Health-ISAC®
Collaborating for Resilience in Health

Emerging SMS/Voice OTP Toll Fraud via Account Sign-up and Patient Portal Flows

Threat Bulletins	**TLP:WHITE**	**Alert Id: b1ee9ba0**	**2026-01-13 13:30:47**

Health-ISAC is tracking an emerging fraud pattern where threat actors exploit SMS and voice One-Time Password (OTP) mechanisms used in account sign-up, patient portal enrollment, telehealth registration, and MFA flows. Attackers mass-create bogus accounts and then repeatedly abuse OTP resend and password reset functions to generate large volumes of SMS and voice calls to premium-rate or high-cost international numbers under their control.

This technique results in direct financial losses from elevated telecommunications charges, potential service disruption, and reputational damage with carriers and patients. It is highly likely that healthcare organizations with lightly protected OTP flows and global SMS/voice reach are at elevated risk.

Members are strongly encouraged to review OTP implementations, implement rate limiting and high-risk destination controls, and establish telecom monitoring and anomaly detection for OTP traffic.

Call to Action & Information Sharing

Health-ISAC encourages members to:

- Report suspected or confirmed OTP toll fraud incidents (including anonymized cost ranges, country codes, and number prefixes) through established Health-ISAC channels.
- Share IOCs/IOAs such as:
  - Destination country codes and prefixes
  - Suspicious carriers
  - IP ranges and ASNs used to drive OTP abuse
- Engage in collaborative working groups focused on:
  - Fraud and abuse of patient-facing digital channels
  - Telehealth security and resilience

2. Threat Overview

2.1 Fraud Technique

Threat actors:

1. Identify healthcare and telehealth services that use SMS/voice OTP for:
   - New patient sign-up or portal enrollment
   - Telehealth account creation
   - Password reset / account recovery
   - MFA / step-up verification
2. Use automation (bots, scripts, headless browsers) to:
   - Create numerous fake or low-value accounts
   - Submit phone numbers they control, such as:
     - Premium-rate numbers
     - International high-cost destinations
     - SIM farms or VOIP numbers with advantageous termination rates
3. Repeatedly trigger OTP delivery using:
   - “Send code” during sign-up
   - “Resend code” / “Didn’t get the code?”
   - “Forgot password” / “Reset password”
   - Alternate channels (switching between SMS and voice OTP)
4. The healthcare organization (or its SMS/voice provider) sends a high volume of OTP messages and calls, incurring:

    - Per-message or per-minute charges
    - Monthly cost spikes and potential threshold overages
5. The attacker (or complicit telecom partners) monetizes this traffic through revenue-sharing or premium-rate arrangements.

2.2 Why Healthcare and Telehealth Are Attractive Targets

- Widespread use of phone-based OTP to “simplify” patient access and meet usability expectations.
- Rapid digital transformation (telehealth, remote monitoring, online scheduling) where security and fraud models may lag behind.
- Patient portals often:
    - Support sign-up with minimal friction
    - Do not apply advanced fraud controls typical in banking/fintech
- Telecom cost visibility is often siloed in procurement or finance, not in the security or fraud team.

---

3. Healthcare & Telehealth Attack Scenarios

Scenario 1: Patient Portal Mass Sign-up

- Threat actor targets an HDO’s patient portal sign-up page.
- Uses disposable email addresses and random names/DoB to create fake “patients.”
- Provides premium-rate mobile numbers hosted in a high-cost jurisdiction.
- Rapidly cycles through sign-up attempts and “resend OTP” to drive thousands of SMS messages over a short period.
- Impact: Sudden, unexplained increase in monthly SMS costs; potential throttling by SMS providers; confusion for operations teams.

Scenario 2: Telehealth App Registration & Password Reset

- Telehealth platform allows global users with SMS/voice OTP for account registration and password reset.
- Attackers create many accounts linked to numbers in specific country codes/prefixes and repeatedly:
    - Trigger password reset for the same accounts
    - Request OTP delivery alternately via SMS and via call
- Impact: High voice call termination costs, especially if calls are billed per minute with minimum durations.

Scenario 3: mHealth/Remote Monitoring App Onboarding

- Consumer-facing mHealth app or remote monitoring platform uses OTP for device enrollment and pairing.
- Enrollments from suspicious geographies and proxies lead to a surge in OTP to countries where the organization has minimal or no real patient presence.
- Impact: Fraudulent telecom spend; possible service degradation if providers throttle or block traffic due to suspected abuse.

---

4. Indicators of Abuse (IoA / IoC)

4.1 Application & API-Level Indicators

- Large spikes in OTP requests on:
    - /signup, /register, /enroll, /verify-phone, /send-otp, or /reset-password endpoints.
- Very low completion rates:
    - High number of OTP sends, but:
        - Few accounts complete enrollment
        - Few logins or downstream “normal” behaviors (e.g., viewing records, scheduling appointments).
- Excessive OTP events per phone number:
    - Dozens/hundreds of OTP messages or calls to the same number per hour/day.
- Multiple accounts linked to similar or sequential phone numbers:
    - Numbers share the same country code and long prefix (e.g., first 6–7 digits).
- High concentration of disposable email domains or obviously auto-generated identities involved in OTP flows.

