



Robocall Mitigation Plan Patient Engagement Centers of America d/b/a PEC360

Legal Entity Patient Engagement Centers of America LLC	D/B/A PEC360	Industry Healthcare SaaS / Patient Communications
Plan Effective Date 2026.07.01	Review Cycle Annual, or upon material change	Plan Owner CTO, Chief Compliance, Privacy, and Security Officer

Introduction

Patient Engagement Centers of America d/b/a PEC360 is committed to providing secure and reliable communication services that enhance public health engagement and appointment management. This Robocall Mitigation Plan ["Plan"] details PEC360's approach to managing voice traffic to prevent the origination of illegal robocall traffic, spoofed caller ID, or unsolicited spam calling regulatory requirements.

Because PEC360 traffic frequently carries Protected Health Information (PHI), this Plan is designed to satisfy telecom compliance obligations without compromising HIPAA Privacy and Security Rule safeguards; all monitoring and enforcement mechanisms described below operate on call metadata and consent/authorization records rather than PHI content.

Terms and Conditions

All PEC360 clients are required to agree to and adhere to PEC360 Terms and Conditions, which strictly prohibits unethical, deceptive, or misleading practices, including the use of our services for telemarketing, unsolicited messages, or any spam-related activities.

Service Overview

PEC360 provides a HIPAA-compliant healthcare SaaS platform that enables covered entities and business associates ("Customers") to communicate with patients related to automated patient appointment reminders via voice API infrastructure provided by Bandwidth, Inc.

Mitigation Strategy

PEC360 does not originate or permit high-risk, unverified telemarketing traffic on our platform. To prevent platform abuse, PEC360 maintains several onboarding strategies to mitigate the risk of robocalls:

- * Verification of customer identity and purpose before onboarding to ensure legitimacy.
- * All customers must be USA based.
- * Corporate Verification: Every Customer using the PEC360 platform must submit a verified Employer Identification Number (EIN) and a physical address.

PEC360 also maintains several systematic protection and platform controls to mitigate the risk of robocalls:

- * Structural Mitigation: PEC360 does not offer open, unrestricted dialing. PEC360 operates a closed, single-purpose software application. Customers cannot upload unverified contact lists or alter call variables.



* No Ad-Hoc Messaging: The software application does not permit manual, ad-hoc dialing or arbitrary message generation by end-users. All voice triggers are entirely systemic, tied directly to confirmed patient healthcare appointments.

* Complete Number Ownership: We do not allow our customers to set caller id themselves. All outbound Caller ID numbers are natively provisioned, owned, and assigned by PEC360 via our upstream tier-1 carrier (Bandwidth). Customers are technically restricted from spoofing or inputting external numbers.

* Call Volume: Each PEC360 Client is limited to the number of concurrent calls that are allowed, preventing any mass calls beyond their specific verified use cases. Volume limits are set to 20 to 80 completed calls per minute.

CDR Monitoring:

* Routine monitoring of customer traffic with special scrutiny of short-duration calls. Average call lengths need to be above a certain threshold.

Partnership with Bandwidth for STIR/SHAKEN Compliance

* PEC360 does not operate its own facilities-based telecommunications core or hold independent STI-GA tokens. PEC360 routes 100% of our outbound voice traffic via SIP trunking/APIs to Bandwidth, Inc. Bandwidth executes STIR/SHAKEN cryptographic signing on our behalf. PEC360 passes all necessary Caller ID verification data to Bandwidth to ensure compliant Attestation levels.

* PEC360 and Bandwidth maintain a compliant status within the FCC's Robocall Mitigation Database, reflecting our commitment to regulatory standards.

Client Engagement and Responsibility

* All answered calls include the ability to opt out and all opt-out requests are automatically applied to prevent future messaging.

* Any clients found in violation of PEC360's Acceptable Use Policy will face immediate suspension or termination of PEC360 services.

Ongoing Commitment

* PEC360 is dedicated to continuous improvement of robocall mitigation tactics, including regular reviews of policies and technologies to adapt to evolving threats and regulatory changes.

* Per FCC requirements, PEC360 will cooperate with the Industry Traceback Group (ITG) and federal authorities. PEC360 pledges to respond to all traceback requests within 24 hours.

Contact Information

For any questions or reports related to robocall activity or misuse of service(s), clients and regulatory bodies can contact PEC360 through the following:

- Email: ellen.brown@pec360.com
- Phone: 843.345.2036
- Address: Patient Engagement Centers of America d/b/a PEC360, 334 E. Bay Street, Ste G PMB 245, Charleston, SC 29401-1592



Certification

PEC360 certifies that this plan is in effect and that PEC360 is committed to complying with all FCC requirements regarding robocall mitigation. PEC360 will submit and maintain this certification in the FCC's Robocall Mitigation Database.