A-LIGN

A-LIGN.com

Type 2 SOC 3

Prepared for:
GoodRx, Inc.

Year:
2025

GoodRx

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

November 1, 2024 to October 31, 2025

Table of Contents

SECTION 1

ASSERTION OF GOODRX, INC. MANAGEMENT

ASSERTION OF GOODRX, INC. MANAGEMENT

December 4, 2025

We are responsible for designing, implementing, operating, and maintaining effective controls within GoodRx, Inc.'s ('GoodRx' or 'the Company') Drug Savings Platform throughout the period November 1, 2024 to October 31, 2025, to provide reasonable assurance that GoodRx'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*, in AICPA, *Trust Services Criteria*, and GoodRx's compliance with the commitments in its Privacy Notice. Our description of the boundaries of the system is presented below in "GoodRx, Inc.'s Description of Its Drug Savings Platform throughout the period November 1, 2024 to October 31, 2025" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period November 1, 2024 to October 31, 2025, to provide reasonable assurance that GoodRx's service commitments and system requirements were achieved based on the trust services criteria. GoodRx'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 are presented in "GoodRx, Inc.'s Description of Its Drug Savings Platform throughout the period November 1, 2024 to October 31, 2025".

GoodRx uses Amazon Web Services ('AWS' or 'subservice organization') to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at GoodRx, to achieve GoodRx's service commitments and system requirements based on the applicable trust services criteria and GoodRx's compliance with the commitments in its Privacy Notice.The description presents GoodRx's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of GoodRx's controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve GoodRx's service commitments and system requirements based on the applicable trust services criteria and GoodRx's compliance with the commitments in its Privacy Notice. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of GoodRx's controls.

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 period November 1, 2024 to October 31, 2025 to provide reasonable assurance that GoodRx's service commitments and system requirements were achieved based on the applicable trust services criteria and GoodRx's compliance with the commitments in its Privacy Notice, if complementary subservice organization controls and complementary user entity controls assumed in the design of GoodRx's controls operated effectively throughout that period.

Kate O'Kelly

Kate O'Kelly
Senior Director, Security and Compliance
GoodRx, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To GoodRx, Inc.:

Subject

We have examined GoodRx, Inc.'s ('GoodRx' or 'the Company') accompanying assertion titled "Assertion of GoodRx, Inc. Management" (assertion) that the controls within GoodRx's Drug Savings Platform were effective throughout the period November 1, 2024 to October 31, 2025, to provide reasonable assurance that GoodRx'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*, in AICPA *Trust Services Criteria*, and GoodRx's compliance with the commitments in its Privacy Notice.

GoodRx uses Amazon Web Services ('AWS' or 'subservice organization') to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at GoodRx, to achieve GoodRx's service commitments and system requirements based on the applicable trust services criteria and GoodRx's compliance with the commitments in its Privacy Notice. The description presents GoodRx's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of GoodRx'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 description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at GoodRx, to achieve GoodRx's service commitments and system requirements based on the applicable trust services criteria and GoodRx's compliance with the commitments in its Privacy Notice The description presents GoodRx's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of GoodRx's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

GoodRx 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 GoodRx's service commitments and system requirements were achieved. GoodRx has also provided the accompanying assertion (GoodRx assertion) about the effectiveness of controls within the system. When preparing its assertion, GoodRx is responsible for selecting, and identifying in its assertion, the applicable trust services criteria, for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system, and complying with the commitments in its Privacy Notice.

.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that 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 its compliance with the commitments in its Privacy Notice. Our examination was conducted in accordance with attestation standards established by the AICPA. 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 description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria

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

Independence and Ethical Responsibilities

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

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 are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating 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.

Opinion

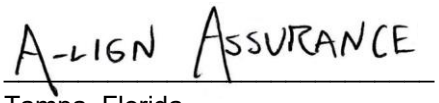
In our opinion, management's assertion that the controls within GoodRx's Drug Savings Platform were suitably designed and operating effectively throughout the period November 1, 2024 to October 31, 2025, to provide reasonable assurance that GoodRx's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of GoodRx's controls operated effectively throughout that period.

The SOC logo for Service Organizations on GoodRx's website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of GoodRx, user entities of GoodRx's Drug Savings Platform during some or all of the period November 1, 2024 to October 31, 2025, business partners of GoodRx subject to risks arising from interactions with the Drug Savings Platform, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

This report is not intended to be, and should not be, used by anyone other than these specified parties.



