System and Organization Controls (SOC) 3

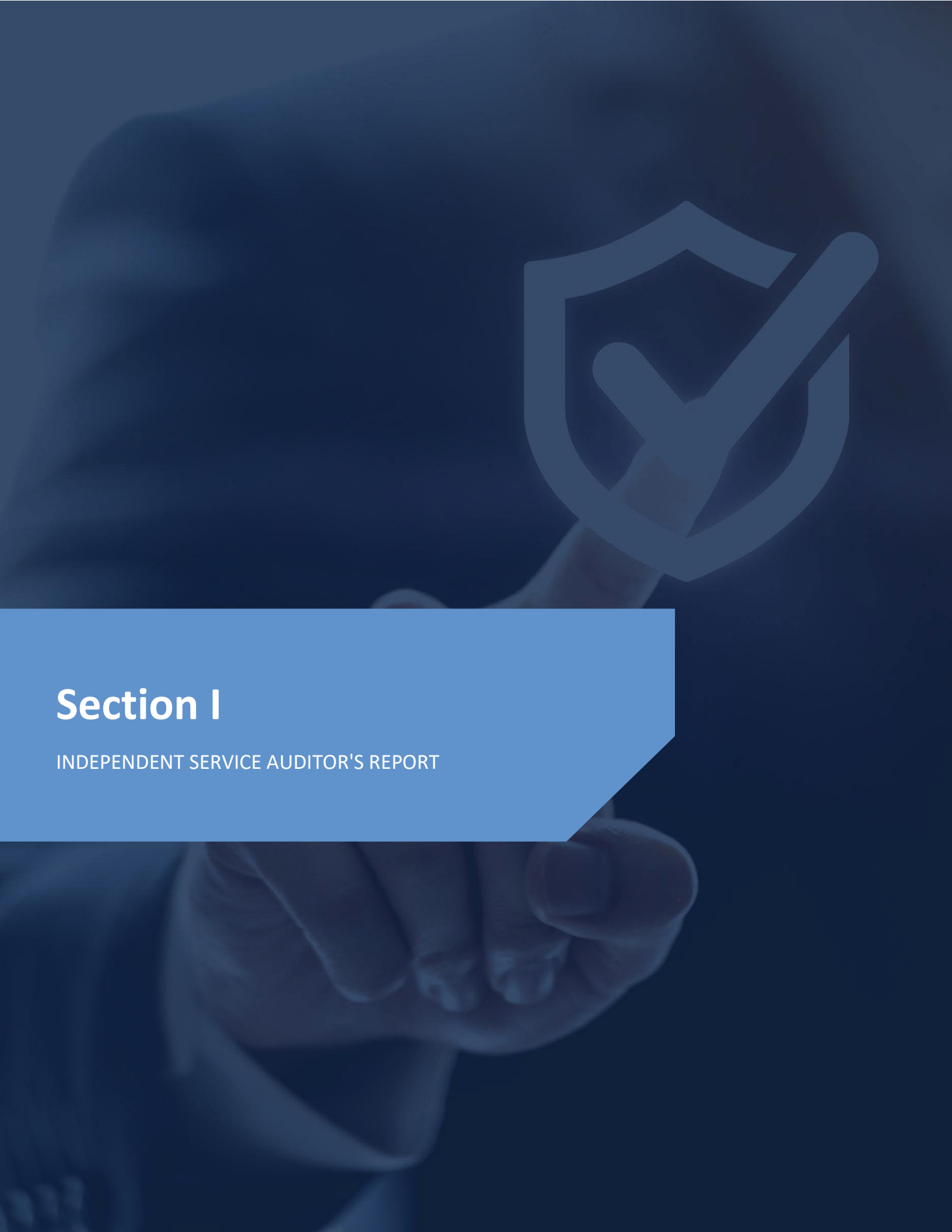
Relevant to the Trust Services Criteria for Security

For the Period
March 18, 2025 to June 16, 2025

Together with Independent Service Auditor's Report

caredove

TABLE OF CONTENTS



Section I

INDEPENDENT SERVICE AUDITOR'S REPORT

Caredove, Inc.

Scope

We have examined Caredove, Inc.'s accompanying assertion titled "Assertion of Caredove, Inc. Management" (assertion) that the controls within Caredove, Inc.'s The Caredove Platform (system) were effective throughout the period March 18, 2025 to June 16, 2025, to provide reasonable assurance that Caredove, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA*, Trust Services Criteria*.

Service Organization's Responsibilities

Caredove, Inc. 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 Caredove, Inc.'s service commitments and system requirements were achieved. Caredove, Inc. has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Caredove, Inc. is responsible for selecting, and identifying in its assertion, the applicable trust service 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 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. 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 controls were not effective in achieving Caredove, Inc.'s service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective in achieving Caredove, Inc.'s 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.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the 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 were achieved based on the applicable trust services criteria. Also, the projection to the

