Security Policies and Responsible Disclosure

Recora treats data security as a top priority and incorporates many strategies to ensure the security of our patients' and our customers' data. If you believe you've found a security vulnerability in any of Recora's software, please notify us. We will work with you to ensure that the issue is promptly remediated.

Disclosure Policy

- If you discover a potential vulnerability, please let us know by emailing security@recorahealth.com, you will receive an acknowledgement within 7 days.
- Provide us with a reasonable amount of time to remediate the issue prior to public disclosure. Our internal SLAs require remediation of critical issues within 30 days.
- We request that you make a good faith effort to avoid violating privacy, degrading Recora's service, or destroying Recora's data.
- Please limit interaction to only accounts you own or for which you have explicit permission to access from the account holder.

Exclusions

Recora asks that researchers, users, and others refrain from performing:

- Spamming
- Social Engineering
- Phishing
- Distributed Denial of Service (DDoS) attacks
- Attacks against Recora's property or data

Contact

The Recora Security Team can be contacted at security@recorahealth.com.