Rocket Rounding

## Rocket Rounding application security for clients - external doc (shareable)

Form factor: Web Application and Mobile Application (iOS and Android)

---

# Table of Contents



---

# 1. Rocket rounding application overview

Rocket Rounding is a cloud-based application (non on-premise) that can be deployed with any client anywhere in the world. Because Rocket Rounding can house sensitive client data, it is important to outline how we handle information security with regards to the application. Moreover, this document is designed to be used in conjunction with a client's application security review. This document can be provided to the client or used as a reference document for filling out client application security reviews.

Rocket rounding does not connect to a client's electronic medical records system (EMR), and does not have to store patient information in order to be successfully used for patient rounding.

Adding PHI to the application is permitted and protected based on the security protocols listed below. A client chooses to limit users from adding PHI to the application and must do so through their application usage policy.

Rocket Rounding ensures the integrity of its application security and will sign a Business Associate Agreement at a customer's request. Additionally, Rocket Rounding carries cyber liability insurance and customers can request to be added to the policy.

Lastly, Rocket Rounding does not store or process any patient personal financial information including the processing of credit cards. Rocket Rounding does not claim to be PCI DSS compliant.

# 2. HITRUST certification

Rocket Rounding does not have HITRUST certification (Health Trust Information Alliance), however it is built on the HITRUST Certified Google Cloud platform (GCP)

a. Access transparency – When Google Cloud Platform administrators access your content, Access Transparency gives you near real-time logs of their actions. https://cloud.google.com/access-transparency

b. VPC service controls – Keeps sensitive data private by defining a security perimeter around GCP resources like Cloud Storage buckets, Cloud Bigtable instances, and BigQuery datasets. https://cloud.google.com/vpc-service-controls

c. Cloud data loss prevention – Provides fast, scalable classification and redaction for sensitive data elements like names, credit card numbers, GCP credentials, and more. https://cloud.google.com/dlp

d. Key management service – Cryptographic keys are managed for cloud services the same way as they are on-premises, to protect secrets and other sensitive data that is stored in Google Cloud Platform. https://cloud.google.com/kms

e. Google Cloud armor – Google Cloud Armor works with Google's global cloud balancing infrastructure and provides always-on attack detection and mitigation. https://cloud.google.com/armor

# 3. NIST 800-66 certification

Rocket Rounding does not have NIST 800-66 certification. This certification is "An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule." It is a set of best practices that can be applied to applications. There is no certification recognized by Health and Human Services for HIPAA compliance. It is a framework and set of rules that are applied in an application framework. Google Cloud Platform has extensive documentation on HIPAA protocols we use, which can be found here: https://cloud.google.com/security/compliance/hipaa

Additionally, Google Cloud Platform has independent auditors that examine controls in their data center, infrastructure, and operations. Google Cloud Platform undergoes yearly audits for the following security standards:

a. **SSAE16 / ISAE 3402 Type II.** There is a public SOC 3 Report and the SOC 2 report can be obtained under NDA. https://cloud.google.com/security/compliance/soc-3

b. **ISO 27001.** Google has earned ISO 27001 certifications for the systems, applications, people, technology, processes and data centers serving Google Cloud Platform. Google Cloud Platform's ISO 27001 certificate is available on the compliance section of their website. https://cloud.google.com/security/compliance/iso-27001

c. **ISO 27017**, Cloud Security. This is an international standard of practice for information security controls based on the ISO/IEC 27002 specifically for cloud services. Google Cloud Platform's ISO 27017 certificate is available on the compliance section of their website. https://cloud.google.com/security/compliance/iso-27017

d. **ISO 27018**, Cloud Privacy. This is an international standard of practice for protection of personally identifiable information (PII) in public cloud services. Google Cloud Platform's ISO 27018 certificate is available on the compliance section of their website. https://cloud.google.com/security/compliance/iso-27018

Rocket Rounding uses heatlhIT.gov's Security Risk Assessment Tool, which is a self-survey tool used to measure administrative safeguards, technical safeguards, and physical safeguards.

# 4. Access to data - strong role-based permissions

Rocket Rounding user profiles are granted access to data based on profile roles within an organization. Role-based access is determined by firebase rules that are written to explicitly allow or deny access to data in the application. User profiles should be assigned to achieve use-cases that are determined by their job function.

