the collection, use, retention, disclosure, and disposal of personal information is documented.	N/A – The Company is not a data controller. User Entities are responsible for the choice, consent, and collection related to the data subjects. Therefore, these criteria are not applicable.

Security, Availability, Processing Integrity, Confidentiality, and Privacy Trust Services Categories		
Non-Applicable Trust Services Criteria		**bswift's Rationale**
P 3.1	Personal information is collected consistent with the entity's objectives related to privacy.	
P 3.2	For information requiring explicit consent, the entity communicates the need for such consent, as well as the consequences of a failure to provide consent for the request for personal information and obtains the consent prior to the collection of the information to meet the entity's objectives related to privacy.	
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	

Security, Availability, Processing Integrity, Confidentiality, and Privacy Trust Services Categories		
Non-Applicable Trust Services Criteria		**bswift's Rationale**
	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

bswift 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, 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)	The Company uses AWS' Elastic Compute Cloud (EC2) for its cloud computing services in an Infrastructure-as-a-Service environment for the third-party 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 uses the AWS Simple Storage (AWS S3) as a Platform-as-a-Service, more specifically a Database-as-a-Service. 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;	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*

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
	• Controls over managing the Platform-as-a-Service components for AWS S3 such as physical servers and operating systems including applying critical patching for this infrastructure; • Controls over AWS 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 AWS S3 Platform components as applicable. 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; • Data restore testing is performed on at least a quarterly basis to verify the integrity of the backup data; • bswift IT operations monitors the network and website for security threats and unusual system activity. Errors are logged, and alerts are generated to notify IT staff when conditions exceed defined threshold settings. Confirmed security events are investigated and resolved. Administrator access to monitoring systems is restricted to appropriate individuals based on job function; and • bswift's production environment is monitored for uptime, latency, utilization, and active services on an ongoing basis, and IT personnel are automatically notified in the event of an incident.	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* P 6.6*
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. The Company also uses the Azure SQL Database, which is a Platform-as-a-Service, more specifically a Database-as-a-Service. The Company also uses Office 365, OneDrive, Entra ID, and Microsoft Defender (MS Defender) Software-as-a-Service. The Company also uses MS Defender for anti-virus 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	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*

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
	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, Entra ID, and MS Defender Software-as-a-Service components 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; • Data restore testing is performed on at least a quarterly basis to verify the integrity of the backup data; • bswift IT operations monitors the network and website for security threats and unusual system activity. Errors are logged, and alerts are generated to notify IT staff when conditions exceed defined threshold settings. Confirmed security events are investigated and resolved; and Administrator access to monitoring systems is restricted to appropriate individuals based on job function; and • bswift's production environment is monitored for uptime, latency, utilization, and active services on an ongoing basis, and IT personnel are automatically notified in the event of an incident.	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 1.4* PI 1.5* P 4.2* P 4.3* P 6.6*

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
Persistent	The Company uses Persistent as a Managed Services Provider (MSP) for security monitoring and vulnerability management over the Company's network and in-scope production environment, for notifying the Company of potential security issues, for end-user device management, and for Entra ID access management. The following control activities are critical to achieving the Applicable Trust Services Criteria: • Controls over the monitoring of the Company's network and in-scope production environment; • Controls over end-user device management; • Controls over provisioning and de-provisioning the Company's users' Entra ID access in accordance with the Company's requests; • Controls over the monitoring, investigation, and remediation of security issues including notifying the Company of potential security issues; and • Controls over vulnerability management and performing internal vulnerability scanning as well as remediating any identified vulnerabilities. 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; • bswift's production environment is monitored for uptime, latency, utilization, and active services on an ongoing basis, and IT personnel are automatically notified in the event of an incident; and • When an incident related to system security, availability, confidentiality, or privacy is detected or reported, a defined incident management process is initiated by appropriate personnel and includes a root cause analysis and corrective actions implemented. If an incident results in an unauthorized disclosure or use of personal information, documentation of how/if the incident was communicated to affected parties and whether the event resulted in a failure to comply with applicable laws and regulations is documented.	CC 2.1* 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 6.6* CC 6.7* CC 6.8* CC 7.1* CC 7.2* CC 7.3* CC 7.4* CC 7.5* CC 8.1* C 1.2* PI 1.4* P 4.3* P 6.3* 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 Responsibilities

Each user entity must evaluate its own system of internal controls for effective risk management and compliance. The internal controls described in this report occur at and are managed by the Company and only cover a portion of a comprehensive internal control structure relevant to a user entity. Each user entity must address the various aspects of internal control that may be unique to its particular organization. This section highlights those portions of the internal control structure that user entities have responsibility to develop and maintain but should not affect the ability of the Company to achieve its service commitments and system requirements.

User Entity Responsibilities	Associated Criteria
User Entities are responsible for ensuring that the authentication of the bswift 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 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 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 bswift Platform.	PI 1.2
User Entities are responsible for the choice, consent, and collection related to the data subjects.	P 2.1 P 3.1 P 3.2

H. Cross-referencing of the bswift LLC SOC 2 Control Activities to the HIPAA Criteria

Safeguard / Area	HIPAA Security Rule 45 CFR Standard	SOC 2 Control Activity Mapping
Administrative Safeguards	§164.308 Administrative safeguards. (Header)	
Administrative Safeguards	§164.308(a) A covered entity or business associate must, in accordance with §164.306: (Header)	
Administrative Safeguards	§164.308(a)(1)(i) **Standard: Security management process.** Implement policies and procedures to prevent, detect, contain, and correct security violations.	CC 1.1-01
Administrative Safeguards	§164.308(a)(1)(ii) **Implementation specifications:** (Header)	
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 2.1-01
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 2.1-02 CC 2.1-04
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 1.1-02
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 2.1-01 CC 2.1-02 CC 4.2-01
Administrative Safeguards	D **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 1.3-01
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 1.1-01
Administrative Safeguards	§164.308(a)(3)(ii) **Implementation specifications:** (Header)	

