imprivata®

# Product Documentation

## Epic Implementation Guide

Imprivata Patient Access

*Last Updated: February 2025*

## Contacting Imprivata

20 CityPoint, 480 Totten Pond Road, 6th Floor

Waltham, MA 02451 USA

Phone: 781-674-2700

Toll-Free: 1-877-OneSign

Fax: 1 781 674 2760

Support: 1 800 935 5958 (North America)

Support: 001 408-987-6072 (Outside North America)

https://www.imprivata.com

support@imprivata.com

## Copyright and Legal Information



## Trademark Information



## Legal Notices



Document revision

# Table of Contents


**Overview** ..... **4**
Documentation Resources ..... 4
**Project Planning** ..... **6**
**App Request Process** ..... **8**
Overview ..... 8
Customer Steps ..... 8
Before Starting the Request Process ..... 8
Obtain the open.epic API Subscription Agreement ..... 8
Obtain the Imprivata Patient Access Apps ..... 8
Request an App ..... 9
Enable External Authentication in Epic ..... 9
Imprivata Steps ..... 9
Configuration for Imprivata Patient Access Application ..... 9
Configuration for Imprivata Patient Access – Photo Upload Application ..... 10
Get Assistance ..... 10
**Implementing Patient Access SMART on FHIR Launch** ..... **11**
Information to Send to the Customer ..... 11
Information to Obtain from the Customer ..... 11
Configure the FHIR Integration in Patient Access ..... 11
**Implementing Patient Access Photo Upload** ..... **12**
Information to Send to the Customer ..... 12
Information to Obtain from the Customer ..... 12
Configure the HL7 Integration in Patient Access ..... 13
Create the HL7 System ..... 13
Add an HL7 Rule ..... 13
**Epic External Authentication Report** ..... **14**

# Overview

Imprivata Patient Access leverages the Epic[1] Generic Authentication framework to initiate external patient authentication, subsequently returning the authenticated patient to Epic. Following activation by the Generic Authentication framework, Imprivata Patient Access executes a standalone SMART on FHIR launch to enable secure authentication and data exchange with the Epic FHIR server. Additionally, Imprivata Patient Access uses the backend OAuth 2.0 for authentication with the customer's HL7 interface, facilitating secure photo uploads to Epic.

This documentation focuses on the steps required to enable and configure SMART on FHIR launch and photo upload in your environment. For instructions on configuring generic authentication, see Patient Lookup Setup and Support Guide.

To integrate with the SMART on FHIR and backend OAuth 2.0 technologies on Epic's platform, Imprivata Patient Access has registered two applications on the Epic Vendor Service website.

Epic customers must request, download, and implement the **Imprivata Patient Access** application in their environments. The **Imprivata Patient Access - Photo Upload** application is optional, so if the Epic customer wants that feature, they must request, download, and implement both applications.

Below are the application names and client IDs required during the application request process.

**Client IDs**

| Application Name | Non-production Client ID | Production Client ID | Description |
|---|---|---|---|
| Imprivata Patient Access | 303a4d28-aad2-48af-a40d-f3cc3c1c825f | 233370ff-7785-4d83-8753-9477f5331dbf | Allows Imprivata Patient Access to perform standalone SMART on FHIR launch<br>Required to enable the main workflows of Imprivata Patient Access. |
| Imprivata Patient Access – Photo Upload | e2673269-0ebe-4ed9-99cd-3ddf5b72ba12 | 8b3dfe11-91be-421b-80ae-cb53f8d7cf09 | Allows Imprivata Patient Access to upload photos to customer using HL7 via HTTPs.<br>This is an optional feature. |

**Epic ProgID**

**ProgID:** Imprivata.PatientAccess.EpicDesktop

The ProgID is used by Epic to determine which application to call when a biometric workflow for patient identification is triggered from within Epic.

This specific ProgID will cause Epic to invoke the Imprivata Patient Access Epic Connector in such workflows, enabling communication between Epic and the Imprivata Patient Access Registrar Client.

# Documentation Resources

Review the following Epic documentation and tutorials, available from the Epic UserWeb for your organization:

- Implementation Strategy Handbook
- Patient Lookup Setup and Support Guide

[1]Epic is a registered trademark of Epic Systems Corporation.