4.2 Telecom & Billing Indicators

- Sudden increase in SMS/voice spend over baseline, especially:
    - Specific country codes or international destinations
    - Specific carrier identifiers/routes
- High volume of OTP traffic to countries where:
    - The healthcare organization has limited or no patient base, or
    - Telehealth services are not officially offered.

- Abnormal proportion of voice OTP vs. historical baseline, especially if:
    - Voice calls are more expensive and monetized by attackers.
- Clusters of traffic to number ranges known to be premium-rate or associated with previous fraud activity.

4.3 Network & Infrastructure Indicators

- Concentrated OTP-triggering traffic from:
    - Data center IP ranges
    - Known VPN/proxy ASNs
- Limited device diversity:
    - Identical user-agents, missing device attributes, or repeated fingerprints across many “different” accounts.

---

5. Affected Services and Stakeholders

- Patient Portals / EHR Web Access
    - MyChart-like portals and similar systems that support direct patient self-enrollment or phone-based verification.
- Telehealth & Virtual Care Platforms
    - Video consultation platforms, digital front doors, remote triage services.
- mHealth Apps / Wellness Platforms
    - Mobile applications for chronic condition management, remote monitoring, digital therapeutics.
- Contact Centers with OTP Flows
    - IVR or agent-assisted flows that trigger OTPs during identity verification.

Key stakeholders: Information Security, Application/Product Owners, Telehealth Leadership, Revenue Cycle/Finance (telecom spend), Fraud/Risk, and Vendor Management.

---

6. Mitigation Strategies

6.1 Design & Access Control (NIST CSF: Protect / CIS Controls)

1. Rate Limiting & Throttling
    - Per phone number:
        - Example: Max 3 OTP sends per number per 15 minutes; max 10 per day.
    - Per IP / device:
        - Example: Max 10 OTP-related requests per IP per hour across all accounts.
    - Per account:
        - Example: Limit password reset requests to 3 per 24 hours.
2. High-Risk Destination Management
    - Restrict OTP delivery to:
        - Countries/regions where you have legitimate patient populations or licensed operations.
    - Maintain:
        - A denylist or “step-up verification” list for:
            - Premium-rate ranges and suspicious prefixes
            - High-fraud countries for telecom abuse
    - For heavily domestic organizations:
        - Consider blocking international OTP outright unless a specific business requirement exists.
3. Enhance Sign-up / Enrollment Proofing
    - Use CAPTCHAs or bot mitigation for sign-up and password reset workflows.
    - Validate:
        - Email patterns (disposable domains)
        - IP reputation and geolocation (e.g., residential vs. data center)
    - Consider requiring additional proof for:
        - New accounts registering from high-risk IP/regions
        - Phone numbers flagged as VOIP, virtual, or known risky ranges.
4. OTP Resend Controls
    - Implement cool-down timers:
        - Example: Resend allowed only once every 60–120 seconds.
    - Limit total number of resends per registration or per session.
    - Clearly communicate to users that repeated resends may be blocked for security.
5. Phone Number Intelligence
    - Where possible, integrate with services that classify:
        - Number type: mobile vs. landline vs. VOIP vs. premium.
    - Apply stricter rules or require alternative verification for VOIP and premium-type numbers.

6.2 Monitoring & Detection (NIST CSF: Detect / CIS Logging & Monitoring)

1. Metrics to Track
    - Number of OTP requests:

        - By endpoint (sign-up, reset, login, device enrollment)
        - By country code/prefix
        - By IP/ASN and device fingerprint
    - Conversion metrics:
        - OTP sent → account successfully activated
        - OTP sent → user logged in within X hours
    - Cost metrics:
        - Daily/weekly telecom spend
        - Cost per country, provider, and number type.
2. SIEM Detection Use Cases
   Below are example rules/patterns (pseudo-SIEM syntax):
3. Rule 1: Excessive OTP per Phone Number
   ```
   WHEN count(otp_requests) BY phone_number OVER 15m > 5
   THEN alert("OTP toll fraud suspected: high volume per phone number")
   ```
4. Rule 2: Spike in OTP to a Single Country
   ```
   WHEN current_1h_otp_to_country(COUNTRY_CODE) >
        3 * avg_otp_to_country(COUNTRY_CODE, last_7d, same_hour)
   AND COUNTRY_CODE not in approved_high_volume_countries
   THEN alert("OTP anomaly: spike to country " + COUNTRY_CODE)
   ```
5. Rule 3: High OTP Volume from Data Center IPs
   ```
   WHEN count(otp_requests) BY src_ip OVER 30m > 20
   AND src_ip_category == "hosting/datacenter"
   THEN alert("Potential OTP abuse from data center IP " + src_ip)
   ```
6. Rule 4: Low Conversion Rate Alert
   ```
   WHEN otp_sent(last_1h) > threshold_min_volume
   AND activation_rate(last_1h) < 20% of baseline_activation_rate
   THEN alert("Significant OTP usage with abnormally low activation rate")
   ```
7. Rule 5: Voice OTP Anomaly
   ```
   WHEN voice_otp_volume(last_1h) > 2 * avg_voice_otp(last_7d, same_hour)
   THEN alert("Voice OTP spike may indicate toll fraud")
   ```
8. Billing and Provider Alerts
    - Request your SMS/voice providers to:
        - Enable spend thresholds with automated alerts and temporary route blocking.
        - Provide near real-time dashboards and API access for:
            - Country-level spend
            - Number-level anomalies and suspected premium-rate abuse.

