

MHI Gateway

Error Codes Reference

Authoritative public API error vocabulary and response handling

Document version 1.0

Publication date 10 August 2026

Classification Public API reference

MICRO HEALTH INITIATIVE

Contents

Use this contents list or the PDF bookmark panel to navigate.

Contents	2
1. Error envelope	3
2. Complete public vocabulary	3
3. Detailed reference	4
AUTHENTICATION_FAILED - HTTP 401	4
FORBIDDEN - HTTP 403	4
INVALID_REQUEST - HTTP 400	4
INVALID_RECIPIENT - HTTP 422	4
INVALID_SENDER_ID - HTTP 422	4
MESSAGE_TOO_LONG - HTTP 422	4
IDEMPOTENCY_CONFLICT - HTTP 409	4
MESSAGE_NOT_FOUND - HTTP 404	4
WEBHOOK_CONFIGURATION_INVALID - HTTP 422	5
RATE_LIMIT_EXCEEDED - HTTP 429	5
USAGE_LIMIT_EXCEEDED - HTTP 429	5
SERVICE_UNAVAILABLE - HTTP 503	5
INTERNAL_ERROR - HTTP 500	5
4. The two HTTP 429 errors	5
5. Safe handling pattern	5
6. Source and scope	6

1. Error envelope

Request-level failures use one JSON envelope. The code is the stable value for program logic; messages and details are sanitized and may vary without changing the code.

```
{
  "error": {
    "code": "INVALID_REQUEST",
    "message": "The request payload is invalid.",
    "details": {},
    "correlation_id": "550e8400-e29b-41d4-a716-446655440000"
  }
}
```

Capture X-Request-ID and X-Correlation-ID response headers before handling the body, including on non-2xx responses.

2. Complete public vocabulary

HTTP	Public code	Meaning / developer response
401	AUTHENTICATION_FAILED	Credential is absent or invalid. Supply an active Bearer credential.
403	FORBIDDEN	The principal lacks permission. Request access or use the correct credential.
400	INVALID_REQUEST	Syntax, headers, or payload validation failed. Correct the request; do not blindly retry.
422	INVALID_RECIPIENT	The recipient is not accepted E.164 input. Correct the recipient.
422	INVALID_SENDER_ID	Sender ID is invalid or not assigned to the application. Use an active assigned Sender ID.
422	MESSAGE_TOO_LONG	Message exceeds 4096 characters. Shorten the message.
409	IDEMPOTENCY_CONFLICT	A key was reused with changed canonical input. Restore original input or use a new key for a new operation.
404	MESSAGE_NOT_FOUND	The public ID is absent from the authenticated scope. Verify the ID and credential scope.
422	WEBHOOK_CONFIGURATION_INVALID	Webhook URL or configuration validation failed. Correct the configuration.
429	RATE_LIMIT_EXCEEDED	Request-rate throttling prevented processing. Honor Retry-After and apply bounded backoff.
429	USAGE_LIMIT_EXCEEDED	A durable tenant or application SMS quota would be exceeded. Contact the tenant administrator; do not treat as transient throttling.
503	SERVICE_UNAVAILABLE	A transient dependency or service condition exists. Retry safely with bounded backoff and jitter.
500	INTERNAL_ERROR	The gateway encountered a sanitized internal failure. Retry only when safe and preserve the idempotency key.

3. Detailed reference

AUTHENTICATION_FAILED - HTTP 401

Public message: Authentication failed.

Meaning and common cause: Credential is absent or invalid.

Developer response: Supply an active Bearer credential.

FORBIDDEN - HTTP 403

Public message: The requested action is forbidden.

Meaning and common cause: The principal lacks permission.

Developer response: Request access or use the correct credential.

INVALID_REQUEST - HTTP 400

Public message: The request payload is invalid.

Meaning and common cause: Syntax, headers, or payload validation failed.

Developer response: Correct the request; do not blindly retry.

INVALID_RECIPIENT - HTTP 422

Public message: Recipient is invalid.

Meaning and common cause: The recipient is not accepted E.164 input.

Developer response: Correct the recipient.

INVALID_SENDER_ID - HTTP 422

Public message: Sender ID is invalid.

Meaning and common cause: Sender ID is invalid or not assigned to the application.

Developer response: Use an active assigned Sender ID.

MESSAGE_TOO_LONG - HTTP 422

Public message: Message exceeds the maximum length.

Meaning and common cause: Message exceeds 4096 characters.

Developer response: Shorten the message.

IDEMPOTENCY_CONFLICT - HTTP 409

Public message: The idempotency key is bound to a different request.

Meaning and common cause: A key was reused with changed canonical input.

Developer response: Restore original input or use a new key for a new operation.

MESSAGE_NOT_FOUND - HTTP 404

Public message: The requested message was not found.

Meaning and common cause: The public ID is absent from the authenticated scope.

Developer response: Verify the ID and credential scope.

WEBHOOK_CONFIGURATION_INVALID - HTTP 422

Public message: Webhook configuration is invalid.

Meaning and common cause: Webhook URL or configuration validation failed.

Developer response: Correct the configuration.

RATE_LIMIT_EXCEEDED - HTTP 429

Public message: The rate limit has been exceeded.

Meaning and common cause: Request-rate throttling prevented processing.

Developer response: Honor Retry-After and apply bounded backoff.

USAGE_LIMIT_EXCEEDED - HTTP 429

Public message: The outbound SMS usage limit has been exceeded.

Meaning and common cause: A durable tenant or application SMS quota would be exceeded.

Developer response: Contact the tenant administrator; do not treat as transient throttling.

SERVICE_UNAVAILABLE - HTTP 503

Public message: Service is temporarily unavailable.

Meaning and common cause: A transient dependency or service condition exists.

Developer response: Retry safely with bounded backoff and jitter.

INTERNAL_ERROR - HTTP 500

Public message: An internal error occurred.

Meaning and common cause: The gateway encountered a sanitized internal failure.

Developer response: Retry only when safe and preserve the idempotency key.

4. The two HTTP 429 errors

Code	What it means	Correct response
RATE_LIMIT_EXCEEDED	Request-rate throttling. This is about request frequency.	Honor Retry-After when present and use bounded backoff.
USAGE_LIMIT_EXCEEDED	Durable outbound SMS quota at tenant or application scope.	Do not retry as throttling. Contact the tenant administrator; details remain empty.

The gateway does not disclose current usage, configured limits, another application's usage, or the exact failed quota scope.

5. Safe handling pattern

- Branch on `error.code` and interpret it with the HTTP status and endpoint context.
- Treat details as optional structured assistance, never as a source of secrets.

- Do not retry authentication, authorization, validation, not-found, or idempotency conflicts without correcting the cause.
- For transient transport failures, 500, or 503, use bounded exponential backoff with jitter.
- For message submissions, retain the original body and Idempotency-Key across safe retries.

6. Source and scope

The vocabulary and statuses are derived from the approved public API contract and its OpenAPI error schema. Messages shown are public, sanitized examples; the OpenAPI operation response lists remain authoritative for which statuses apply to each endpoint.