- Getting Started with HL7 Interfaces tutorial

# Project Planning

The table below details some fundamental tasks that both the customer and Imprivata may need to undertake during the integration installation. The **Who Should Be Involved** column lists broader groups for readability, but here are more specific details about the stakeholders included in each of these groups:

- **Imprivata stakeholders:** Project leadership, implementation team, technical team
- **Customer Operational stakeholders:** Operational leadership, super users, subject matter experts
- **Customer IT Stakeholders:** Point person for Client ID downloads, Epic[1] Application analysts and TS (for the applications that own the workflow that integrates with Imprivata apps), Interface administrator and Epic EDI, ECSA (Web & Service Servers administrator) and Epic Client Systems TS, ECSA (Citrix and Desktop administrator) and Epic Client Systems TS, Users & security team, Training team (for the application that owns the workflow that integrates with the app being installed, if the app requires changes to the user workflows), Epic Technical Coordinator and Best Friends Forever (BFF) (optional).

| Task | Who should be involved | Description |
|---|---|---|
| Project prioritization and contracting | • Operational leadership<br>• IT leadership<br>• Imprivata leadership | The organization has communicated interest in the Imprivata Patient Access product to Imprivata leadership and the project is ready to begin. |
| Kickoff call | • Operational stakeholders<br>• IT stakeholders<br>• Imprivata stakeholders | Identify who should be involved, designate responsibilities, and set initial timelines for the project. |
| App request process | • Point person for client ID downloads<br>• Imprivata administrator | To initiate the app implementation process, someone from the customer organization will request to download the Imprivata Patient Access apps.<br>See App Request Process section for details. |
| User and security setup | Users & security team | Configure users and security as required by the integration. This requirement is integration and technology specific. It will be fully owned by the customer organization. |
| Interface setup | Interface administrator and Epic EDI | Configure the required interfaces as needed the photo upload app.<br>Imprivata must communicate the Interface Type, triggering, and field-level message requirements to the customer organization.<br>See Implementing Patient Access Photo Upload for more information.<br>Skip this step if the photo upload feature is not needed. |
| Interconnect setup | ECSA (Web & Service Servers administrator) and Epic Client Systems TS | Configure the web services server as needed by the app. They can look at Imprivata apps' client IDs to determine the API requirements. |
| Allow content | ECSA (Citrix and Desktop administrator) and Epic Client Systems TS | Configuration that allows Imprivata apps to communicate with Epic software from outside the customer organization's firewall and function appropriately. |

[1]Epic is a registered trademark of Epic Systems Corporation.

| Task | Who should be involved | Description |
|---|---|---|
| Application build | Application analyst and TS | Configuration that allows Imprivata apps to work well with relevant Epic application user workflows.<br>This requirement is integration and technology specific. See Implementing Patient Access Smart on FHIR Launch for more information about how to approach this communication. |
| End-to-end testing | • Application analyst and TS<br>• Imprivata implementation team | Test standard and edge case workflows to ensure Imprivata Patient Access is working as expected. |
| Training | • Application analyst and training team<br>• Imprivata implementation team | Train users how to use Imprivata Patient Access and the changes to their Epic workflow. |
| Cut over to Production | All involved stakeholders | Prepare to go live. Move all relevant build in Epic and outside system configuration from test environments to production. |

# App Request Process

## Overview

Every Epic[1] community member has at least one user with the **Able to Purchase Apps** security role, which allows them to download an app on behalf of their organization. Customers should identify the user with this security role and complete the App Request Process.

If a customer is unsure who holds this role, they should contact their Epic representative or email VendorServicesTS@epic.com for assistance.

Customers can download Imprivata Patient Access applications from the Showroom page.

## Customer Steps

### Before Starting the Request Process

Customer project teams should refer to their Epic Implementation Strategy Handbook, which is accessible only to community members. This handbook provides a comprehensive guide for planning an app implementation project.

### Obtain the open.epic API Subscription Agreement

Epic customers who wish to use a third-party application registered on the open.epic website must sign the open.epic API Subscription Agreement.

