



UnifiMD 1.2 Patient Data API

This manual will assist software developers and other 3rd parties connect and extract patient data as well as walk you through the required setup to create a public and secure web server connected to your UnifiMD Database. We do recommend consulting with an experience Information Technology provider.

Table of Contents

- [Terms of Service](#)
- **Installation / Configuration**
 - a. [Enabling users inside of UnifiMD](#)
 - b. [Create a read only login to your SQL Server](#)
 - c. [Setting up a secure web server](#)
- **API Calls**
 - a. [Test Environment](#)
 - b. [Sample Application](#)
 - c. [Patient Identification and Selection](#)
 - d. [Data Category Requests](#)



Terms of Service

If you have any questions, please contact us at support@mailchs.com

Thank you for selecting Complete Healthcare Solutions. By using our software, demonstrations, data, subscription service and/or our website, you agree to comply with our Terms of Service, as stated herein. The software we license to you and the users in your business or organization is referred to as the "Service".

Your use of this Service is an unconditional acceptance of our Terms of Service; provided you have the legal capacity to enter into contracts for yourself or for your organization. You are required to provide current and accurate information as part of our account registration process. We reserve the right to change or modify our Terms of Service at any time without prior notice; however, we will post any new Terms of Service on our website.

I. ACCOUNT USE

All users must be 13 years or older to use this Service. Accounts and user logins may not be registered via automated methods. You may create separate logins for as many users as you need but sharing of user logins is not permitted. You must maintain the security of your account and all user passwords. You may not use this Service for any illegal or unauthorized purposes, such as violating third party copyrights. You are responsible for your account, user activities, and posted content. This service is for use only within the United States of America and the US Territories and thus not subject to the European Union General Data Protection Rule (GDPR).

III. MODIFICATIONS TO THE SERVICE

We reserve the right to modify or discontinue the Service (or any part thereof) with or without notice to you. We are not liable to you or any third party for any modification, price change, suspension or discontinuance of the Service.

IV. OWNERSHIP RIGHTS

Your profile and the content you provide to the Service remain yours. However, by sending your content to other users (via any of the available methods), you agree to allow others to view and share your content. You may not duplicate, copy, modify, or reuse any portion of the HTML/CSS or visual design elements without our prior, express written permission.

V. OTHER CONDITIONS

Your use of this Service is at your sole risk. The Service is provided on an "as is" and "as available" basis. Technical support is only provided to paying support customers. You agree not to violate our copyright and not to reproduce, duplicate, copy, sell, resell, modify or exploit any portion of the Service or access to this Service without our prior, express written permission. You must not store or post pornographic, obscene, defamatory, threatening or otherwise objectionable content, or content that violates any person's intellectual property or links to such content, through the Service. You must not transmit any malicious programs such as viruses, worms and other code or programs intended to inflict harm.



VI. DISCLAIMER OF WARRANTIES

THE SERVICE IS PROVIDED ON AN “AS IS” AND “AS AVAILABLE” BASIS. WE EXPRESSLY DISCLAIM ALL WARRANTIES AND CONDITIONS OF ANY KIND, WHETHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO THE IMPLIED WARRANTIES AND CONDITIONS OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. NO INFORMATION OR ASSISTANCE, WHETHER WRITTEN OR ORAL, PROVIDED BY US OR ANY THIRD PARTY TO YOU SHALL CREATE OR EXTEND ANY WARRANTY.

WE DO NOT WARRANT THAT OUR SERVICE WILL BE UNINTERRUPTED OR FREE OF ERRORS OR OMISSIONS AND WE DO NOT GUARANTEE THE PRIVACY, SECURITY, AUTHENTICITY AND NON-CORRUPTION OF ANY INFORMATION TRANSMITTED THROUGH THIS SERVICE OR THE INTERNET. WE SHALL NOT BE RESPONSIBLE FOR ANY DELAYS, ERRORS, FAILURE TO PERFORM, INTERRUPTIONS OR DISRUPTIONS IN THE SOFTWARE OR SERVICES CAUSED BY OR RESULTING FROM FORCE MAJEURE EVENTS, ACTS OF THIRD PARTIES, OMISSIONS OR CONDITIONS BEYOND OUR REASONABLE AND FORSEEABLE CONTROL.

VII. LIMITATIONS OF LIABILITY

We shall have no liability, whether under any legal theory of warranty, contract, tort (including our negligence or the negligence of any third party), strict liability, or otherwise, regarding the Service or other actions performed by us and relating in any way to this Terms of Service, except as specified in the HIPAA Business Associate Agreement. In no event shall we or any third parties be liable for any special, indirect, incidental, or consequential damage or loss of any nature (such as damages for delay, damage to property, lost profits, death or injury to person, or any claims of those not a party to this Agreement) which may arise in connection with the Service or other acts performed under or relating to this Terms of Service.