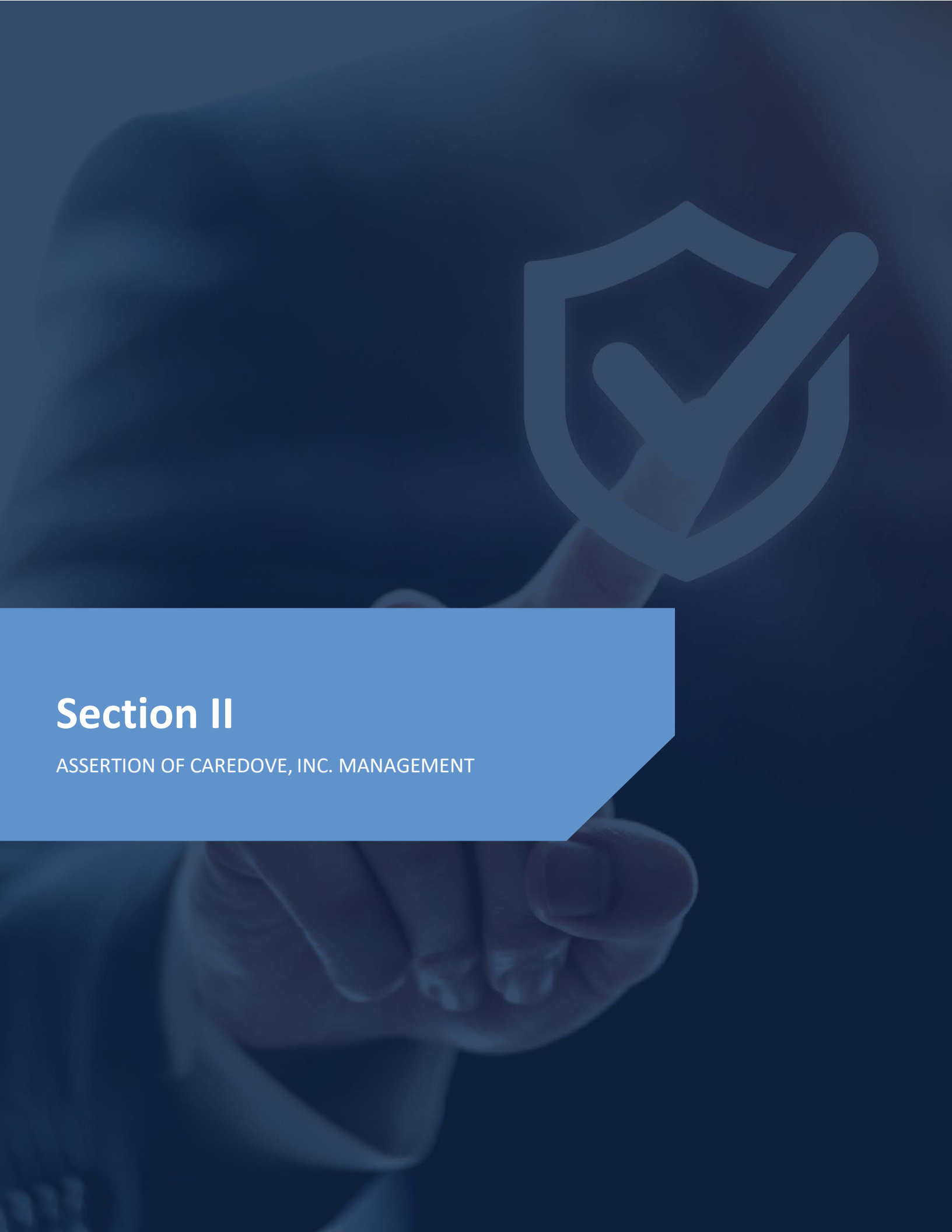
future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Caredove, Inc.'s The Caredove Platform were effective throughout the period March 18, 2025 to June 16, 2025, to provide reasonable assurance that Caredove, Inc. service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

JohansonGroup LLP

Colorado Springs, Colorado
September 29, 2025



Section II

ASSERTION OF CAREDOVE, INC. MANAGEMENT

We have prepared the accompanying description of Caredove Inc.'s "The Caredove Platform (system) " for the period March 18, 2025 to June 16, 2025, (description) based on the criteria for a description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria) (description criteria). The description is intended to provide report users with information about Caredove Inc.'s "The Caredove Platform (system) that may be useful when assessing the risks arising from interactions with Caredove Inc.'s system, particularly information about system controls that Caredove has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy Categories (applicable trust services criteria) set forth in TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022) in AICPA, Trust Services Criteria.

We are responsible for designing, implementing, operating, and maintaining effective controls within Caredove, Inc.'s The Caredove Platform (system) throughout the period March 18, 2025 to June 16, 2025, to provide reasonable assurance that Caredove, Inc.'s service commitments and system requirements relevant to Security were achieved. Our description of the boundaries of the system is presented in the section of this report titled, "Description of The Caredove Platform" and identifies the aspects of the system covered by our assertion.

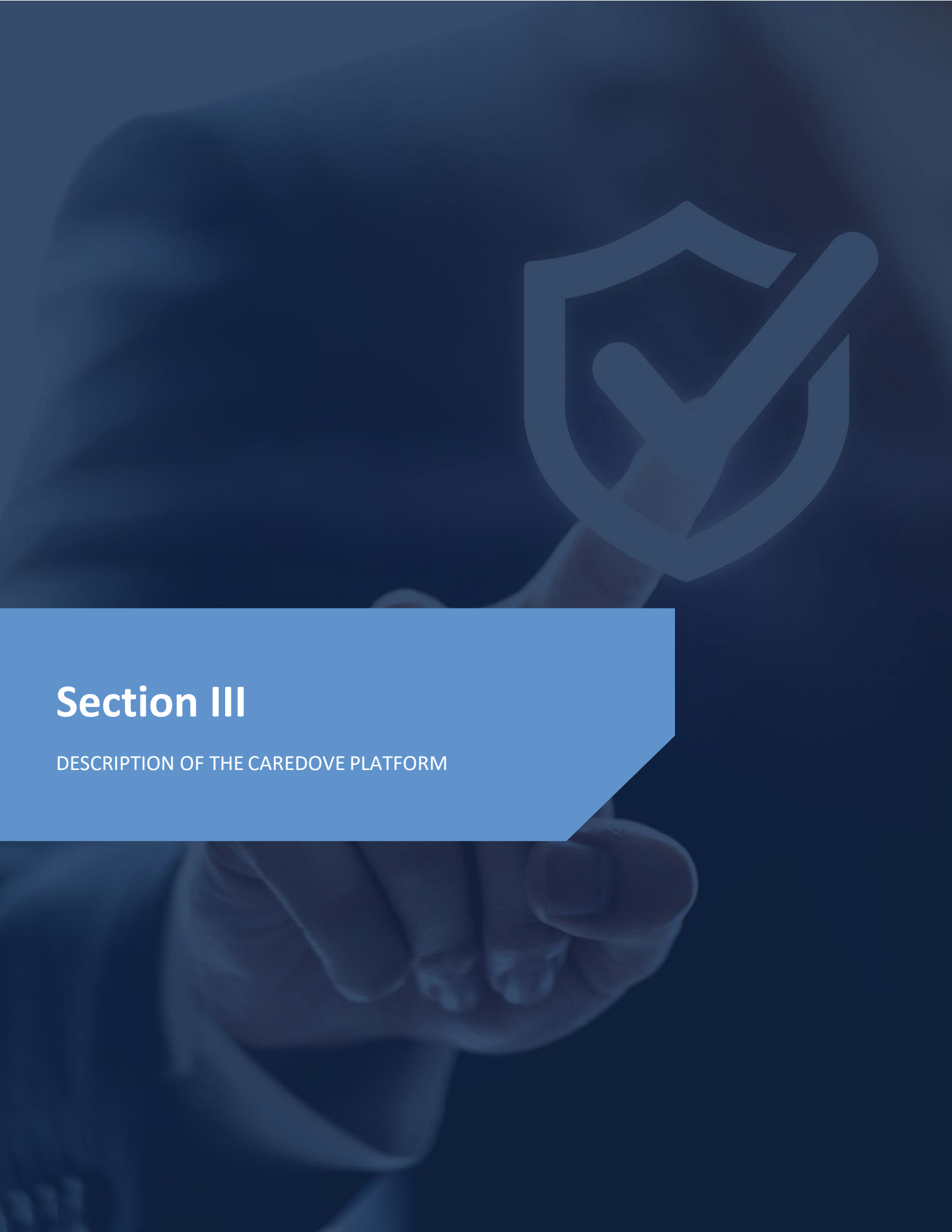
We have performed an evaluation of the effectiveness of the controls within the system throughout the period March 18, 2025 to June 16, 2025, to provide reasonable assurance that Caredove, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA*, Trust Services Criteria.*

