

Robocall Mitigation Plan

[REDACTED ORGANIZATION]

Date: [REDACTED]

Executive Summary

[REDACTED ORGANIZATION] recognizes the importance of robust robocall mitigation to protect patients, providers, and stakeholders. This plan details our approach to preventing, detecting, and mitigating illegal robocalls in compliance with federal regulations.

Introduction & Scope

This document outlines the robocall mitigation strategy, ensuring adherence to the TRACED Act, STIR/SHAKEN framework, and FCC guidelines. It covers:

- Technical measures
- Policy measures
- Ongoing monitoring
- Response protocols

Regulatory Framework

- TRACED Act (2019)
- STIR/SHAKEN
- TCPA (Telephone Consumer Protection Act)
- FCC (Federal Communications Commission)

Robocall Mitigation Measures

4.1 Technical Measures:

- Caller ID Authentication
- Call Analytics
- Traffic Monitoring
- Number Validation
- Blacklisting

4.2 Policy Measures:

- Consent Verification
- Internal Controls
- Training
- Third-Party Vetting

Monitoring & Compliance

- Audit Logs: Maintain call logs and system records for at least 12 months.
- Periodic Reviews: Perform quarterly reviews of robocall mitigation effectiveness.
- External Audits: Engage third-party audits annually to validate compliance.
- Reporting: Promptly report suspected illegal robocall activity to the FCC.

Incident Response Plan

- Investigation
- Containment
- Notification
- Remediation
- Post-Incident Review

Conclusion

[REDACTED ORGANIZATION] is committed to maintaining the integrity of its communication systems and ensuring compliance with robocall mitigation standards. Our plan leverages technical and policy safeguards to reduce the risk of fraudulent robocalls.

Contact

[REDACTED]