### Obtain the Imprivata Patient Access Apps

1. The user with **Able to Purchase Apps** security should visit the Showroom page and locate the Imprivata Patient Access application by entering application name **Imprivata Patient Access**. The application will be found with a “Request Application” option available.
2. If the photo upload feature will be implemented, the customer can search for the **Imprivata Patient Access – Photo Upload** application using the app’s client IDs provided earlier in this document.

   Both non-production and production client IDs can be used for the search. The application will be found with a **Request Client ID** option available.

The app details page for each application provides information about the app, displays any previous app versions, and allows users with **Able to Purchase Apps** security the option to proceed with the download.

Imprivata apps use access and refresh tokens, and the duration of these tokens can be specified during this process.

[1]Epic is a registered trademark of Epic Systems Corporation.

## Request an App

When a customer clicks **Request Client ID** or **Request Application** for the app needed, an email notification is sent to the Imprivata Epic Vendor Administrator for approval before the client IDs are synced.

The Imprivata Administrator must enable keys for the integration to function correctly. See the section below for actions required from the Imprivata side.

## Enable External Authentication in Epic

The Imprivata Patient Access app is launched based on actions taken within Epic. The information in this section provides recommendations for how the customer should configure buttons and workflows with their Epic team. For detailed information about configuring Epic, see the *Epic Patient Look-up and Support Guide* section "Enable External Authentication and Lookup Devices".

- **Look up window.** Authenticate button in lower left corner. Used in multiple workflows.
- **Patient station.** Enroll and Authentication buttons on the toolbar.
- **Appointment desk.** Enroll and Authentication buttons on the toolbar.
- **ED arrival.** Enroll and Authentication buttons on the toolbar.
- **DAR.**
  - Enroll and Authentication buttons on the toolbar.
  - Include Enroll and Authentication options from the right-click context menu that appears when you select the patient from the DAR.

# Imprivata Steps

1. After an Epic customer requests a client ID, the Imprivata Epic Vendor Administrator will enable keys for that member.
2. The Imprivata Epic Vendor Administrator enables the keys by clicking **Activate for Non-Production** or **Activate for Production** for a customer on the Interested Organizations page in Vendor Services.
3. When enabling keys for an Epic customer, the Imprivata Administrator can specify additional configurations before approving the request. See the sections below.
4. Vendor Services sends an email to users with **Able to Purchase Apps** security, confirming the app download.

## Configuration for Imprivata Patient Access Application

To configure the Imprivata Patient Access application:

1. **Endpoint URL:** Imprivata Patient Access does not use an app-specific endpoint URL.

   The default endpoint URL (https://ps.sys.prod.imprivata.com/ps-provider-web/api/v3/fhir/callback) listed on the app configuration page should be used for all customer environments.
2. **JWK Set URL:** Imprivata Patient Access utilizes an app-specific JWK set URL.

Each customer environment should have a unique, tenant-specific JWK set URL, which can be found in the customer's Admin Console under the HL7 system page.

a. Navigate to **Integrations > HL7**, then click **Add HL7 System** and click **Copy JWK URL**.

## Configuration for Imprivata Patient Access – Photo Upload Application

To configure the Imprivata Patient Access - Photo Upload application:

1. **JWK Set URL:** Imprivata Patient Access utilizes an app-specific JWK set URL.

   Each customer environment should have a unique, tenant-specific JWK set URL, which can be found in the customer's Admin Console under the HL7 system page.

   a. Navigate to **Integrations > HL7**, then click **Add HL7 System** and click **Copy JWK URL**.

> **IMPORTANT:**
> The Imprivata Epic Vendor Administrator must first approve the app for non-production before it can be approved for production. The administrator can update configurations by clicking Update Non-Production Download or Update Production Download
>
> Only one environment type can be updated at a time.

Within twelve hours, client records with the app's client ID are created or updated in the Epic community member's environments. This is the final required step before the integration can be built.

# Get Assistance

If you encounter any issues with the app request process, contact VendorServicesTS@epic.com for assistance.

