Consent

Overview

If your organization is enabled, when a message is dispatched via API, consent can be verified against one or more consent agreements. The agreements to verify are determined via the consent element array of objects in your request body using codes as keys.

Example snippet from dispatch request body

```
{
    . . .
    "consent": [
        {
            "code": "MARKETING",
            "respect": true
        },
        {
            "code": "CONSENT",
            "respect": false
        }
    ],
    . . .
}
```

⬅ A custom consent agreement MARKETING has been added and caller wishes to respect this consent.

⬅ The reserved consent agreement CONSENT has explicitly been set to false. Messages will deliver in clear-text regardless of settings in the patient's profile.

New codes are determined by you as maintained via API using `consentAgreementUpsert`. However, two consent agreement codes are **reserved** by OhMD: **SMS** and **CONSENT**. These two codes affect text message delivery.

Code	Default Consent Decision[5]	SMS Opt-In Keyword(s)	SMS Opt-Out Keyword(s)	Grantee	Grantor	Description
SMS[6]	PERMIT	START UNSTOP	STOP	DEVICE	DEVICE	Controls whether any text message is permissible to send to the phone number. This is the master consent required by all mobile network operators.
CONSENT	DENY	CONSENT	**None**. May be toggled in the OhMD App.	DEVICE	DEVICE	Determines if messages are sent via private links or as clear-text text messages.

[5] In the `consent` object, this element is called `decision` and the enumeration PERMIT and DENY in deference to standard FHIR terminology. In practice PERMIT is often called **default "Opt-Out",** DENY, **default "Opt-In"**.
[6] The SMS code affects all text messages whether the actual protocol is SMS, MMS, or RCS.

You can maintain reserved consent agreements via API calls, but you cannot create a consent agreement using a reserved code or you will receive an error. **NOTE:** Although you can revoke SMS consent via API (e.g. STOP), **you cannot grant (e.g. START/UNSTOP) SMS consent via API. The patient must send START or UNSTOP from their mobile device to opt back in. This rule is enforced by the mobile network operators.**

Additionally you cannot choose to verify SMS – it is always verified as required by the mobile network operators whether you include SMS in your consent array or not.

Opt-In / opt-Out keywords associated with the reserved codes SMS and CONSENT are also reserved and cannot be specified as a keyword in custom consent agreements.

Default Consent Decision

Each consent agreement has a default consent decision, either PERMIT or DENY.

A default DENY consent agreement is in force without patients taking any action to execute the agreement. Examples include a consent to perform surgery and OhMD's own consent to receive clear-text SMS communications from your organization; one cannot commence a surgery or send a clear-text SMS unless consent is granted.[7]

Other consent agreements may default to PERMIT. These are in force without the patient taking any action. Examples Include disclosures of health information to public health authorities, participation in record sharing to other treating providers, etc. Unless one revokes consent, one is presumed to have consented. The SMS consent agreement is a default PERMIT agreement because an organization is free to send a patient SMS messages unless the patient texts STOP from their mobile device.

It's important to know if your consent defaults to PERMIT or DENY because it affects what you need to send in the consent object via API. Default DENY consent agreements must explicitly be set to `false` or they will be enforced.

Consent Grantor and Grantee

Consent is given or revoked by a grantor to a grantee. Healthcare organizations usually think of the grantor as the patient. However, due to the unique nature of mobile devices, the grantor (or generally in application, the revoker) of consent may be the **device**. This is because a phone that sends a STOP or START message opts in / opts out the device for all patients associated with the phone number. When a mother sends a STOP message from her mobile

[7] Whether the CONSENT consent agreement is in force by default at your organization is established at the time you onboard with OhMD.

phone, she is also denying consent for any messaging to a son or daughter who is associated with that phone number. LIkewise, OhMD considers the CONSENT consent agreement to be a device consent — if a patient responds CONSENT from his or her device, all patients associated with that device have opted in to receiving clear text SMS messages from that phone number at the organization.

Typically consent maintained by your organization will be grantor=PATIENT, grantee= ORGANIZATION; most healthcare agreements are between an individual and an organization. This is an important distinction to understand when engaging with patients via SMS. You may have received consent from your patients to receive electronic communications and recorded that in your EHR, but an individual may override that at the device level via a STOP keyword and this cannot be overridden.