Caredove, Inc.'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 the accompanying system description.

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 March 18, 2025 to June 16, 2025, to provide reasonable assurance that Caredove, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

Caredove, Inc. Management
September 29, 2025



Section III

DESCRIPTION OF THE CAREDOVE PLATFORM

Company Background

Caredove Inc. is a software company located at 25 Mississaga St E, Suite 5, Orillia, ON L3V 1V4, Canada. It has approximately 20 employees. It was founded in 2012 by Jeff Doleweerd and Tim Berezny after years of consulting in the healthcare space. Jeff comes from a business background, and Tim from a systems engineering background. Caredove believes that everyone should be able to easily connect and engage with the care that helps them remain independent and healthy at home.

Description of Services Provided

The Caredove Platform enables community healthcare networks to manage and action referral traffic from healthcare providers and community members. The platform comprises a dashboard, forms, and a search component, with integrations for external referral systems and popular Electronic Medical Record EMR) systems.

Caredove allows healthcare networks to effectively promote their services, enabling both the public and clinicians to sign up, schedule convenient appointments, or search for services. It facilitates efficient onboarding of new clients by healthcare agencies. Agencies can either join existing networks or create new initiatives with partner organizations to address specific local healthcare needs. Additionally, local health agencies can organize trusted networks to address regional healthcare challenges, pool resources, and enhance referrals.

The Caredove Application has three main components:

Forms: Allows healthcare services to capture patient data, e.g., in referrals

Search and Booking: Allows both practitioners and the public to search for a service based on a number of criteria, including geographical location. Once a service is found, Caredove enables date-time booking for the healthcare service.

Dashboard: Allows Caredove customers and their agents to manage or create referrals manage booking and availability configure

healthcare service listings build forms generate reports

Caredove's Transitional Upgrade State

Caredove is gradually deprecating its legacy system in favour of a more modern system with even greater security features. Caredove's original PHP monolith, referred to as "Legacy" has had key front-end components of forms and search replaced with updated components (c.2020) dubbed "C5". Shortly thereafter work began on a new back-end intended to replace Legacy's role as the core data processor. This most recent iteration is dubbed "C6". At present, all of these components are active simultaneously as deprecation efforts continue. For example, Legacy and C5 customer forms have almost entirely been migrated to C6 - a notable achievement for the Caredove team. Because different components of the system sometimes have different security features, the names "Legacy", "C5" and "C6" will continue to be referenced throughout this report.

Principal Services Commitments and System Requirements

Caredove designs processes and procedures to meet objectives based on commitments to users, applicable laws and regulations, and established financial, operational, and compliance requirements. System services adhere to internal security commitments detailed in our Privacy Policy, Terms and Conditions (available on our website under "Legal & Privacy"), and the Trust Report at http://trust.caredove.com .

Scope of this Report

The Caredove system is evaluated against the Security, Availability, and Confidentiality criteria of the AICPA Trust Services Framework.

The Processing Integrity criterion is excluded because Caredove does not execute financial or monetary transactions on behalf of customers. The Privacy criterion is excluded because, under our Data Processing Agreements, Caredove acts solely as a data processor while each healthcare organization remains the data controller for any PHI/PII transmitted through the platform; customers control what data is collected and how it is used. The period for the present report is between March 18 June 17 2025 inclusive.

Security Commitments

Security commitments include, but are not limited to, the following:

- Configurations for role-based user access control.
- Intrusion detection systems for external security threats.
- Regular vulnerability scans and penetration testing.
- Policies for data retention and disposal.
- Encryption in transit and at rest

Encryption & Key Management

Caredove uses encryption both in-transit and at-rest. The in-transit mechanism is TLS 1.2 Amazon Certificate Manager certificates on ALB . Certificates are AWS-managed. Web traffic is not allowed on port 80, and always forced to SSL. Database connections internal to the Caredove AWS account are also encrypted, using the Amazon Certificate Authority rds-ca-rsa2048-g1.
Caredove employs two “at rest” encryption mechanisms for customer data:

All databases are encrypted at rest by AWS-managed KMS keys. AWS CloudTrail logs all KMS API calls. Both AWS-managed keys and CMKs are auto-rotated annually.

In addition to the above, the C6 Postgres database encrypts PHI at the field level, preventing even devs with DB access from viewing PHI.

Components of the System

The System description is comprised of the following components:

- **Infrastructure** – The collection of physical or virtual resources that supports an overall IT environment, including cloud infrastructure (for example, servers, storage, and networks) and IT hardware (desktops and laptops) that the service organization uses to provide the services.
- **Software**: Application programs, supporting software OS, middleware, utilities), databases, external web applications, and in-house developed applications (including mobile and desktop applications).
- **People**: Personnel involved in governance, operations, security, development, and management.
- **Data**: Transaction streams, files, databases, tables, processed outputs.
- **Procedures**: Automated and manual procedures for service initiation, authorization, performance, delivery, and reporting.

