The Receptionist for iPad

Security Overview

How does the iPad Receptionist store information?

We've taken extra care in building a secure visitor management system that you can feel confident capturing and storing your contacts information as well as your visitor details. All information is stored on a secure AWS Amazon server via the Heroku hosting environment.

Is the information between the iPad and the server encrypted?

Yes! All traffic to the application from the iPad and browser is encrypted using HTTPS. The connection is encrypted using AES_256_CBC, with SHA1 for message authentication and DHE_RSA as the key exchange mechanism.

Is my credit card information safe?

Yes! All your billing information is safe. None of your Credit Card information is stored in the iPad Receptionist database or by the application. All of our payment processing is managed by Recurly and they are PCI-DSS Level 1 compliant (https://docs.recurly.com/pci-dss-compliance).

Will my contacts' information be used by the iPad Receptionist in any way?

Absolutely not! You don't have to worry about any of your information being used or sold. We never contact your list of contacts directly unless needed for customer support related issues. We send out periodic emails to the email address associated with your account to inform your team of App Updates or important status details that may affect your account. If for any reason you'd like to be removed from the mailing list, simply unsubscribe at any time.
At The iPad Receptionist, nothing is more important to our company than the privacy of and integrity of our customer's data. The iPad Receptionist takes precautions including administrative, technical, and physical measures to safeguard your personal information against loss, theft, and misuse, as well as unauthorized access, disclosure, alteration, and destruction. The The iPad Receptionist web application and database is a cloud-based, service hosted on Saleforce.com's, Heroku Cloud Application Service. As a Heroku customer our application and customer data is protected using the following Security Assessments and Practices.

Penetration Testing and Vulnerability Assessments

The iPad Receptionist employs two layers of vulnerability assessment:

> *Third party security testing of the Heroku application is performed by independent and reputable security consulting firms. Findings from each assessment are reviewed with the assessors, risk ranked, and assigned to the responsible team.*
>
> *We use CodeClimate to perform code analysis and security assessments of our application prior to deploying to production. Findings from this tool are tracked as bugs in our backlog, and are prioritized based on risk against the other features that are currently being developed.*

Physical Security

Heroku utilizes ISO 27001 and FISMA certified data centers managed by Amazon. You can learn more about their security capabilities by visiting https://www.heroku.com/policy/security. Amazon has many years of experience in designing, constructing, and operating large-scale data centers. This experience has been applied to the AWS platform and infrastructure. AWS data centers are housed in nondescript facilities, and critical facilities have extensive setback and military grade perimeter control berms as well as other natural boundary protection. Physical access is strictly controlled both at the perimeter and at building ingress points by professional security staff utilizing video surveillance, state of the art intrusion detection systems, and other electronic means. Authorized staff must pass two-factor authentication no fewer than three times to access data center floors. All visitors and contractors are required to present identification and are signed in and continually escorted by authorized staff.

Amazon only provides data center access and information to employees who have a legitimate business need for such privileges. When an employee no longer has a business need for these privileges, his or her access is immediately revoked, even if they continue to be an employee of Amazon or Amazon Web Services. All physical and electronic access to data centers by Amazon employees is logged and audited routinely. For additional information see: https://aws.amazon.com/security

Data Encryption

Heroku's Continuous Protection is designed to keep your data safe, secure, and available. With the launch of Heroku Postgres DbX, Continuous Protection ensures encryption-at-rest on all databases. Continuous Protection also keeps our database available. By performing 20 diagnostics health checks to their databases every 30 seconds, Continuous Protection monitors that our database is up and running to meet our applications' needs. And if a diagnostic should fail then automated systems repair the database, automatically. Continuous Protection also helps to keep your data secure. These safety measures include paranoid system configurations, automatic security patch application (often before exploits are publicly announced), regular intrusion tests, required enforcement of impossible-to-guess database credentials, and required SSL-encrypted connections from all outside clients. Encrypting all data at rest allows Heroku to comply with the most stringent security requirements. In the exceedingly unlikely event of a physical breach of our underlying infrastructure (i.e., if someone broke into the datacenter and removed the disk drives), your data would remain safe and secure.

For any additional information on our security practices please feel free to reach out to us directly.