A patient-to-device consent is not a valid type due to its inherent overlap with patient-to-organization consents. If an organization has more than one phone number, the phone numbers are likely assigned to particular departments (Cardiology vs. Psychiatry) or particular use cases (appointment reminders vs. lab results notifications).

Custom Consent

Organizations may add an unlimited number of custom consent agreements via API. Adding a custom agreement allows organizations to specify during dispatch which OhMD managed consents are required. Once a custom consent agreement is created, you cannot change its consent parties nor its default consent decision.

Some organizations may choose to manage consent entirely inside their systems and withhold dispatch based upon consent maintained in your source system rather than using OhMD's consent features. However, note that **SMS consent cannot be maintained inside your own system** because OhMD must abide by mobile network operating rules. If you choose to maintain other consents, you still must check for SMS consent or you may receive an error during dispatch.

Consent API Examples

Create a New Consent Agreement `consentAgreementUpsert`

Practice wishes to send lab results to patients. Legal department insists on receiving consent before sending via SMS any PDFs containing lab results. Organization administrator sets up a new consent type.

```
POST /api/consentAgreementUpsert HTTP/1.1
Content-Type: application/json
x-api-key: K2H5E8Z9A9W9GK9VFGSRZHDS4Z31GHEG199CD9Z3S5BT230HZFATA
x-api-secret: S4P4ZGY68R78YBTWGNBTNQC3Y136AZJ7VA8399XPV8M9B9Q5PSZB2
x-organization-id: 01HGH4Z0F1CEKG1PA6M2AGPZFZ
{
   "code": "LABS",
   "grantor": "PATIENT",
   "grantee": "ORGANIZATION",
   "longName": "Lab Results",
   "description": "Patient consents to receive lab results as a PDF via text.",
   "decision": "PERMIT",
   "consentInterval": "2 years",
   "en": {
       "requestTemplate": "{{patient.preferredName}}: Dr. Jones would like to request your consent to receive
lab results via SMS. SMS messages are unencrypted and may disclose health information to anyone who can access
your mobile device. Consent to receive these messages will remain in effect {{#if
consent.effectiveUntil}}}until {{consent.effectiveUntil}}{{else}}indefinitely{{/if}} unless you type OPTOUT
LABS. To consent type OPTIN LABS. To stop all messages from {{organization.name}} type STOP.",
       "permitResponseTemplate": "Thank you for consenting to receive lab result messages.",
       "denyResponseTemplate": "You will not receive lab results via SMS. To opt back in, type OPTIN LABS",
       "permitResponse": [
           "OPTIN LABS"
       ],
       "denyResponse": [
           "OPTOUT LABS"
       ]
   }
}
```

Start Consent Workflow `consentWorkflowStart`

After creating a consent agreement via API, practice wishes to start the consent SMS workflow for two patients.

```
POST /api/consentWorkflowStart HTTP/1.1
Content-Type: application/json
x-api-key: K2H5E8Z9A9W9GK9VFGSRZHDS4Z31GHEG199CD9Z3S5BT230HZFATA
x-api-secret: S4P4ZGY68R78YBTWGNBTNQC3Y136AZJ7VA8399XPV8M9B9Q5PSZB2
x-organization-id: 01HGH4Z0F1CEKG1PA6M2AGPZFZ
{
   "recipient": [
       {
           "identifier": {
               "id": "2000"
           }
       },
       {
           "identifier": {
               "id": "2001"
           }
       }
   ]
}
```

Set Consent Gained Via 3rd Party Method

`consentUpsert`

Practice hosts an opt-in form on its website for gaining consent. This operates outside of the OhMD SMS consent workflow and practice needs to update consent so messages can send. No expiration date is set, so the agreement remains in effect indefinitely.

```
POST /api/consentUpsert HTTP/1.1
Content-Type: application/json
x-api-key: K2H5E8Z9A9W9GK9VFGSRZHDS4Z31GHEG199CD9Z3S5BT230HZFATA
x-api-secret: S4P4ZGY68R78YBTWGNBTNQC3Y136AZJ7VA8399XPV8M9B9Q5PSZB2
x-organization-id: 01HGH4Z0F1CEKG1PA6M2AGPZFZ
{
   "recipient": [
       {
           "identifier": {
               "id": "2000"
           }
       }
   ],
   "consent": {
       "code": "LABS",
       "status":"ACTIVE",
       "effectiveDate":"2023-10-10"
   }
}
```