Infrastructure

Caredove Inc. maintains a system inventory that includes virtual machines, computers (desktops and laptops), and networking devices (switches and routers). The inventory documents device name, inventory type, description and owner. To outline the topology of its network, the organization maintains the following network diagram(s).

Network Diagram

Please see Vanta for the Network Diagram

Region & Availability Zones

- All production workloads run in **ca-central-1** AWS Montréal), except for address search and maps (in GCP, regionless) and Netlify front-end code hosting. Cronofy Outlook integration) runs in the Canadian Data Center.
- **Cross-AZ RDS/Aurora backups** are enabled by default; full multi-AZ application fail-over is on the FY 25 roadmap once cost optimizations are complete.

VPC Architecture

VPC	Primary Workloads	Notes
Legacy + C5 VPC	Yii v1 "Legacy" app, C5 Django + React services, search sites	Peered to C6 VPC
C6 VPC	Laravel Vapor 3 Lambda fns / env), Aurora Serverless v2 PostGIS , React front-end Netlify)	Peered to Legacy VPC for data sync

Security groups are limited to same subnet, except in cases like peering (adding another subnet). Database security groups are least-privilege and audited.

Compute & Containers

Stack	Runtime	Orchestration	Purpose
Legacy	PHP 7.1 on nginx + Workerman	**ECS Fargate** Clusters: legacy-fargate-prod, legacyfargate-sandbox)	Core scheduling & referral engine
C5	React UI (customer-facing), Laravel Nova API and front-end (internal only), Django API and front-end (internal only)	**ECS Fargate** C5 FormsProd-1, caredo Django), **EC2** Laravel Nova)	Transitional forms & search
Utility	Node micro-services	**ECS Fargate** (utility-server)	PDF filler, API gateway
C6	PHP 8.x Laravel Vapor)	**Lambda** + API Gateway	Next-gen forms, field-level crypto
Phoenix FHIR	Node FHIR server	Stand-alone **EC2**	Standards gateway
VPN	OpenVPN AS	Stand-alone **EC2**	Mandatory jump-point for DB access

Databases & Storage

- **Legacy MySQL 8** RDS, encrypted, daily snapshots, 7-day retention)
- **Legacy/PostGIS PostgreSQL 14** RDS, encrypted, daily snapshots, 7-day retention)
- **C5 PostgreSQL 14 PostGIS (**RDS, encrypted, daily snapshots, 7-day retention**)**
- **C6 Aurora Serverless v2 PostgreSQL 14 PostGIS** (encrypted, autoscaling 0.5 8 ACUs, daily snapshots, 7-day retention)

All buckets default to **SSE KMS**; only caredove-app-storage-public allows anonymous GetObject over HTTPS.
EFS used for legacy files shared between containers. It is also used for a customer's learning module SFTP/NGINX microsite (grandfathered).

Network & Load Balancing

LB	Type	Listeners	Key Use-Cases
web-app	ALB	80→443, 443, 2020, 3000, 3020, 8080	Production Legacy & C5
web-sandbox	ALB	same ports	Non-prod
c5web-app	ALB	443	Internal Django/Nova
Caredove-Production-NLB Caredove-Sandbox-NLB	NLB Elastic IP	443	Static IP required by integration partner

All target groups use health checks; AWS WAF in front of all ALBSs

VPN & Peering

- OpenVPN EC2 is the only ingress path to RDS/Aurora.
- Security groups allow DB traffic **only from VPN CIDR + peered VPCs**.

Software

Note: See "Integrations" in Vanta for full list, vendor assessments and risk levels. The following list includes core non-AWS SAAS software required in the deployment and operation of the Caredove application. AWS Software used includes GuardDuty for security monitoring.

System/Application	Purpose
New Relic	Monitoring application used to provide monitoring, alert, and notification services for Caredove Inc. platform
Google Cloud	Geo services (maps, address search)
GitHub	Private code repository and CI/CD workflows
Intercom	Customer Support
Netlify	Front-end code hosting

Devices

Caredove has a comprehensive policy for managing physical devices, including employee computers, as outlined in their Asset Management Policy and Workstation Security Policy.

Device Security: Employees are responsible for securing company equipment, especially when transported or stored outside company facilities. Devices must be physically secured, for example, by locking them in offices or using cable locks when not in use.

Software and Encryption: Software security is enforced by Jamf Pro and Jamf Protect (planned migration to Kandji), enforcing the requirements in the Access Control Policy and the Workstation Security Policy. All software on Caredove-owned devices must be authorized and approved by the Chief Privacy Officer. Full disk encryption is employed where appropriate, and devices must have active anti-malware and firewall protection.

Loss or Theft: Any loss of devices must be reported immediately.

BYOD Policy: Employees may use their own devices if pre-approved, but these devices should not access Protected Health Information (PHI).

People

Caredove employs dedicated team members for operations, support, and product development. The IT/Engineering team manages system monitoring, backups, and recovery. The company prioritizes hiring skilled personnel, providing task-specific and security-related training.

Management includes:

- CEO Jeff Doleweerd
  CTO Tim Berezny
-

Teams include:

- **Operations**: Maintaining infrastructure availability and security.
  Devops, IT, Security and Compliance: Managing productivity, operational technologies, security and privacy.
-
  - **Product Development**: Handling software lifecycle, including development, testing, deployment, and maintenance.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING

Control Environment

Integrity and Ethical Values

Caredove Inc. has established specific control activities to ensure that integrity and ethical values are clearly communicated, acknowledged, and enforced within the organization. The controls implemented by Caredove include:

- **Employee Background Checks (HRS-1)**: Caredove conducts comprehensive background checks for all new employees during the hiring process to verify their suitability and integrity for the role.
- **Code of Conduct (HRS-2, HRS-3)**:
  - Employees are required to formally acknowledge the company's Code of Conduct at the time of hire, which outlines expected ethical behaviors and standards. Employees who violate this code are subject to disciplinary actions consistent with Caredove's disciplinary policy.