# Implementing Patient Access SMART on FHIR Launch

The Imprivata Patient Access App is launched directly to the authorize endpoint outside of an EHR session and requests context from the EHR's authorization server. The sections below provide instructions on what information is needed from both the customer and from Imprivata to enable the SMART on FHIR standalone launch.

## Information to Send to the Customer

1. **Client IDs** - The customer will use either the Non-Production or Production client ID in their SMART on FHIR configuration, depending on the environment.

Only the client IDs for the Imprivata Patient Access app are required for the customer to configure in their SMART on FHIR launch configuration.

| Application Name | Non-Production Client ID | Production Client ID |
|---|---|---|
| Imprivata Patient Access | 303a4d28-aad2-48af-a40d-f3cc3c1c825f | 233370ff-7785-4d83-8753-9477f5331dbf |

## Information to Obtain from the Customer

The customer coordinates with their Epic[1] team to obtain the following information:

1. **Technical Connection information** - The Interconnect instance base URL for FHIR API traffic.

   Example: https://vendorservices.epic.com/interconnect-amcurprd-oauth
2. **Data Mapping Requirements** - The FHIR OID for patient medical record number (MRN),

   Example: urn:oid:1.2.840.114350.1.13.0.1.7.5.737384.14

## Configure the FHIR Integration in Patient Access

With the information above, the Imprivata implementation engineer uses the customer's Patient Access Admin Console to configure the FHIR integration.

1. In the Patient Access admin console, navigate to **Integrations > FHIR**.
2. In the **Interconnect instance base URL** box, type the address of the interconnect instance base URL. The value is the {InterconnectInstanceBaseURL}/api/FHIR/R4.
3. In the **Client ID** box, type the client identifier for the FHIR service. If this is a test tenant, this is the non-production ID for the Imprivata Patient Access app. If this is the production tenant, this is the production client ID.
4. In the **FHIR OID** box, type the FHIR OID for patient medical record number (MRN).
5. In **System Type**, select **Epic**, then click **Save**.

[1]Epic is a registered trademark of Epic Systems Corporation.

# Implementing Patient Access Photo Upload

The Imprivata Patient Access – Photo Upload application is a backend FHIR application that sends patient photos to the customer's HL7v2 interface using OAuth 2.0 Backend Authentication. The customer's Interface team must set up the required HL7v2 interfaces and can contact their Epic[1] EDI support for assistance. For general guidance on implementing interfaces, see the Getting Started with HL7 Interfaces tutorial.

## Information to Send to the Customer

1. **Client IDs** - The customer will use either the Non-Production or Production client ID in their Backend OAuth 2.0 configuration, depending on the environment. The customer's IT team will map the client ID to an Epic user account for the purposes of auditing and providing security to invoke web service calls made by the backend application.

   Only the client IDs for the Imprivata Patient Access – Photo Upload app are required.

| Application Name | Non-production Client ID | Production Client ID |
|---|---|---|
| Imprivata Patient Access – Photo Upload | e2673269-0ebe-4ed9-99cd-3ddf5b72ba12 | 8b3dfe11-91be-421b-80ae-cb53f8d7cf09 |

2. **Interface the app requires -** HL7v2
3. **The communication method -** HL7v2 interfaces support HTTPS
4. **Description of interface filter criteria** - Imprivata sends an A31 event that contains the patient photo and MRN to HL7v2 interface via HTTPS.

   **Example**

```
MSH|^~\&|IMPRIVATA||test|test|20240723171010||ADT^A31||T|2.3
EVN|A31|20240723171010|
PID|1||3983^^^AssigningAuthority^MR|||||
OBX|1|ED|IJL||^^JPG^BASE64^{ImageBase64String}
```

## Information to Obtain from the Customer

The customer coordinates with their Epic team to obtain the following information:

1. **HL7v2 Interface endpoint (HTTPs)**

   Example: https://vendorservices.epic.com/interconnect-amcurprd-oauth/api/epic/2015/EDI/HTTP/HL7v2/12870103
2. **Technical Connection information** - The Interconnect instance base URL for FHIR API traffic.

   Example: https://vendorservices.epic.com/interconnect-amcurprd-oauth
3. **HL7 Message Field Mapping Requirements**

[1]Epic is a registered trademark of Epic Systems Corporation.