Tampa, Florida
December 4, 2025

SECTION 3

GOODRX, INC.'S DESCRIPTION OF ITS DRUG SAVINGS PLATFORM THROUGHOUT THE PERIOD NOVEMBER 1, 2024 TO OCTOBER 31, 2025

OVERVIEW OF OPERATIONS

Company Background

GoodRx is the leading platform for medication savings in the U.S., used by nearly 30 million consumers and over one million healthcare professionals annually. Uniquely situated at the center of the healthcare ecosystem, GoodRx connects consumers, healthcare professionals, payers, pharmacy benefit managers, pharmaceutical manufacturers, and retail pharmacies to make saving on medications easier. By reducing friction and inefficiencies, GoodRx helps consumers save time and money when filling prescriptions so they can get the care they deserve.

Description of Services Provided

Located in Santa Monica, California, GoodRx provides a website and mobile application that identifies prescription drug prices and offers coupons for adjudication in the United States. GoodRx gathers current information about prices from pharmacies across the United States and tracks discounts to help customers find the least expensive local pharmacy for their prescriptions. GoodRx also provides a subscription program called GoodRx Gold via website and mobile applications that allow customers to access even greater prescription discounts at select pharmacies.

Principal Service Commitments and System Requirements

Legal Commitments

GoodRx has committed to complying with law in the provision of its services. Customer commitments are outlined through their Terms & Conditions.

Contractual Commitments

GoodRx executes contracts with its clients to ensure that the scope of services provided is defined. The organization defines service commitments on a per-client basis.

System Design

GoodRx designs its prescription price comparison system to meet its legal and contractual commitments. These commitments are based on the services that GoodRx provides to its clients, the laws and regulations that govern the provision of those services, and the financial, operational, and compliance requirements that GoodRx has established for its services. GoodRx establishes operational requirements in its system design that support the achievement of its legal and contractual commitments. These requirements are communicated in GoodRx's system policies and procedures, system design documentation, and contracts with clients.

Components of the System

Infrastructure

GoodRx maintains documented network diagrams that illustrate the company architecture. The organization uses software to generate network diagrams based on the AWS network infrastructure. Enterprise clients are isolated from the customer clients within an isolated Virtual Private Cloud (VPC).

GoodRx maintains a system inventory that captures the device name, device type, vendor, Operating System (OS), and location. AWS built-in functionality is used to manage and monitor its system inventory, which is automatically updated as resources are created and removed. Device inventories are maintained electronically via Mobile Device Management (MDM) solutions.

Software

Primary software used to provide GoodRx's Drug Savings Platform includes the following:

Primary Software		
Organization	**Technology Process / Layer**	**Summary**
AWS	Virtual Infrastructure	AWS provides a virtual infrastructure, including operating system and database components, to process, store and maintain pricing and claims data through the deployment of various services such as S3, RDS, Redshift, and EC2
Fastly	Content Delivery	Fastly is a Content Delivery Network (CDN) that fronts GoodRx's public-facing domains and provides caching and security protections
Google Workplace (G Suite)	Account Provisioning	Google Workplace provides workplace collaboration for GoodRx Personnel through a suite of cloud productivity applications and e-mail hosting
GitHub	Code Hosting	GitHub is a cloud based distributed version control and source code management service. GoodRx manages multiple code repositories which support multiple parts of core business processes
Looker	Business Intelligence Platform	Looker is a Business Intelligence (BI) solution that is used to generate dashboards to track various pricing, claims, and spend activity across GoodRx. Access is managed following GoodRx's Account Management & Access Control Policy
Okta	Single Sign-on (SSO)	Okta is an identity management service which is leveraged for creating identity federations and SSO capabilities to cloud applications in GoodRx's environment. Access to Okta is administered by the GoodRx IT Team and aligns to the corporate Password Policy
OneTrust	Data Privacy and Governance	OneTrust is a cloud compliance platform that enables data deletion and summary program
Stripe	Payment Processing	Stripe is a Payment Processing solution that is used to receive payments for the GoodRx Care Telemedicine, and Gold Business lines at GoodRx. Access is managed following GoodRx's Account Management & Access Control Policy
SumoLogic	Log Management	SumoLogic Security Information and Event Management (SIEM) is a logging tool for monitoring and troubleshooting, used by GoodRx's Security & Engineering Teams

People

GoodRx maintains a hierarchical structure that is separated into distinct, functional areas to ensure business efficiency and segregation of duties. The organization has established lines of authority throughout the company to ensure that departments have the appropriate level of oversight. Senior Vice Presidents / C-level executives oversee each business line and report to the Chief Executive Officer (CEO).