  - Contractors engaged by Caredove are required to acknowledge the company's Code of Conduct within their contractual agreements, ensuring consistent ethical standards across all personnel.

- **Confidentiality Agreements (HRS-4, HRS-5)**:
  - All employees must sign a confidentiality agreement as part of their onboarding, which explicitly prohibits the unauthorized disclosure of proprietary or confidential information, including client-related information.
  - Contractors must similarly sign confidentiality agreements at the commencement of their engagement, reinforcing confidentiality obligations consistently throughout all levels of engagement.
- **Performance Evaluations (HRS-6)**: Managers at Caredove conduct formal performance evaluations of their direct reports at least annually, reinforcing accountability, adherence to ethical standards, and performance expectations.
- **Security Awareness Training (SAT-1)**: All Caredove employees are required to complete security awareness training within 30 days of hire and subsequently on an annual basis. This ensures continual reinforcement of security best practices and ethical handling of company and customer data.

Commitment to Competence

Competence levels translate into job-specific requirements, supported by ongoing training.

Caredove Inc. ensures employee competence through clearly defined role requirements and ongoing skills development. Specific controls include:

- Defined Position Requirements:
  Management maintains clearly documented job descriptions that explicitly outline the skills, qualifications, and experience levels required for each role. This ensures consistent expectations for competence across the organization.
- Annual Performance Evaluations (HRS-6):
  Managers perform formal performance evaluations for all direct reports annually. These evaluations verify and document employee competence, identify opportunities for professional growth, and ensure alignment with organizational standards.
- Security Awareness and Ongoing Training (SAT-1):
  Employees complete mandatory security awareness training within 30 days of hire, with refresher training conducted annually thereafter. This regular training ensures continuous reinforcement of security practices and maintains the requisite competence levels among staff.

Management Philosophy and Operating Style

Caredove Inc.'s management philosophy emphasizes balancing rapid technological advancement with responsible stewardship of customer data. Specific controls supporting this philosophy include:

- **Executive Management Meetings (Administrative)**:
  Regular executive management meetings are conducted to discuss strategic initiatives, operational performance, and significant business decisions, ensuring alignment across leadership.
- **Regulatory and Industry Briefings (Security & Privacy Governance)**:
  Management receives periodic briefings and updates on relevant regulatory, industry, and security changes affecting Caredove's operations and services. This ensures informed decision-making and proactive compliance.

Organizational Structure and Assignment of Authority and Responsibility

Caredove Inc.'s organizational structure clearly defines roles, responsibilities, and reporting relationships, facilitating effective planning, execution, control, and monitoring of organizational objectives. Specific controls include:

- **Organizational Charts (Administrative)**:
  Clearly documented organizational charts are maintained to outline key areas of authority and reporting relationships. These charts are regularly updated and communicated to all employees, ensuring transparency and clarity regarding role expectations and hierarchies.
- **Policy and Communication of Objectives (Security & Privacy Governance)**:
  Policies explicitly communicate appropriate business practices and standards of knowledge and experience required of key personnel. Regular internal communications and training reinforce organizational objectives, ensuring employees clearly understand their individual roles, responsibilities, and accountability.

HR Policies and Practices

Caredove Inc.'s success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. Caredove Inc.'s human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific controls:

- New employees are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment. HRS 5
- Evaluations for each employee are performed on an annual basis HRS 6
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist IAC 8
- New employees require a background check HRS 1

Data

Data, as defined by Caredove Inc., constitutes the following:

User and account data includes Personally Identifiable Information PII) and operational data from employees, customers, and third-party entities. Data may also include Protected Health Information PHI. Access to PII and PHI is strictly controlled by provisioning system permissions aligned with job roles, supported by ongoing monitoring.

Category	Description	Examples
Public	Non-confidential, publicly available	• Press releases • Public website

Internal	Management-approved internal use	• Internal memos • Design documents • Product specifications Correspondences
Customer data	Confidential customer provided information	• Customer operating data • Customer PII • Customers' patients' PII/PHI • Anything subject to a confidentiality agreement with a customer
Company data	Confidential operational information	• Legal documents • Contractual agreements • Employee PII • Employee salaries

Tenant Isolation

Caredove is a multi-tenant SaaS platform. Every record that represents a customer resource (user, referral, appointment, audit event, file, etc.) is related to an organization_id foreign-key.

- In legacy services C5 , organization_id is an **integer** primary key; in the next-gen C6) services it is a **UUID**, eliminating key-guessing attacks.
- All data access is performed exclusively through the application layer. The Laravel, Django, and Node service layers attach an organization_id filter to every query built through their respective ORMs. Direct SQL access is not provided to customers.
- Application middleware short-circuits any API call where the authenticated user's organization_id does not match the target resource, returning HTTP 403.
- **Field-level encryption** AES 256 GCM via Laravel Crypt + libsodium) is used in C6 for PHI/PII columns so that read-only database users cannot view sensitive data.

GCP Usage Scope

Caredove's use of Google Cloud Platform is limited to **Google Maps Platform APIs** for geocoding and address-auto-complete. Google is responsible for the physical and network security of the Maps infrastructure. Caredove is responsible for:

- safeguarding API keys in AWS Secrets Manager, enforcing per-host quotas and referrer
- restrictions, and reviewing the GCP SOC 2 bridge letter annually TPM 2
- No Caredove customer data is stored on GCP resources.

Processes and Procedures

Caredove Inc. maintains comprehensive management-developed policies and procedures for information security, reviewed at least annually (GOV-11). These policies address key areas including physical security, logical access, system availability, change management, data communications, risk assessment, data retention, and vendor management.

Physical Security

Physical security for data centers and infrastructure is managed by AWS and reviewed annually by Caredove via AWS Artifact (PES-1, PES-2, PES-3).

Logical Access

Caredove Inc. provides employees and contractors access to infrastructure through a clearly defined role-based access control system (RBAC). Access to systems is divided into three distinct privilege levels: Administrator, User, and No Access. User access and roles are reviewed quarterly to ensure adherence to the principle of least privilege (GOV-7, GOV-10).

Management is responsible for provisioning system access based on clearly defined roles and responsibilities and conducting employee background checks (HRS-1). Employees must review Caredove Inc.'s security policies (GOV-11) and complete security awareness training (SAT-1) within 30 days of hire.