Safeguard / Area	HIPAA Security Rule 45 CFR Standard	SOC 2 Control Activity Mapping
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 6.2-01
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 6.2-02
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 6.1-06
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 1.1-01
Administrative Safeguards	§164.308(a)(4)(ii) **Implementation specifications:** (Header)	
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 6.2-02
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 6.1-04 CC 6.2-02
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 1.1-03 CC 1.4-02
Administrative Safeguards	§164.308(a)(5)(ii) **Implementation specifications. Implement:** (Header)	
Administrative Safeguards	§164.308(a)(5)(ii)(A) **Security reminders (Addressable).** Periodic security updates.	CC 5.2-07

Safeguard / Area	HIPAA Security Rule 45 CFR Standard	SOC 2 Control Activity Mapping
Administrative Safeguards	§164.308(a)(5)(ii)(B) **Protection from malicious software (Addressable).** Procedures for guarding against, detecting, and reporting malicious software.	CC 2.1-02 CC 2.1-03 CC 6.8-01
Administrative Safeguards	§164.308(a)(5)(ii)(C) **Log-in monitoring (Addressable).** Procedures for monitoring log-in attempts and reporting discrepancies.	CC 2.1-04 CC 6.6-01
Administrative Safeguards	§164.308(a)(5)(ii)(D) **Password management (Addressable).** Procedures for creating, changing, and safeguarding passwords.	CC 6.1-06 CC 6.1-09
Administrative Safeguards	§164.308(a)(6)(i) **Standard: Security incident procedures.** Implement policies and procedures to address security incidents.	CC 1.1-01 CC 4.2-01
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 1.1-01 CC 4.2-01
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 7.4-01 CC 7.5-02
Administrative Safeguards	§164.308(a)(7)(ii) **Implementation specifications:** (Header)	
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 7.4-01
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 7.4-01 CC 7.5-02
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 7.5-02
Administrative Safeguards	§164.308(a)(7)(ii)(D) **Testing and revision procedures (Addressable).** Implement procedures for periodic testing and revision of contingency plans.	CC 7.5-02
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 7.5-02

Safeguard / Area	HIPAA Security Rule 45 CFR Standard	SOC 2 Control Activity Mapping
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 1.1-01 CC 1.3-02
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 1.3-03
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 1.3-03
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 1.3-03
Physical Safeguards	§164.310 Physical safeguards. (Header)	
Physical Safeguards	§164.310 A covered entity or business associate must, in accordance with §164.306: (Header)	
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:** (Header)	
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 7.5-02

Safeguard / Area	HIPAA Security Rule 45 CFR Standard	SOC 2 Control Activity Mapping
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.
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 1.1-01
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:** (Header)	
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 6.5-01
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.

Safeguard / Area	HIPAA Security Rule 45 CFR Standard	SOC 2 Control Activity Mapping
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. (Header)	
Technical Safeguards	§164.312 A covered entity or business associate must, in accordance with §164.306: (Header)	
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 1.1-01 CC 6.1-14 CC 6.2-02
Technical Safeguards	§164.312(a)(2) **Implementation specifications:** (Header)	
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 5.2-02 CC 5.2-03 CC 5.2-16
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 7.5-02
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 6.1-08
Technical Safeguards	§164.312(a)(2)(iv) **Encryption and decryption (Addressable).** Implement a mechanism to encrypt and decrypt electronic protected health information.	CC 6.1-01 CC 6.1-02 CC 6.1-04 CC 6.7-01
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 2.1-04
Technical Safeguards	§164.312(c)(1) **Standard: Integrity.** Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	CC 1.1-01 CC 6.2-01 CC 6.2-02 CC 6.5-01 CC 6.7-01
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 2.1-04 CC 5.2-16

Safeguard / Area	HIPAA Security Rule 45 CFR Standard	SOC 2 Control Activity Mapping
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.
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 5.2-16 CC 6.6-01 CC 6.7-01
Technical Safeguards	§164.312(e)(2) **Implementation specifications:** (Header)	
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 5.2-16 CC 6.6-01 CC 6.7-01
Technical Safeguards	§164.312(e)(2)(ii) **Encryption (Addressable).** Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	CC 6.1-01 CC 6.7-01
Organizational Safeguards	§164.314 Organizational requirements. (Header)	
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 1.3-03
Organizational Safeguards	§164.314(a)(2) **Implementation specifications (Required).** (Header)	
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. (Header)	
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 1.3-02 CC 1.3-03
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 1.3-02 CC 1.3-03
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 1.3-03

Safeguard / Area	HIPAA Security Rule 45 CFR Standard	SOC 2 Control Activity Mapping
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 1.3-03
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. (Header)	
Organizational Safeguards	§164.316 A covered entity or business associate must, in accordance with §164.306: (Header)	

Safeguard / Area	HIPAA Security Rule 45 CFR Standard	SOC 2 Control Activity Mapping
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 1.1-01 CC 1.1-03 CC 1.3-01
Documentation Safeguards	§164.316(b)(1) **Standard: Documentation.** (Header)	
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 1.1-01 CC 1.3-01
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 1.1-01 CC 1.1-03 CC 1.3-01
Documentation Safeguards	§164.316(b)(2) **Implementation specifications:** (Header)	
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 6.5-01
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 1.1-02 CC 1.1-03 CC 1.1-05 CC 1.3-01
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 1.3-01 CC 2.1-01


Aprio