6.3 Response & Containment (NIST CSF: Respond)

- Immediate Actions on Suspicion or Detection
    - Temporarily:
        - Block affected country codes/prefixes
        - Increase rate limiting thresholds globally and per phone number
    - Coordinate with:
        - Telecom/SMS providers to:
            - Suspend suspected premium routes
            - Review recent traffic and charges
    - Identify impacted:
        - Accounts, phone numbers, IPs, and endpoints
    - Estimate financial exposure and rapidly escalate to:
        - Security leadership
        - Finance / procurement
        - Legal/Compliance as needed.
- Post-Incident Hardening
    - Incorporate lessons learned into:
        - WAF rules
        - API gateway policies
        - OTP implementation standards
    - Update:
        - SIEM rules
        - Dashboards

        - Thresholds and allow/deny lists.

---

7. Recommended API-Level Thresholds & Controls (Examples)

These are illustrative and should be tuned to each organization’s traffic profile:

- Per Phone Number:
    - <= 3 OTP sends per 15 minutes
    - <= 8–10 OTP sends per 24 hours
- Per IP Address:
    - <= 20 OTP-related requests per 30 minutes
    - Stricter limits for IPs categorized as hosting/data center addresses
- Per Account (Registration + Reset):
    - Sign-up: <= 3 OTP sends per registration attempt
    - Password reset: <= 3 OTP sends per account per 24 hours
- Per Country Code:
    - Set a per-day maximum OTP volume per country based on:
        - Historical patient distribution
        - Telehealth expansion plans
    - For non-core markets:
        - Low thresholds with auto-block + alert on exceedance.
- Global Spend Caps:
    - Define daily and monthly telecom spend limits with:
        - Automated alert at 70–80% of threshold
        - Hard stop at 100% threshold, with manual override if explained by legitimate events (e.g., major campaign).

---

8. Governance, Policy, and Vendor Management

- Explicitly classify telecom/OTP fraud as a financial and operational risk in:
    - Enterprise risk registers
    - Digital front door and telehealth risk assessments
- Require in SMS/voice provider contracts:
    - Fraud detection and anomaly alerting
    - Spend caps and emergency route shutoff capabilities
    - Support for premium-range and high-risk prefix blocking.
- Incorporate OTP/toll fraud scenarios into:
    - Secure SDLC and threat modeling for new patient-facing apps
    - Red team / purple team exercises (e.g., simulated OTP flooding from multiple IPs).

Recommendations:
9. Recommendations for Health-ISAC Members

- Short Term (0–30 Days)
    - Identify all applications using SMS/voice OTP (patient portals, telehealth apps, mHealth, internal portals).
    - Implement basic rate limiting on OTP APIs and set preliminary country-level thresholds.
    - Review last 3–6 months of telecom/SMS billing for:
        - Sudden spikes
        - Unusual destinations or routes.
- Medium Term (1–6 Months)
    - Integrate OTP events into your SIEM and establish anomaly-based alerts.
    - Work with telecom/SMS providers to:
        - Restrict or monitor high-risk routes
        - Implement spend caps and “kill switches.”
    - Enhance sign-up and reset flows with stronger bot and abuse controls.
- Long Term (6–18 Months)
    - Mature to risk-based OTP with multi-factor checks (IP reputation, device fingerprinting, number intelligence).
    - Where feasible, expand beyond SMS/voice OTP toward:
        - App-based push approvals
        - FIDO2/WebAuthn for staff and high-risk transactions.
    - Participate in Health-ISAC information sharing on:
        - Fraudulent prefixes, carriers, and IP indicators
        - Case studies and best practices for OTP fraud mitigation.

TLP:WHITE: Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Conferences, Webinars, and Summits:

https://h-isac.org/events/

Share Threat Intel:

For guidance on sharing indicators with Health-ISAC via HTIP, please visit the Knowledge Base article "HTIP - Share Threat Intel" here.

The "Share Threat Intel" feature allows for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

Turn off Categories:

For guidance on disabling alert categories, please visit the Knowledge Base article "HTIP Alert Categories" here.

RFI Handling - Request to Distribute To Members::

The Health-ISAC Threat Operations Center is asking that recipients redistribute this message to your membership and either aggregate the responses or have them respond directly to toc@h-isac.org.

For Questions or Comments:

Please email us at toc@h-isac.org