Upon employee termination, Management ensures that system access is deprovisioned within 24 hours of termination to maintain security.

Computer Operations (Availability)

Caredove Inc. maintains rigorous internal SLA monitoring, comprehensive incident response plans, and vulnerability and system monitoring procedures (OPS-1). Regular system backups are performed and documented according to company policy (GOV-5).

Source Control

Caredove utilizes GitHub as its source control platform. All production branches are protected and require at least one approved pull request and passing continuous integration (CI) tests.

Continuous Integration and Continuous Delivery (CI/CD)

Caredove employs GitHub Actions integrated with AWS SAM/CloudFormation for continuous deployment, with configurations securely managed through environment-specific secrets. Deployments occur frequently—often daily—from Monday through Friday. Robust rollback mechanisms are available via one-click CloudFormation stack versioning, an EFS "circuit breaker," and automatic scaling. The ‘EFS circuit breaker’ ensures that if file system mounting or data copy operations fail during deployment, containers will not pass health checks, automatically preventing promotion of the faulty release and preserving service continuity.

Change Management

Change approval is fully automated via pull-request reviews in GitHub. Emergency changes ("hotfixes") follow the same rigorous review and deployment process to ensure consistency and security (CFG-1, GOV-6, GOV-13).

Role	Responsibility	Contact Path
IR Commander CTO	Decision authority, external comms	Mobile, Slack
DevOps Lead	Triage AWS events, execute containment	Mobile, Slack
CPO	Privacy impact assessment & regulator notice	Mobile, Slack
Cloudticity NOC	24 7 infra escalation	Support email ("urgent" in subject for SLA)

The role of Cloudticity, Caredove's Managed Cloud Provider

Cloudticity (see service agreement and vendor assessment in Vanta) provides infrastructure-level support for Caredove in AWS. Predominant security responsibilities include real-time breach monitoring. Predominant infrastructure responsibilities include on-request assistance and emergency assistance. Cloudticity maintains its own AWS account, which connects to Caredove's through detailed permissions.

Identity & Access Management

- **RBAC via AWS IAM**; Dev team holds "Power User" role **only in the dev account**.
  - DevOps lead as well as Cloudticity holds "Power User" role in dev and production.
- **MFA enforced** for all console and root users.
- On/Off-boarding tickets in Vanta trigger automatic GitHub + AWS access changes (≤ 24 hrs SLA .

- **Continual IAM review** by Vanta - password and key rotations
- **Cross-account roles** are not offered, except for the managed cloud provider, Cloudticity (e.g., no customer cross-account connections).

Backup & Disaster Recovery

Asset	Backup Method	Frequency	Retention	DR Testing
RDS MySQL & PG	Automated snapshots	Daily @ 05:30–06:30 UTC	7 days	Quarterly point-in-time restore in sandbox
Aurora Serverless	Cross-AZ snapshots	Daily @ 09:58–10:28 UTC	7 days	Same as above
EFS	AWS Backup vault	Daily	14 days	Annual restore test

S3 critical buckets	Versioning	Real-time	Temp customer data (e.g., zip packages of referral materials) 7 days (lifecycle)	Random object restore test semiannually

Non-PHI, masked DB clones are restored **biweekly** into the dev account to validate backup integrity.

Computer Operations - Availability

Caredove Inc. maintains robust policies and procedures to ensure availability and rapid response to incidents affecting service continuity:

- **Incident Response Plan (IRO-1, IRO-2, IRO-3)**: Caredove Inc. maintains a comprehensive incident response plan, which is tested annually. Procedures clearly define the steps for identifying, logging, reporting, resolving, and communicating incidents to relevant parties.
- **System Monitoring and Vulnerability Management (OPS-1, MON-1, MON-2, END-1, VPM-1, VPM-2)**: Internal monitoring covers all key applications, databases, and cloud storage using New Relic and AWS monitoring services (GuardDuty, CloudWatch, Alarms) to ensure compliance with SLA requirements. AWS ECS image scans and Dependabot are utilized to identify vulnerabilities in source code and dependencies, with an internal SLA guiding remediation.
- **Penetration Testing and Vulnerability Scanning (IAO-2, VPM-2)**: Caredove Inc. engages Oppos, an external security firm, to perform annual penetration tests and quarterly vulnerability scans. Identified vulnerabilities are tracked and remediated promptly in accordance with internal SLAs.

Change Management

Caredove Inc. has established clear and thorough change management practices to maintain system integrity and reliability:

- **Systems Development Life Cycle (CFG-1)**: Caredove maintains documented Systems Development Life Cycle (SDLC) policies to standardize the documentation, initiation, testing, and implementation of all changes. Change control processes clearly outline the required documentation, quality assurance testing, user acceptance testing (UAT), and approval procedures.
- **Change Control Procedures (GOV-6, GOV-13)**: All application and infrastructure changes are documented through a formal ticketing system (GitHub Issues and Pull Requests), with management approval documented prior to production deployments. Quality assurance and UAT results are systematically documented and associated with each change request.
- **Version Control and Rollback Capability**: GitHub version control software is employed to track code changes and facilitate rollback capabilities, ensuring transparency and accountability of all changes made by developers.

Data Communications

Caredove Inc. leverages AWS as its primary platform-as-a-service (PaaS), managed through Cloudticity, to streamline operations, network security, and system resilience:

- **Network Security and Configuration (NET-1, NET-2, NET-3, NET-4, NET-5)**: AWS provides a simplified logical network configuration and effective firewall protections around Caredove Inc.'s application containers, allowing only secure, encrypted (HTTPS) ingress from designated endpoints. Network segmentation, firewall rulesets, and system hardening standards are regularly reviewed and maintained.
- **Container and Infrastructure Management (CRY-4, CRY-1, CRY-5, IAC-10, IAC-12, IAC-13)**: AWS Fargate and ECS automatically manage the provisioning and deprovisioning of containers, maintaining system availability. Authentication to all production systems uses unique usernames/passwords or SSH keys and requires multi-factor authentication for remote access over encrypted connections.