The Board of Directors has also been established to provide oversight functions, additionally, the Audit & Risk Committee, Compensation Committee, and Nominating and Corporate Governance Committee exist to supplement the board's expertise. An organization chart is maintained to illustrate the corporate structure, including leadership, reporting lines, and separation of reporting duties.

Data

The Data Retention Policy and Procedure requires that the organization retain data based on tier designation. The organization maintains a Data Classification Policy that classifies data according to the following levels:

- Public Information
- Confidential Information
- Highly Confidential Information

The organization has controls in place to ensure that application service transactions are protected. In each request a secure token is generated, and the organization uses secure tokens to protect against Cross-Site Request Forgery (CSRF) attacks. The organization uses best practices for deploying its encryption methods (e.g., Transport Layer Security (TLS).

GoodRx handles claims data related to customers' use of a prescription coupon for the GoodRx and GoodRx Gold customer lines.

Privacy Commitments

The following table describes the information included as part of the Drug Savings Platform of GoodRx:

Client Data	Reporting
• Name, date of birth, and demographic information (e.g., age, gender, etc.) • Home, work, billing, and/or shipping addresses • E-mail address • Home and/or mobile phone number • Health, prescription, pharmacy, and related information • Web Behavior Information **Note:** E-mail address, or mobile phone number are only required for an account (e.g., in connection with GoodRx Gold) and not for coupons.	• General pricing, location, and access information related to drugs and medications

Notice and Communication of Objectives Related to Privacy

GoodRx maintains privacy policies on its website that communicate privacy objectives to its customers. The general privacy policy addresses how information is collected and used. The general privacy policy applies to customers that have agreed to use GoodRx services, and this policy covers the GoodRx website and mobile apps.

Choice and Consent

Customers provide information to the organization based on agreed-upon services. Customers enrolled in GoodRx Gold may be expected to provide additional information than members who use the general GoodRx service. The privacy policy states that GoodRx uses data collected, including data linked to a customer's name and contact information to fulfill services, and the services used dictates the amount of personal information the customer provides.

Collection

Personal information is collected in accordance with the privacy policy. GoodRx collects most information directly from its users, and such collection is in accordance with the privacy policy. When GoodRx collects information from third-parties, its contracts' language ensures that the third-party is collecting information lawfully.

Use, Retention, and Disposal

The privacy policies define the limits on how personal information is used. The organization retains customer records based on internal policies and contractual and/or regulatory requirements and applies retention as applicable. The Audit and Logging Policy addresses the requirement for the organization to log actions related to data access, for audit logs showing the date and time such data is accessed, and log storage.

The Data Retention Policy and Procedure addresses object reuse and disposal. The policy specifies that the organization uses appropriate disposal procedures to securely destroy, delete, or otherwise archive Confidential Information and Highly Confidential Information. GoodRx enlists shred services to securely shred its paper media and receives a certificate of destruction once documents are destroyed. The organization also completely cleans any electronic media before it is made available for reuse.

Access

When customers create accounts on GoodRx and GoodRx Gold, they can see on their accounts certain personal information is stored. GoodRx (and GoodRx Gold) accounts require password-less authentication that sends real-time login credentials to the applicable e-mail or Short Message Service (SMS) number. GoodRx may also receive communication information provided by visitors, such as e-mail addresses and phone numbers. Recipients of communications may unsubscribe from e-mails by clicking a link in the e-mails and may unsubscribe from texts by texting "stop." If users wish to access a summary or delete their data, they can navigate to the GoodRx privacy portal and complete a request for data to be deleted or summarized and sent to the user. GoodRx provides deletion options to GoodRx customers and data access options for users in accordance with applicable law.

Disclosure and Notification

The Data Classification Policy and Procedure addresses the processes and requirements for disclosing personal information. Per policy, the disclosure of personal information can only occur when the appropriate agreement is in place, and workforce members ensure that there is an appropriate confidentiality agreement in place prior to disclosing sensitive data or confidential information. GoodRx communicates instances when the organization does share personal information in its privacy policy. The organization maintains an inventory that documents whether personal information is shared with specific third-parties.