Receiving Facility: the expected values in MSH.5

Receiving Application: the expected values in MSH.6

MRN Assigning Authority: the expected values in PID.3.4

MRN Type Code: the expected values in PID.3.5

4. Data Mapping Requirements - The FHIR OID for patient medical record number (MRN)

   Example: urn:oid:1.2.840.114350.1.13.0.1.7.5.737384.14

# Configure the HL7 Integration in Patient Access

With the information above, the Imprivata implementation engineer uses the customer's Patient Access Admin Console to configure the HL7 integration.

## Create the HL7 System

1. In the Admin Console, navigate to **Integrations > HL7**. Click **Add HL7 system**.
2. In the **Client ID** box, type the client identifier for the service. If this is a test tenant, this is the non-production ID for the Imprivata Patient Access – Photo Upload app. If this is the production tenant, this is the production client ID.
3. In the **HL7v2 interface endpoint** box, type the address of the endpoint. The value is {HL7v2 interface HTTPS endpoint}.
4. In the **Token Endpoint** box, type the address of the endpoint. The value is {InterconnectInstanceBaseURL}/oauth2/token}.
5. In the **Receiving facility (MSH.5)** box, specify the receiving facility. The value is the expected value in MSH.5.
6. In the **Receiving application (MSH.6)** box, specify the receiving application. The value is the expected value in MSH.6.

## Add an HL7 Rule

Rules define the Patient Access events, such as Photo Added, that can trigger Patient Access to send messages.

HL7 Outbound rules must have patient identifiers configured to send within the HL7 message.

To add an HL7 rule:

1. Click **+ Add HL7 Rule.**
2. Specify the following information:
   a. **Friendly Name.** Enter a friendly name that describes the rule.
   b. **FHIR OID**. Enter the FHIR OID for patient medical record number (MRN).
   c. **HL7 identifier assigning authority (PID3.4)**. The expected value in PID.3.4.
   d. **HL7 identifier coding system (PID3.5)**. The expected value in PID.3.5.

# Epic External Authentication Report

Imprivata recommends that you engage your Epic[1] TS to get access to the **External Patient Authentication Report** from Cogito, which should be available in the report library for Reporting Workbench.

This report should provide you with the location information that you need.

**External Patient Authentication Report**

| Event Type | Patient Name | Patient MRN | User | Date/Time | Department | Reason |
|---|---|---|---|---|---|---|
| External patient authentication success | MyChart, Teddy | 202500 | Liddel, Alice | 04/23/2024 09:08:12 AM | EMH Surgery | |
| External patient authentication error | MyChart, Damon | 202499 | Liddel, Alice | 06/28/2024 09:51:29 AM | EMH Surgery | |
| External patient authentication failed | MyChart, Allie | 202497 | Liddel, Alice | 07/13/2024 12:32:26 PM | EMC Cardiology | |
| External patient authentication skip | MyChart, Christine | 202498 | Liddel, Alice | 07/28/2024 10:16:41 AM | EMH Surgery | Time Constraint |

| Epic Event Types | Patient Access User Activities |
|---|---|
| External patient authentication enrollment | Enrollment Success |
| External patient authentication lookup success | Identification Success |
| External patient authentication no search results | Identification Failed |
| External patient authentication lookup override | Identification Failed |
| External patient authentication lookup skip | Identification Cancelled |
| External patient authentication success | Verification Success or Verify to Enroll Success |
| External patient authentication failed | Verification Failed |
| External patient authentication failure override | Verification Failed |
| External patient authentication skip | Verification Cancelled |
| External patient authentication unknown patient warning | Verify to Enroll cancelled before enrollment submit |
| External patient authentication unknown patient used | Verify to Enroll cancelled before enrollment submit |
| External patient authentication error | Launch error |

[1]Epic is a registered trademark of Epic Systems Corporation.

**NOTE:**
Epic does not always use the same language that Imprivata uses in our Patient Access solution, and so Imprivata representatives prefer to be involved in calls and correspondence with Epic where possible, so that we can help you get the information that you need.