- **Third-Party Vendor Management (TPM-1, TPM-2)**: Agreements with vendors such as Cloudticity are documented, ensuring comprehensive security and privacy requirements. A robust vendor management program includes an inventory of critical third-party vendors and annual security and privacy reviews.
- **Data Encryption and Customer Data Handling (CRY-2, DCH-1, DCH-5, AST-2)**: Customer data is securely encrypted at rest and in transit, with restricted privileged access to encryption keys. Data classification policies ensure proper handling and security, and customer data is promptly removed from the environment following termination of service.

System Boundaries

Boundaries cover only infrastructure, software, people, procedures, and data directly supporting provided services. AWS and Google Cloud Platform services are subservices, not within the direct system boundaries.

Layer / Control Domain	AWS Responsibility	Caredove / Cloudticity Responsibility	Evidence Pointer Vanta Control ID, Run-book, etc.)
Physical Security & Power	Owns and secures datacenter facilities, HVAC, UPS, generators	N/A (inherited)	AWS SOC 2, ISO 27001 reports
Network Edge & Hypervisor	DDoS protection, border routers, host OS patches for EC2/Lambda/Fargate	N/A (inherited)	AWS SOC 2
VPC & Subnet Design	N/A	Define CIDRs, NACLs, private vs. public subnets, VPC endpoints	IAC 6, NET 2
Security Groups / Firewall Rules	N/A	Least-privilege SGs, ALB/NLB listener restrictions	NET 3, NET 4
Identity & Access Mgmt.	Provides IAM service and MFA mechanisms	Create roles, enforce MFA, quarterly access review	IAC 7
Compute Configuration ECS, Lambda, EC2	Provides managed runtimes and Fargate isolation	Harden task definitions, patch base images, SSM patching of EC2 VPN/FHIR	VPM 1
Data Encryption in Transit	TLS endpoints on ALB/NLB, AWS Certificate Manager	Enforce TLS 1.2 , HSTS; rotate ACM certs yearly	CRY 4, IAC 13, NET 1
Data Encryption at Rest	Operates KMS, HSMs, disk encryption	Own CMKs, manage key policies, annual rotation	CRY 4

Logging & Monitoring	Delivers CloudTrail, GuardDuty, Config	Enable all-region CloudTrail, forward to immutable S3, alerting via Slack/PagerDuty	MON 2, MON 4, OPS 1
Back-ups & DR Infra	Manages snapshot storage and durability	bi-weekly restores	GOV 5

Risk Assessment Process

Caredove Inc.'s risk assessment process identifies and manages risks that could potentially affect Caredove Inc.'s ability to provide reliable and secure services to our customers. As part of this process, Caredove Inc. maintains a risk register to track all systems and procedures that could present risks to meeting the company's objectives (see Vanta). Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. The risk register is reevaluated annually, and tasks are incorporated into the regular Caredove Inc. product development process so they can be dealt with predictably and iteratively.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Caredove Inc.'s system; as well as the nature of the components of the system result in risks that the criteria will not be met. Caredove Inc. addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Caredove Inc.'s management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Information and Communication Systems

Information and communication are an integral component of Caredove Inc.'s internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. Caredove Inc. uses several information and communication channels internally to share information with management, employees, contractors, and customers. Caredove Inc. uses chat systems and email as the primary internal and external communications channels. Structured data is communicated internally via SaaS applications and project management tools. Finally, Caredove Inc. uses in-person and video "all hands" meetings to communicate company priorities and goals from management to all employees.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Caredove Inc.'s management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

Monitoring, Logging & Alerting

Layer	Tooling	Alerts Routed To	Typical MTTR
Infra / CloudTrail	AWS GuardDuty, Oxygen Cloudticity)	Slack #securityalerts, PagerDuty	Depending on severity. High/Critical severity, < 15 minutes. Medium or low severity, ticketed and actioned when possible.
Application	New Relic APM + synthetics, Cloudwatch alarms	Slack #alertsdowntime, NR dashboards	< 15 minutes for outage reports
Containers	CloudWatch Logs Insights, cloudwatch alarms	Slack #aws-alerts	< 30 min for unexpected/new
WAF	AWS WAF Geo, SQLi, HTTP Flood, IP Reputation)	Slack #aws-alerts	Real-time, in principle. In practice, no events.

On-going Monitoring

Cloudticity provides intrusion detection systems, plus SOC2 checks (redundant upon Vanta), and AWS security best-practice checks. Github provides dependency security checks. AWS provides ECS container software security checks.
Caredove Inc.'s management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.
Management's close involvement in Caredove Inc.'s operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Caredove Inc.'s personnel.

Reporting Deficiencies

Our internal risk management tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents (see Privacy Incident and Breach Management). Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

Changes to the System

Type 1

No significant changes have occurred to the services provided to user entities in the last 3 months preceding the end of the review date.

Type 2:

During the audit period, Caredove implemented the following notable changes to its systems and operational environment:

- **Infrastructure Improvements:**
    - Enhanced Legacy system session management using AWS DynamoDB.
    - Improved shared file management between containers using AWS Elastic File System (EFS).
- **Database Upgrades:**
    - Upgraded PostgreSQL databases across all environments from version 12 to version 14.
- **Device Management:**
    - Engaged Kandji for Mobile Device Management (MDM) solutions, initially in testing and configuration phase; existing MDM provided by Jamf was utilized throughout the audit period.
- **Quality Assurance and Testing:**
    - Adopted and implemented a new software testing platform, Currents.dev, to enhance quality assurance practices.
- **Monitoring Enhancements:**
    - Expanded metric collection and reporting by integrating additional metrics with New Relic.
- **Personnel:**
    - Two employees returned from maternity leave; no significant changes in senior management or key personnel occurred.

Incidents

Type 1:

No significant incidents have occurred to the services provided to user entities in the last 3 months preceding the end of the review date.

Type 2:

<u>During the audit period, the following incidents occurred:</u>

- **Operational Incidents:**
    - Experienced intermittent CPU overages impacting performance and availability on the Legacy ECS Fargate environment.
    - Resolved by installing PHP OpCache, significantly improving resource efficiency and stability.