Potential unauthorized disclosures of information are documented as part of the incident response procedures. The organization has formally documented policies that define requirements for documenting a breach. The security official role is satisfied by the Sr. Director of Security and Compliance. The Legal Team and Security Team is responsible for investigating occurrences of unauthorized disclosures and breaches. As applicable, the Business Associate Agreement (BAA) and/or data processing agreement that GoodRx enters into with covered entities or third-parties requires that the organization notify relevant individuals about breaches. The Incident Response procedure governs the communication process in response to a breach and dictates that the organization notifies appropriate parties in compliance with its contractual obligations and/or applicable law.

GoodRx establishes mutual Non-Disclosure Agreements (NDAs), data protection addendums and BAAs with third-parties that have access to confidential information, personal information, or protected health information, as applicable. These agreements contain strict limitations on the use and disclosure of data, obligations to maintain appropriate safeguards, and requirements to report and remediate any security incidents or data breaches in accordance with applicable law and company policies.

The organization has a process for providing data subjects with an inventory of personal information held. The Patient Advocacy Escalation Guidelines has formally documented processes for responding to privacy-related requests. Additionally, the Data Subject Privacy Rights Management Policy defines processes for providing customers with a disclosure of information held by the organization for the data subject.

Quality

Customers that use the organization's applications are responsible for ensuring that the information provided is accurate and updated. Some of the information for the organization's customer line of business is collected directly from the customer, who is responsible for providing accurate information. Customers have the ability to access certain information in the GoodRx applications and edit information as needed to ensure that it remains current.

Monitoring and Enforcement

Customers are provided a process through which to escalate inquiries, complaints, and disputes to appropriate personnel. For the organization's customer line of business, the Patient Advocacy Team is the first point of contact for any inquiries, complaints, and disputes, and the Patient Advocacy Team members are trained to escalate issues as appropriate. The contact form is available on the organization's website, where users can submit inquiries, complaints, and disputes. The website also has a phone number posted that users can call to communicate issues.

Processes, Policies and Procedures

Management has developed and communicated policies and procedures to guide the provision of the organization's services. These are reviewed on an annual cadence within the calendar year and any changes required are authorized by management. These cover the following key security life cycle areas:

- Data classification
- Categorization of information
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls

- Performance of annual management self-assessments to assess security controls
- Authorization, changes to, and termination of information system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup storage
- Incident response
- Maintenance of restricted access to system configurations, user functionality, master passwords, and security devices

Physical Security and Environmental Controls

The in-scope system and supporting infrastructure is hosted by AWS. As such, AWS is responsible for the physical security and environmental safeguard controls for the in-scope system. Refer to the 'Subservice Organizations' section below for controls managed by AWS.

Logical Access

The Account Management and Access Control Policy documents the process for the granting of access to systems. GoodRx uses ServiceNow to document the access-authorization process and the granting of access rights. The organization authorizes access based on the principle of least privilege and conducts quarterly user access reviews to ensure that only necessary personnel retain access that is appropriate for their daily job role and responsibilities. For each system, the system owner is responsible for authorizing access. The Account Management and Access Control Policy requires a unique identifier for any person that accesses the AWS administrative control panel; the policy defines use cases for shared accounts.

GoodRx uses Okta as its primary logical access control systems. The organization maintains a Password Policy that defines password composition requirements, which are based on NIST 800-63B password guidelines, and these requirements are enforced in Okta for applications in the GoodRx environment. Okta requires that passwords have a minimum of at least 12 characters, and require a combination of letters, numbers, and symbols.

Users are required to use phishing-resistant Multifactor Authentication (MFA) when accessing company systems. The Password Policy requires that Personnel use MFA to access Managed Systems. GoodRx uses Okta federation for accessing the AWS environment, and Okta systematically enforces phishing resistant MFA, which is documented within GoodRx policies.

The Account Management and Access Control Policy defines SLAs for revocation of access upon termination, for both voluntary and involuntary use cases. The revocation process is completed using the termination checklist.

GoodRx has a process in place for clients to register and deregister to/from online services. Clients can self-register for customers GoodRx and GoodRx Gold through the appropriate member-facing website. Users can cancel their own account, or they can contact the GoodRx Customer Support Team to cancel their account.