# 5. Information security

Rocket Rounding's Information Security approach is not contained in a policy, but is a collection of policies and procedures that include the following:

a. Risk assessment and business continuity
b. Change management

c. Disaster Recovery

# 6. Risk assessment and business continuity

Rocket Rounding uses heatlhIT.gov's Security Risk Assessment Tool, which is a self-survey tool used to measure Administrative Safeguards, Technical Safeguards, and Physical safeguards.

a. Rocket rounding has a documented procedure in place that addresses disaster recovery and business continuity. These are also referenced in our SLAs

b. Rocket rounding does not perform annual disaster recovery and business continuity testing due to the small size of the organization. All information processing systems use Google Cloud Platform, which has robust step-by-step plans to deploy a disaster recovery instance that does not impact our development, staging, or production environments. If a client requires the organization to test our backup, restore, and cleanup capabilities, this can be discussed contractually.

   Google Cloud Platform offers features that are key to disaster recovery planning. From Google:

   - **A global network**. Google has one of the largest and most advanced computer networks in the world. The Google backbone network uses advanced software-defined networking and edge-caching services to deliver fast, consistent, and scalable performance.

   - **Redundancy**. Multiple points of presence (PoPs) across the globe mean strong redundancy. Your data is mirrored automatically across storage devices in multiple locations.

   - **Scalability**. Google Cloud is designed to scale like other Google products (for example, search and Gmail), even when you experience a huge traffic spike. Managed services such as App Engine, Compute Engine autoscalers, and Datastore give you automatic scaling that enables your application to grow and shrink as needed.

   - **Security**. The Google security model is built on over 15 years of experience with helping to keep customers safe on Google applications like Gmail and G Suite. In addition, the site reliability engineering teams at Google help ensure high availability and prevent abuse of platform

resources. You can learn more about Google's security model here: https://cloud.google.com/security

- **Compliance**. Google undergoes regular independent third-party audits to verify that Google Cloud is in alignment with security, privacy, and compliance regulations and best practices. Google Cloud complies with certifications such as ISO 27001, SOC 2/3, and PCI DSS 3.0.

# 7. Change management

Rocket Rounding has Change Management procedures in place that are designed to establish consistent practices for introducing development changes at Rocket Rounding and its parent company Smpl Inc. Consistent Change Management practices are required to ensure security and accountability. The company's change management procedures can be found here:

# 8. Vendor workforce security

All of Rocket Rounding's employees and contractor workforce is located in the United States. This includes all remote services performed by employees or contractors.

# 9. Authentication and authorization

Rocket Rounding supports authentication and authorization through Google's Firebase Authentication services. This service supports the following:

a. Minimum password complexity no less than 6 characters. Custom solutions such password complexity policies that include specia alpha, numeric, case, and special characters should be defined by the organization utilizing the application.

b. Automated account lockout after a series of attempts. This is based on a series of variables determined to be a threat by Google Firebase admin. High frequency of attempts will lock a users account.

c. End-user initiated password changes

d. Solution supports password reset actions by a 3rd party and/or helpdesk analysts and require users to change their password at next login

e. The prevention of duplicate user accounts

f. Full protection of stored passwords through enforcement of cryptographic hashing. Rocket Rounding uses a password-based encryption utility from firebase that uses an internally modified version of scrypt to hash account passwords.

g. The ability to deactivate user accounts without deleting the target account

h. The ability for security administrators to suspend all access of a terminated user without affecting other users of the process / service / solution

Does not support

a. Enforces changing of passwords at least every 90 days

b. Automated user password resets based on correct answers to pre-defined security questions

# 10. Audit logs

Google Cloud Platform and its Firebase platform-as-a-service have admin activity audit logs. These record operations that modify and configuration or metadata in the application. These cannot be disabled and can only be accessed while logged into Google Cloud Platform.

**User audit logs**

A client can request that user audit logs are explicitly enabled on the platform at additional cost. At this point, Firebase Management writes Data Access audit logs. Data Access audit logs contain API calls that read the configuration or metadata of resources, as well as user-driven API calls that create, modify, or read user-provided resource data. Data Access audit logs do not record the data-access operations on resources that are publicly shared (available to All Users or All Authenticated Users) or that can be accessed without logging into Google Cloud Platform.

https://firebase.google.com/support/guides/cloud-audit-logging/firebase-management

*Note, Rocket Rounding  does not currently provide a way for our audit logs to be integrated into a 3rd-party information event management system.

# 11. Application security and data segmentation

a. **Security and data segmentation:**

Rocket Rounding has segregated development, staging, and production environments.