- **Security/Privacy Incidents:**
    - One notable privacy incident occurred involving unintended disclosure of Protected Health Information (PHI) when a referral containing actual PHI was incorrectly routed to a non-intended recipient organization.
    - Incident response included immediate investigation, notification, mitigation, and follow-up training reinforcement (documented separately in attached privacy incident report).
- **Minor Privacy Events:**
    - Minor privacy events (e.g., users inadvertently posting PHI in Intercom or other support channels) occurred periodically. Each event was promptly recorded, mitigated, and documented in the internal #security Slack channel. Due to their minor nature, short-lived exposure, and rapid mitigation, these were classified internally as minor events rather than incidents.
- **Vulnerability Management:**
    - Routine vulnerability scans identified some outdated software dependencies.
    - Packages were upgraded whenever possible. When upgrades posed compatibility or operational risks, the exceptions were documented, evaluated, and formally accepted within the Risk Register maintained in Vanta.
- **Alerts and Monitoring:**
    - Security monitoring via AWS GuardDuty, Cloudticity Oxygen, and Vanta continuously generated alerts. Critical alerts were immediately addressed, false positives suppressed, and lower priority alerts managed according to defined SLAs.

Criteria Not Applicable to the System

Upon review, **Processing Integrity** and **Privacy** criteria remain appropriately excluded:

- **Processing Integrity** criteria are not applicable because Caredove neither processes financial transactions nor maintains financial transaction records on behalf of customers.
- **Privacy** criteria remain excluded as Caredove acts strictly as a data processor. Customers maintain full data controller responsibilities, including data collection, use, and management decisions.

Subservice Organizations

Primary Subservice Providers:

- **Amazon Web Services (AWS):**
    - Provides cloud infrastructure services, including compute (EC2, ECS, Lambda), database (RDS, Aurora), storage (S3, EFS), network management (Route 53, ALB/NLB, AWS Config, WAF), encryption (KMS), monitoring (CloudWatch, GuardDuty), configuration management (CloudFormation, Systems Manager), security management (IAM, Secrets Manager), and certificate services (AWS Certificate Manager).

- **Cloudticity LLC:**
    - Managed Service Provider (MSP) responsible for:
        - Continuous security posture management (via Oxygen platform).
        - 24x7 infrastructure monitoring, maintenance, and incident response.
        - Assistance with security, compliance, and vulnerability management.
        - Managed AWS account operations and support, including regular infrastructure health checks and quarterly architecture reviews .

Additional Subservice Providers:

- **Netlify:** Provides hosting and continuous deployment (CI/CD) services for React-based front-end applications.
- **New Relic:** Offers Application Performance Monitoring (APM), infrastructure health metrics, alerting, and analytics.

Other listed vendors (e.g., GitHub, Kandji, Currents.dev, Jamf) do not directly store or process PHI and are thus not classified as critical subservice providers for SOC2 reporting purposes.

Subservice Provider - AWS

Primary Infrastructure

Hardware Type	Purpose
AWS Elastic Compute Cloud (EC2)	Provides virtual computing resources and infrastructure
AWS Elastic Container Service (ECS)	Container orchestration for deployment, scaling, and management
AWS Elastic Load Balancers (ALB/NLB)	Load balances internal and external traffic
Amazon Virtual Private Cloud (VPC)	Protects network perimeter, restricting inbound/outbound access
Amazon S3	Scalable storage for data upload/download
AWS RDS and Aurora	Relational database services with backups and redundancy
AWS Lambda	Serverless computing for event-driven applications
AWS CloudWatch	Monitoring, logging, and alarms
AWS Web Application Firewall (WAF)	Protects web applications from common exploits
AWS Certificate Manager (ACM)	Issues and manages TLS/SSL certificates
AWS Route53	Domain name system (DNS) management
AWS Systems Manager	Operational insights and configuration management
AWS Secrets Manager	Secure storage and rotation of secrets
AWS Identity & Access Management (IAM)	Secure management of access to AWS resources
AWS Key Management Service (KMS)	Encryption key management and auditing

Primary Software

System/Application	Operating System	Purpose
AWS GuardDuty	AWS	Intrusion detection and threat monitoring

System/Application	Operating System	Purpose
AWS Config	AWS	Configuration auditing and compliance monitoring

Subservice Description of Services

AWS provides critical cloud infrastructure hosting, computing, storage, networking, security, and monitoring services that underpin the availability, security, and performance of the Caredove platform.

Subservice Provider – Cloudticity, LLC

Primary Infrastructure

Hardware Type	Purpose
Cloudticity Oxygen Platform	Continuous security posture and compliance management
Managed AWS Infrastructure	24x7 infrastructure management and monitoring

Primary Software

System/Application	Operating System	Purpose
Cloudticity Oxygen	Cloudticity SaaS	Security monitoring, incident response, compliance management

Subservice Description of Services

Cloudticity provides managed services including continuous security monitoring, compliance management, and infrastructure operations for AWS-based resources.

Subservice Provider - Netlify

Primary Infrastructure

Hardware Type	Purpose
Netlify CDN	Continuous deployment and hosting of React-based front-end applications

Primary Software

System/Application	Operating System	Purpose
Netlify Platform	Netlify SaaS	Deployment, hosting, CDN management

Subservice Description of Services

Netlify provides front-end hosting, CDN distribution, and continuous deployment services.

Subservice Provider – New Relic

Primary Infrastructure

Hardware Type	Purpose
SaaS Platform	Application and infrastructure monitoring and analytics

Primary Software

System/Application	Operating System	Purpose
New Relic APM	New Relic SaaS	Application performance monitoring and alerting

Subservice Description of Services

New Relic provides application performance monitoring, infrastructure metrics collection, alerting, and analytics to support operational availability and performance.

Complementary Subservice Organization Controls

1. User entities are responsible for understanding and complying with their contractual obligations to Caredove Inc.
2. User entities are responsible for notifying Caredove Inc. of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Caredove Inc. services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Caredove Inc. services.
6. User entities are responsible for providing Caredove Inc. with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Caredove Inc. of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.
8. User entities are responsible for validating network egress rules if they restrict traffic to Caredove's static NLB IP.
9. User entities are responsible for all data lifecycle decisions (collection, access, deletion, consent) regarding PHI/PII within the Caredove platform; Caredove functions solely as a data custodian under customer instruction.