Computer Operations - Backups

The Business Continuity and Disaster Recovery Policy and Procedure which address plans to maintain or restore operations and ensure availability of information following an interruption of critical business processes. The document addresses:

- Recovery response teams
- List of critical components and software
- Notifications and team responsibilities
- Requirements to retain evidence of Business Continuity Plan maintenance
- Management approval

- Conditions for activating the plan
- Awareness and education activities
- Test schedule

Data used to provision GoodRx's services is stored in AWS; however, workforce members may access and work with such data via managed devices (e.g., endpoints).

AWS backups are configured to capture daily backups.

The Technical Operations Team coordinates with personnel and data providers to minimize interruption of services, if any. The recovery process may include assessing the cause and extent of the service disruption, notifying clients and users of the service disruption, and working with server hosts and data providers to provide interim services to users as well as to restore the full extent of services. The organization has defined Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) based on application recovery tiers to ensure that they align with the organization's Service Level Agreement (SLA) requirements.

Refer to the 'Subservice Organizations' section below for additional details on controls that are the responsibility of AWS.

Computer Operations - Availability

Problem Management

GoodRx maintains an Incident Response Policy and Procedure that addresses the organization's response processes to alerts received from the security systems. Incidents are captured in the Security Incident Reporting Form to document critical incident details. As appropriate, the team also uses the Breach Determination Form to determine if an incident rises to the level of breach as defined by HIPAA and to ensure compliance with any HIPAA breach reporting obligations, to the extent applicable.

The Incident Response Policy and Procedure outlines the requirements for responding to security alerts generated by the organization's monitoring and detection systems. Alerts from these systems are routed to multiple destinations to ensure broad visibility and prompt action. High-priority alerts are escalated to the appropriate engineering or security operations leads for review and response. Team members with incident response responsibilities participate in periodic tabletop exercises to confirm their understanding of procedures and roles during a security event.

GoodRx has processes in place to ensure that customers can submit information about complaints and security breaches. For the organization's customer line of business, customers are provided contact information through the company website.

System Monitoring

Various systems are used to log and monitor data at GoodRx. The following tools are in place:

- Sumo Logic is employed as a log aggregator ingesting error logs, security logs, corporate Palo Alto Firewall logs, web access logs, Virtual Private Network (VPN) access logs, and web logs with log retention of one year
- Datadog is employed for application performance monitoring with PagerDuty alerts to engineers

Monitoring alerts are delivered to a dedicated Slack channel. Network logging is implemented across the entire infrastructure.

The organization uses AWS' Auto-Scaling service to manage capacity planning of production instances. Auto-scaling configurations can be adjusted as needed to manage expected traffic and then used to spin up (or down) additional Elastic Cloud Compute (EC2) instances when traffic exceeds or sinks below projections. Hosts that are spun up by auto-scaling services are automatically added to the defined load balancer. Monitoring of these instances is conducted with CloudTrail and Datadog.

The GoodRx headquarters in Santa Monica and the satellite offices in San Francisco and New York use Palo Alto next generation firewalls. Uniform Resource Locator (URL) Filtering and other monitoring controls are used to monitor Internet bound traffic from the Santa Monica office and remote users connected to the Prisma Cloud VPN service. Detection and protection definitions and updates are automatically deployed by Palo Alto.

Refer to the 'Subservice Organizations' section below for additional details on controls that are the responsibility of AWS.

Change Control

Change Management

GoodRx has implemented a SDLC and Change Management Policy to manage change requests, reviews, approvals, and implementation. The organization uses GitHub to document change requests, which are linked to Jira tickets. Changes are authorized prior to deployment to production; the creator of the change request is not permitted to approve the change. Change deployments are appropriately communicated to internal personnel via Slack channels. The change process includes the following attributes:

- Clearly identified roles and responsibilities
- Impact of the change request
- Testing prior to implementation of change
- Authorization and approval
- Post-installation validation
- Back-out or recovery plans

System configuration standards are formally documented and implemented to ensure that systems are consistently and properly hardened. The organization uses AWS and Center for Internet Security (CIS) best-practices hardening standards as the basis for its system configuration standards. Configuration standards are updated with critical security updates and regular updates to ensure that the latest security threats are addressed.