I. **Development** – strictly used for developer access to test new functionality and/or test patch fixes based on customer and internal bug reports.

II. **Staging** – strictly used for developer and end-user testing of new functionality and/or test patch fixes based on customer and internal bug reports.

III. **Production** – Strictly used by customers for performing the intended use of the application.

# 12. Antivirus software

Rocket Rounding uses Google Cloud Platform servers, which are protected by the most up-to-date anti-virus software

# 13. Server locations

Rocket Rounding uses Google Cloud Platform servers. These servers are physically located in the United States and outside the United States. This provides redundancy and guaranteed uptime for all of Rocket Rounding's products. Google is a global company and cannot guarantee that all data is stored on servers in the United States.

# 14. Application security and access controls

Rocket Rounding can verify that all systems hosting our applications are protected by two-factor authentication. Use of generic passwords and system-level accounts that cannot be attributed to a single user are not used. Vendor and employee account provisioning is handled based on job descriptions and job duties. Periodic audits are performed by administrative leaders to ensure all system level access is granted to only the appropriate individuals. There is no policy or procedure in place to require these periodic audits, as those with such access is highly limited to only a few individuals in the company, and access is immediately terminated when an employee or vendor is no longer employed or contracted with the organization.

Moreover, should issues be identified, Rocket Rounding administrators have the ability to disable the application in its entirety or disable a customer location and/or network should an issue arise where all customer access needs to be disabled.

# 15. Application security physical controls

Rocket Rounding uses Google Cloud Platform infrastructure and hosting, which is located in a highly secure data center facility. From google:

“Google data centers feature a layered security model, including safeguards like custom-designed electronic access cards, alarms, vehicle access barriers, perimeter fencing, metal detectors, and biometrics. The data center floor features laser beam intrusion detection.

Our data centers are monitored 24/7 by high-resolution interior and exterior cameras that can detect and track intruders. Access logs, activity records, and camera footage are reviewed in case an incident occurs. Data centers are also routinely patrolled by experienced security guards who have undergone rigorous background checks and training. Fewer than one percent of Googlers will ever set foot in one of our data centers.”
https://cloud.google.com/security/overview

When a client is no longer using the Rocket Rounding Application, their application network is set to a disabled state. The application requires a 30-day waiting period before any of the data can be destroyed and removed from the application. At the request of the client, the data can be deleted from the application. All backup media referencing client data is then removed from any backup media.

From google: “When retired from Google’s systems, hard disks containing customer information are subjected to a data destruction process before leaving Google’s premises. First, disks are

logically wiped by authorized individuals using a process approved by the Google Security Team. Then, another authorized individual performs a second inspection to confirm that the disk has been successfully wiped. These erase results are logged by the drive's serial number for tracking. Finally, the erased drive is released to inventory for reuse and redeployment. If the drive cannot be erased due to hardware failure, it is securely stored until it can be physically destroyed. Each facility is audited on a weekly basis to monitor compliance with the disk erase policy." https://cloud.google.com/security/overview

# 16. Application security network controls

Rocket Rounding uses Google Cloud Platform infrastructure and hosting, which uses the most up-to-date network security controls. Including, but not limited to:

i. Secured Service APIs and Authenticated Access

ii. Logging

iii. Data Encryption

iv. Secure Global Network

v. Intrusion detection

vi. Security scanning

All of the above are properly managed and maintained under Google Cloud Platform. More can be found here: https://cloud.google.com/security/overview

# 17. Vulnerability management and critical patches

Rocket Rounding ensures the frameworks it utilizes are up-to-date and are compatible versions that have long-term-support for security patches to address any vulnerabilities. Moreover, Google Cloud Platform performs independent security audits and management of critical network and server patches within 30-days of their release.

## 18. Endpoint protection

Rocket Rounding uses Google Cloud Platform endpoints, which are protected using best practices.

## 19. Network communication encryption

Rocket Rounding uses HTTPS and SSL for all network transmission. Google Cloud Platform also encrypts all customer data at rest. For more information: https://cloud.google.com/security/overview

## 20. Dedicated information security experts

Rocket Rounding has a dedicated information security professional consultant to aid, assist, and review all information security policies to make sure they adhere to best practices.

## 21. Cyber liability insurance

Rocket Rounding and its parent company Smpl Inc. carry cyber liability insurance underwritten by The Hartford. An organization requiring cyber liability insurance can be added to the policy by contacting our legal representative.