Robocall Mitigation Program Description

Humworld Inc. (HumHealth) | Filed in the FCC Robocall Mitigation Database | Version 1.0 | November 2026

1. Overview and scope of calling

Humworld Inc. ("HumHealth") provides a care-management software platform, offered through its HumHealth website, to healthcare practices and facilities ("Customers"). The platform is designed to let authorized Customer users place calls to their own patients from HumHealth's website. HumHealth's voice function is not an open calling service, a predictive or automatic dialer, or a telemarketing tool.

HumHealth currently uses Plivo and plans to use Bandwidth Inc. for calling. This program describes calling through Bandwidth. HumHealth will enable calling for a Customer only after the Customer has accepted HumHealth's calling terms and conditions and its Calling Acceptable Use Policy.

Calls will be made only for patient care and care coordination, such as follow-up on a care plan, an appointment or a callback. Each call will be started by a person from a patient record, to a telephone number held in that Customer's own patient records.

The platform may not be used for illegal robocalls, caller ID spoofing, fraud, telemarketing (including prerecorded or artificial-voice telemarketing), lead generation, debt collection, political calling or consumer marketing.

A call starts in the user's web browser and connects through the calling service of HumHealth's upstream provider, which carries the call to the patient's telephone number on the public telephone network.

Incoming calls to a facility's HumHealth telephone number will be forwarded through HumHealth's upstream provider to a single telephone number that the Customer sets for that facility. HumHealth will not use incoming call forwarding to place calls to anyone else, and forwarding will not use prerecorded or artificial-voice messages.

2. Role in the call chain and STIR/SHAKEN status

HumHealth acts as a voice service provider without a STIR/SHAKEN implementation obligation. It has not implemented STIR/SHAKEN on any portion of a network it controls. HumHealth does not own, operate or lease telecommunications network infrastructure, does not operate telephone switches, SIP trunks or session border controllers, does not interconnect directly with other carriers, and holds no SPC token and no STIR/SHAKEN certificate.

The basis is that HumHealth lacks control over the network infrastructure necessary to implement STIR/SHAKEN, as described in 47 CFR 64.6305(d)(2)(i). HumHealth does not rely on an expired small-provider extension. HumHealth's upstream provider carries the call and signs it on its own network at the attestation level it assigns. HumHealth's position rests on its lack of control over the network infrastructure, not on that signing. Not having implemented STIR/SHAKEN does not reduce HumHealth's duty to maintain this program and to cooperate with traceback and enforcement requests.

3. Call controls

Before calling is enabled for any Customer, HumHealth will have these controls in place:

- Authorized users only. Only authenticated users of an approved Customer will be able to place calls. Calling will be a permission granted by role and limited to patients on the user's care team or facility. Access will be removed when a user's role changes or ends.
- Person-initiated calls. Each call will be started individually by a user from a patient record, to a number on that patient's record. The platform will not use an automatic telephone dialing system and will not send prerecorded or artificial-voice calls. Users will not be able to upload call lists or generate bulk calls.
- Caller ID control. The number shown to the patient will be set by HumHealth's servers, not by the user's browser. It will be limited to telephone numbers assigned to the Customer's facility on HumHealth's accounts with its upstream providers. Users will not be able to enter or change the caller ID, and caller ID will not be altered or spoofed.
- Call records. For each call, including forwarded calls, HumHealth will record the facility, the user, the date and time, the number called, the caller ID shown and the call length. These records will identify who placed any call and support traceback.
- Patient privacy. Monitoring for robocall mitigation will use call metadata and will not require access to the content of calls.

4. Customer identification and acceptable use (47 CFR 64.1200(n)(4))

Before calling is enabled for a Customer, HumHealth will identify the Customer by facility name and National Provider Identifier (NPI), as entered by the Customer. As part of its agreement with HumHealth, the Customer must accept HumHealth's calling terms and conditions and HumHealth's Calling Acceptable Use Policy ("AUP"). The administrator who sets up the facility accepts both on the Customer's behalf and confirms that they are authorized to do so. This is the Customer's agreement to enable calling. Calling will stay disabled for a facility until that agreement is recorded. HumHealth records each Customer's acceptance of the calling terms and the AUP. The calling terms and the AUP require the Customer and its users to use calling only for lawful patient-care purposes; to comply with the Telephone Consumer Protection Act, the FCC's robocall rules and applicable privacy law; not to make illegal robocalls, prerecorded or artificial-voice calls without the required consent, or calls for telemarketing or lead generation; not to spoof caller ID or use any number not assigned by HumHealth; and not to share logins. The Customer agrees to cooperate with

traceback requests. HumHealth will not onboard telemarketing dialer operators, lead-generation callers or other high-risk robocall business models. HumHealth may suspend or terminate calling for violations of the AUP and may share information with law enforcement and regulators.

5. Upstream provider

HumHealth sends calls to the public telephone network only through its upstream providers. Before sending traffic through a provider, HumHealth confirms that the provider is listed in the Robocall Mitigation Database. HumHealth will review notices from its upstream providers about authentication, traffic or the Robocall Mitigation Database and respond to them. If HumHealth adds or changes a provider, it will review the new provider for lawful calling, traceability and robocall mitigation before sending traffic, and will update this program and its filing.

6. Monitoring and analytics

HumHealth will review call activity by user and by facility using its call records and the reporting available from its upstream providers. Indicators it will look for include unusual call volume or sudden spikes, a high share of very short calls, calls to many different unrelated numbers, calls that do not fit a patient-care use, and complaints, traceback requests or carrier notices. HumHealth does not operate its own call analytics system and will rely on the analytics and blocking that its upstream providers apply on their networks. It uses no separate third-party analytics vendor. If it engages one, it will update this program.

7. Investigation and enforcement

HumHealth will investigate suspected illegal or unauthorized calling promptly, whether it comes from its own monitoring, a customer review, a notice from an upstream provider, a complaint, a traceback request or a regulator. It will be able to suspend a user or a facility's calling, require corrective action, preserve the records, notify the upstream provider where appropriate and cooperate with the FCC, law enforcement and the Industry Traceback Group. Each action will be documented.

8. Traceback commitment

HumHealth commits to respond within 24 hours to all traceback requests from the Federal Communications Commission, law enforcement and the industry traceback consortium, and to cooperate with those entities in investigating and stopping any illegal robocallers that use its service to originate calls. The responsible contact is the Robocall Mitigation Contact named in HumHealth's filing in the Robocall Mitigation Database.

9. Recordkeeping

HumHealth will keep Customer account records, records of acceptance of the calling terms and the AUP, user permissions, call records, caller ID assignments, investigation and enforcement records and traceback responses, and will retain them as long as needed to respond to traceback requests and investigations and to meet applicable legal requirements.

10. Regulatory history

At no time in the prior two years has HumHealth, which has no parent company or subsidiaries, or any entity under common ownership, management, directors or control, been the subject of a formal Commission, law enforcement or regulatory agency action or investigation with accompanying findings of actual or suspected wrongdoing due to transmitting, encouraging, assisting or otherwise facilitating illegal robocalls or spoofing, or a deficient Robocall Mitigation Database certification or program description.

11. Ownership, review and updates

An officer of HumHealth, designated by its management, owns this program. It is reviewed at least once a year before the annual recertification, and whenever HumHealth's network role changes, it gains the ability or obligation to implement STIR/SHAKEN directly, it changes or adds an upstream provider, or it enables calling for a new Customer. HumHealth revises its filing within 10 business days of any change to the information in it.