Personnel responsible for system configurations stay knowledgeable of appropriate ways to securely configure the organization's systems. Personnel review current AWS documents; subscribe to industry publications, social media feeds of researchers, and security organizations; and attend industry conferences, where security topics and best practices are discussed.

Application Development

GoodRx develops applications to support its business model. GoodRx has separate development and production environments and uses the DevOps methodology, continuous deployment, and automated tools to manage its deployment processes.

For changes to the web application code, GoodRx requires peer code review to ensure that quality code is committed to the code base. GoodRx also uses Snyk for static analysis of web application code. GoodRx uses a bug bounty program hosted through HackerOne to work with and reward researchers who find bugs that make it out to production. In addition, GoodRx has an internal Security Team which provides various ad-hoc tests as needed to ensure quality and security.

GoodRx source code is stored in a private GitHub repository. Access to the repository is invite-only and is managed by engineering leads. Personnel accounts are also required to use phishing resistant MFA for access. In addition to being a code repository, GitHub is also used for version control. The Security Team is alerted of any membership changes to the GitHub organization.

Application Change Management

Changes are managed through the Jira ticketing system with the employment of a Kanban board used to manage the backlog with sprints of two or four weeks. The change process includes the following attributes:

- Change requests, approved by appropriate departmental management, are received by IT personnel and recorded
- Technical specifications are developed for significant changes
- A testing strategy is prepared and followed
- Source code is checked-out or copied to a test or development environment
- Program changes are tested in a separate, controlled environment
- Snyk is employed to check security vulnerabilities
- Appropriate personnel perform the migration of changes to production in a controlled manner
- Back-out procedures are documented

Data Communications

GoodRx enforces firewall configurations to ensure that internal private networks are adequately protected. The organization uses a combination of VPCs and security groups to protect the perimeter of the network.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place.

Penetration testing is conducted to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology specified by GoodRx. The third-party vendor's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications and occurs from both outside (external testing) and inside the network.

Vulnerability scanning is performed by a third-party vendor on a weekly basis in accordance with GoodRx policy. The third-party vendor uses industry standard scanning technologies and a formal methodology specified by GoodRx. These technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis. Scans are performed during non-peak windows. Tools requiring installation in the GoodRx system are implemented through the Change Management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Authorized Personnel may access the system from the Internet through the use of leading VPN technology. Personnel are authenticated through the use of phishing resistant MFA methods.

Boundaries of the System

The scope of the report herein includes the Drug Savings Platform hosted on AWS infrastructure located in the United States only.

This report does not include the cloud hosting services provided by AWS at multiple facilities.

Changes to the System Since the Last Review

No significant changes have occurred to the services provided to user entities since the organization's last review.

Incidents Since the Last Review

No significant incidents have occurred to the services provided to user entities since the organization's last review.

Criteria Not Applicable to the System

All Common/Security, Availability, Processing Integrity, Confidentiality and Privacy criteria were applicable to the GoodRx Drug Savings Platform.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS at multiple facilities.

Subservice Description of Services

AWS is responsible for providing and monitoring physical safeguarding for IT infrastructure to help ensure that unauthorized access to the IT infrastructure does not occur. AWS is also responsible for providing environmental safeguards (e.g.: power supply, temperature control, fire suppression) against certain environmental threats. Additional responsibilities relevant to AWS include managing and monitoring logical access to the underlying network, virtualization management, and storage devices for its cloud hosting services where GoodRx systems reside.

Complementary Subservice Organization Controls

GoodRx's services are designed with the assumption that certain controls will be implemented by the subservice organization. Such controls are called complementary subservice organization controls. It is not feasible for all of the Trust Services Criteria related to GoodRx's services to be solely achieved by GoodRx control procedures. Accordingly, the subservice organization, in conjunction with the services, should establish their own internal controls or procedures to complement those of GoodRx.

The following subservice organization controls should be implemented by AWS to provide additional assurance that the Trust Services Criteria described within this report are met:

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.4, CC7.2	Key Management System (KMS)-Specific - Recovery key materials used for disaster recovery processes by KMS are physically secured offline so that no single AWS employee can gain access to the key material.
		KMS-Specific - Access attempts to recover key materials are reviewed by authorized operators on a cadence defined in team processes.
		Physical access to the data center is approved by an authorized individual.

