Statement on Security and Privacy

May 2024

Purpose

At RxBenefits, the security and privacy of the information we are entrusted with is of the highest importance to us. As technology advances, so do the threats organizations face on a consistent basis. RxBenefits has taken the necessary steps to create, and continuously improve, a robust and comprehensive Information Security program.

This document provides a high-level overview of the steps we have taken to ensure that the information we encounter remains secure and private.

RxBenefits, Inc.
3700 Colonnade Pkwy, #600
Birmingham, AL 35243

General Oversight

Quarterly HIPAA Training

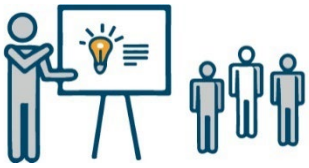
All RxBenefits employees are required to complete quarterly Security and HIPAA training. This training covers HIPAA Security Rule, HIPAA Privacy Rule, and Information Security best practices.

Continuous Phishing Education

On a continuing basis, our phishing platform disperses a randomized phishing campaign to all RxBenefits employees. If the user fails by clicking a link or opening an attachment, they are directed to take required training.

Employee Onboarding – Security Training

New employees coming into RxBenefits are required to take assigned security and HIPAA training promptly after their start date. This training provides new employees an overview of security best practices and expectations when working at RxBenefits.



Security Governance

RxBenefits maintains a formal documented security policy, approved by management, consistent with industry best practice frameworks. Additionally, we undergo an annual audit for both SOC1 Type 2 and SOC2 Type 2 (SSAE-18) attestations.

Risk Management

RxBenefits maintains a formal, documented risk management policy and procedure to address risks within the organization. This process includes the annual assessment of third-party relationships, enterprise risk identification and treatment, and annual assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI.

Compliance

To ensure that RxBenefits abides by applicable regulatory requirements and federal/state laws, we have dedicated individuals to handle compliance related activities. These individuals also monitor changes within the regulatory or legal environment and ensure we remain compliant.

RxBenefits, Inc.
3700 Colonnade Pkwy, #600
Birmingham, AL 35243

Data Security

Anti-virus & Malware Protection

RxBenefits' utilizes market leading software for Endpoint Detection & Response (EDR). Agents are installed on all servers and workstations and signatures are updated nightly.

Secure Authentication

All external access to RxBenefits' network environment utilizes Multi-Factor Authentication (MFA). Passwords follow National Institute of Standards and Technology (NIST) guidelines for minimum length, complexity, and periodic password changes. Single sign on (SSO) is leveraged for key applications.

Encryption

Employees are trained that all emails containing PHI must be encrypted. In addition, the email gateway inspects emails before leaving the domain and automatically encrypts if PHI is detected.

Servers containing PHI are encrypted at rest with AES-256 encryption. File transfers only occur using SFTP.

Logging and Monitoring

All logs are enabled on systems including critical assets and feed into our security information and event management (SIEM) system. System logs are monitored 24x7x365 through a combination of in-house and managed services.

Vulnerability and Patch Management

All systems within RxBenefits are patched at regular intervals. In the event of a critical vulnerability being detected, the patch will be distributed as quickly as possible. Various channels are used to receive alerts of new vulnerabilities that may affect the information assets within RxBenefits.

RxBenefits, Inc.
3700 Colonnade Pkwy, #600
Birmingham, AL 35243

Data Privacy

Data Location

All data housed at RxBenefits resides within the United States.

Data is not stored in India as part of our Global Operations Center location.

PHI Confidentiality

RxBenefits uses a minimum necessary approach to access to PHI and other sensitive information. Additionally, we ensure that all contractual agreements are followed and fully honored with respect to whom may have access to PHI held in our possession.

All subcontractors that will interact with ePHI must have an executed BAA and continue to meet the security/privacy requirements determined by RxBenefits.

Breach Notification

RxBenefits has processes to ensure that, in the event a breach was to occur, proper steps are taken to immediately rectify the breach, mitigate damages, and notify the covered entity per regulatory (e.g., OCR) and contractual requirements.

Organizational Resiliency

Business Continuity

RxBenefits has procedures in place to continue business operations when faced with an adverse event. In the event the corporate office is affected, employees have the capability to perform their job duties remotely.

Back-ups & Disaster Recovery

RxBenefits maintains, and annually tests, a formal Disaster Recovery Plan. In the event of a system failure or disruption, our Disaster Recovery Plan involves a failover to our backup data center. Backups are taken hourly and pushed offsite nightly, no portable media (e.g., Tapes) are used in this process. Offsite backup storage is encrypted at rest.

Incident Response

RxBenefits' has an established Incident Response Plan that is updated and tested annually. This Plan consists of assigned roles and responsibilities for team members, along with necessary emergency contact information. Results of the annual tabletop exercise are used to enhance and strengthen the plan.

RxBenefits, Inc.
3700 Colonnade Pkwy, #600
Birmingham, AL 35243

Security & Privacy for Global Operations Center

RxBenefits' has an established Global Operations Center (GOC) located in Hyderabad, India. Employees at this location are expected to follow all RxBenefits information security and privacy guidelines while performing their job duties as additional support for our internal operations.

The following is being implemented in addition to the controls mentioned above in this document to ensure the security and privacy of sensitive information and internal resources. These controls apply to the processes and personnel of the Global Operations Center (GOC).

Secure Connectivity

Employees at the Global Operations Center are required to access their dedicated virtual machines within our US-based AWS Workspaces environment through the RxBenefits managed secure connection.

Endpoint Protection

Employees at the Global Operations Center use endpoint devices that are protected and controlled by the same internal controls that apply to our US-based devices.

Training & Awareness

Information security and HIPAA training must be completed by all newly hired employees of the Global Operations Center and quarterly thereafter.

RxBenefits, Inc.
3700 Colonnade Pkwy, #600
Birmingham, AL 35243