Remind Security Overview

UNLIKE EMAIL, STANDARD TEXT MESSAGES, and systems like robocall or autodialers—which often aren't compliant with regulations like FERPA and COPPA—Remind is a messaging app built for education.

With Remind, a user's personal contact information stays private and isn't shared without user permission. Remind saves all communication to user accounts, which allows teachers, administrators, and participants to access a complete message history at any time. Verified school administrators on Remind also have the ability to manage staff accounts, review participant lists and basic usage statistics, and request message history directly.

The privacy and security of personal information in the school environment is a top priority for Remind. To enhance our users' security, Remind employs two kinds of security features, those that are user-facing and those that are embedded in our service. Our approach is guided by three principles:

Control
Our users, including school administrators, own their data and control their experiences.

Transparency
We work hard to protect user information and invest in auditing, improving, and sharing our practices.

Safety
We believe online safety is a shared responsibility, and we actively collaborate with our community to keep the Remind experience safe.

This paper provides a current overview of the state of Remind's security. Our approach takes advantage of advanced cloud computing practices while maintaining strict policies to ensure the security and integrity of the data we manage. Remind is committed to working with administrators, third-party auditors, penetration testing firms, and policy advisors to continually strengthen our investments across all aspects of our security.

Overview

Security on Remind consists of five critical components. These enable us to maintain data security and integrity on multiple levels for data entry, transfer, storage, and access:

- Corporate governance
- Physical security
- Environmental security
- Software security
- Regulatory compliance

Corporate Governance

Educators and families entrust Remind with important and highly sensitive information, which drives our commitment to the security of all information stored on our computer systems. This includes policies that guide the behavior of our employees, some of which are outlined below.

- All Remind employees and contractors sign agreements that require them to preserve and protect the confidentiality of sensitive information they may access while doing their jobs.
- All Remind employees are scrutinized by mandatory background checks.
- Employees are required to enable two-factor authentication in every internal and external service where two-factor authentication is made available and practical.

- All computers and mobile devices issued by Remind, as well as any software that runs on those machines, are encrypted where possible and password-protected.
- We work with industry-leading auditors to review and guide our security policies and procedures. We undertook NIST Cybersecurity Framework Gap Analysis with NCC Group and obtained safety certification from iKeepSafe.
- All employees receive privacy and security training at least annually.

Physical Security

Physical access to user information is strictly controlled.

- All Remind premises require key card entry.
- Remind does not require the on-site storage of any personally identifiable information (cloud-based storage).
- All work computers and laptops provided to Remind personnel have encrypted disks.

Environmental Security

Remind uses Amazon Web Services (AWS) and other third-party services within the AWS environment to host and operate its databases. AWS is an industry-leading cloud service platform that provides Remind with nondescript facilities, professional security staff, controlled access, video surveillance, intrusion detection, and other security features. All data is separated from outside connections, and access is limited to select, current members of the Remind team.

- Remind stores its data within an AWS region that is FedRAMP compliant.
- Remind's main database and all backups are encrypted at rest.
- The AWS cloud infrastructure has been designed and managed in compliance with regulations, standards, and best-practices, including HIPPA, SOC 1/SSAE 16/ISAE 3402 (formerly SAS70), SOC 2, SOC 3, PCI DSS Level 1, ISO 27001, FedRAMP, DIACAP and FISMA, ITAR, FIPS 140-2, CSA, and MPAA.
- Learn more about Amazon's security policies.

Software Security

Remind's infrastructure is built on industry-tested technology and security practices.

- Remind uses encryption, firewall, and network security software.
- Remind uses single sign-on (SSO) and two-factor authentication (TFA).
- Any VPN access to Remind systems requires SSO and TFA. VPN access is required for many services, including remote access (through SSH) to production servers and management tools.
- Logging into confidential parts of company systems requires time-limited SSH keys generated by classified users. All SSH requests are logged for auditing.
- Low-level auditing software is run on all systems to record potentially malicious actions that may take place.
- Remind runs periodic penetration tests, then logs and resolves discovered issues.
- All Remind clients use TLS/SSL when communicating with our servers.
- Remind has a host-based intrusion detection system to detect unauthorized access to production hosts.
- Audit logs are sent to a central location for storage and analysis. Access to production servers and interaction with production systems is audited and logged

Remind's designated Incident Response Manager, Jason Fischl (VP of Engineering), is in charge of handling the response to data breaches. The Incident Response Team can be reached at security@remindhq.com.

Regulatory Compliance

Given the sensitive nature of student and education data, Remind understands the importance of meeting the legislative requirements of COPPA and TCPA as well as helping schools comply with federal FERPA regulations.

At Remind, the security and privacy of student information are paramount. To provide safe, simple, and secure messaging for schools, Remind is committed to following industry best practices in regards to accessing, collecting, and transferring data. Remind's security-centered approach should help schools comply with federal mandates like FERPA and remain confident in the integrity and security of their data.