Subservice Organization - AWS		
Category	**Criteria**	**Control**
		Physical access is revoked within 24 hours of the employee or vendor being deactivated.
		Physical access to the data center is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to the server locations are recorded by Closed Circuit Television Camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to the server locations are managed by electronic access control devices.
		Electronic IDS are installed within data server locations to monitor, detect and automatically alert personnel of security incidents.
Availability	A1.1	AWS maintains a capacity planning model to assess infrastructure usage and demands at least monthly, and usually more frequently (e.g., weekly). In addition, the AWS capacity planning model supports the planning of future demands to acquire and implement additional resources based upon current resources and forecasted requirements.
		AWS contingency planning and incident response playbooks are maintained and updated to reflect emerging continuity risks and lessons learned from past incidents. The AWS contingency plan is tested on at least an annual basis.
		Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics.
	A1.2	Amazon-owned data centers are protected by fire and detection suppression systems.
		Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and system monitor and control air temperature and humidity at appropriate levels.
		Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in an Amazon owned data center.
		Amazon owned data centers have generators to provide backup power in case of electrical failure.
		Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, UPS units, and redundant power supplies.
		AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards.
		Simple Storage Service (S3)-Specific - S3 performs continuous integrity checks of the data at rest. Objects are continuously validated against their checksums to prevent object corruption.

Subservice Organization - AWS		
Category	**Criteria**	**Control**
		S3-Specific - When disk corruption or device failure is detected, the system automatically attempts to restore normal levels of object storage redundancy.
		S3-Specific - Objects are stored redundantly across multiple fault-isolated facilities.
		S3-Specific - The design of systems is sufficiently redundant to sustain the loss of a data center facility without interruption to the service.
		RDS-Specific - If enabled by the customer, Relational Database Service (RDS) backs up customer databases, stores backups for user-defined retention periods, and supports point-in-time recovery.
		Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics.
		Incidents are logged within a ticketing system, assigned severity rating and tracked to resolution.
		Critical AWS system components are replicated across multiple Availability Zones and backups are maintained.
		Backups of critical AWS system components are monitored for successful replication across multiple Availability Zones.
Processing Integrity	PI1.5	AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards.
		S3-Specific - S3 performs continuous integrity checks of the data at rest. Objects are continuously validated against their checksums to prevent object corruption.
		S3-Specific - When disk corruption or device failure is detected, the system automatically attempts to restore normal levels of object storage redundancy.
		S3-Specific - Objects are stored redundantly across multiple fault-isolated facilities.
		S3-Specific - The design of systems is sufficiently redundant to sustain the loss of a data center facility without interruption to the service.
		RDS-Specific - If enabled by the customer, RDS backs up customer databases, stores backups for user-defined retention periods, and supports point-in-time recovery.

GoodRx management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant Trust Services Criteria through written contracts, such as SLAs. In addition, GoodRx performs monitoring of the subservice organization controls, including reviewing attestation reports over services provided by vendors and the subservice organization.

COMPLEMENTARY USER ENTITY CONTROLS

GoodRx's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to GoodRx's services to be solely achieved by GoodRx control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of GoodRx's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User organizations should implement sound and consistent internal controls regarding general IT system access and system usage appropriateness for all internal user organization components associated with GoodRx.
2. User organizations should practice removal of user accounts for any users who have been terminated and were previously involved in any material functions or activities associated with GoodRx's services.
3. Transactions for user organizations relating to GoodRx's services should be appropriately authorized, and transactions should be secure, timely, and complete.
4. For user organizations sending data to GoodRx, data should be protected by appropriate methods to ensure confidentiality, privacy, integrity, availability, and non-repudiation.
5. User organizations should implement controls requiring additional approval procedures for critical transactions relating to GoodRx's services.
6. User organizations should report to GoodRx in a timely manner any material changes to their overall control environment that may adversely affect services being performed by GoodRx.
7. User organizations are responsible for notifying GoodRx in a timely manner of any changes to personnel directly involved with services performed by GoodRx. These personnel may be involved in financial, technical, or ancillary administrative functions directly associated with services provided by GoodRx.
8. User organizations are responsible for adhering to the terms and conditions stated within their contracts with GoodRx.
9. User organizations are responsible for developing, and if necessary, implementing a business continuity and disaster recovery plan (BCDRP) that will aid in the continuation of services provided by GoodRx.