X. ENTIRE AGREEMENT

The Business Associate Agreement, our current Terms of Service, and our current End User License Agreement represent our entire agreement with you and supersede any prior agreements or prior terms of service or policies.

XI. APPLICABLE LAW & JURISDICTION

Our Terms of Service are subject to the governing laws of the State of Massachusetts. Only courts of competent jurisdiction in Palmer, Massachusetts shall have original jurisdiction over any disputes arising hereunder or relating to the Software or Services.

XII. Assignment

We may assign these Terms of Service to the surviving entity in a sale, merger or reorganization, or to any purchaser of all or substantially all of the assets of the business to which these Terms of Service relates, or to any affiliate of such entity. Subject to the foregoing, these Terms of Service shall be binding upon and inure to the benefits of the parties to these Terms of Service and their respective heirs, legal representatives, successors and permitted assigns.



Enabling Users inside of UnifiMD.

1. Click on the Configuration Menu
2. Click FHIR Access Logins
3. Click New
4. Enter a username, password and description describing the purpose of this login.
 - a. A new login should be created for each interface. Do not share logins, otherwise there will be no way to accurately audit
 - b. Use a strong password consisting of at least 12 characters that are a combination of letters, numbers and symbols (@, #, \$, %, etc). Use letters in both uppercase and lowercase.



Creating a SQL Server Read Only Login (You may require the assistance of your IT Admin or UnifiMD support team to complete this step)

1. Open SQL Server Management Studio. This should be installed on your server. If not installed, download instructions and links can be found here
 - a. <https://docs.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms?view=sql-server-2017>
2. Open Object Explorer from the View Menu
3. Expand Security
4. Right Click Logins and click New Login
5. Enter the Login Name
6. Choose SQL Server Authentication
7. Enter a Secure Password
8. Click the User Mapping Page
9. Select Your UnifiMD Practice database(s)
10. Select the user role of db_datareader



Setting up A Web Server in IIS (This step will likely require assistance from your IT Admin)

The methods for enabling a web server will vary depending on your operating system.

The methods for requesting a certificate will also vary on your operating system as well as your hosting provider.

1. Enable IIS on your web server
 - o For your reference here is an article to help you enable IIS on Server 2012
<https://www.atlantic.net/cloud-hosting/how-to-configure-iis-windows-server-2012/>
 2. Download the UnifiMD FHIR API web service files to your webserver. unifimdfhirapiwebservices.zip can be downloaded by clicking [here](#).
 3. After downloading UnifiMD, extract the files from the archive and place the ReleaseFHIR folder in C:\inetpub\.
 4. Open the file C:\inetpub\ReleaseFHIR\Web.config
 5. Find the value "DefaultConnectionString"
 - a. value="Data Source=**Enter your SQL server instance name here**;Initial
 - b. Catalog=**Enter your Unifi Practice Database Name Here**;
 - c. User ID=;Password= Enter the SQL Username and Password that you [created earlier in this guide](#).
 6. Order a new domain name or setup an existing one.
 7. Create an SSL Certificate Request in IIS and order an SSL Certificate to secure your site
 - o *Here is an article to setup an SSL Certificate with GoDaddy*
<https://www.godaddy.com/help/iis-10windows-server-2016-generate-csrs-certificate-signing-requests-27348>
- b. You can repeat these steps for each practice that you would like to enable API Access. Each database does require it's own unique site but they can be hosted on the same web server.

Recommendations:

Use a dedicated web server. Do not use a database server or workstation as your web server.

Place your webserver in a DMZ section of your network off of your domain

Disable SSL 2.0 and 3.0 on your web server

Disable TLS 1.0

Configure Secure Ciphers



Test Environment

A client may setup their own test environment by creating a 2nd database, and website, however CHS hosts an Interactive site that can be used for testing.

Visit <https://unifimdapi.com/unifimdapi/index>

User: Demo

Password: Demo

Patient Sample:

Unique ID: 415

Steve Lyashtuck

07/04/1943

Male

Test Application

A sample client application is available to download as well. [Click Here to download.](#)

Once downloaded and extracted, you can launch the sample application from CHSAPICalls\CHSAPICalls\bin\Debug\chsreference.exe.

You may test using the credentials in the CHS Sandbox above, or in production once the end user had completed the web server setup.

- a. [Enabling users inside of UnifiMD](#)
- b. [Create a read only login to your SQL Server](#)
- c. [Setting up a secure web server](#)



Patient Identification and Selection

- To test in the CHS Sandbox, you will need the URL, Credentials and Patient Sample located [here](#).
- To test in production with an end user, the web server setup described earlier in this manual must be complete.
 - d. [Enabling users inside of UnifiMD](#)
 - e. [Create a read only login to your SQL Server](#)
 - f. [Setting up a secure web server](#)

Functions

- [Authentication](#)
 - {"UserName":"demo","Password":"demo"}

The Get Patient ID's will return values based on the following demographics. The more data that is entered, the more specific your results will be.

- [POST /Patient/GetPatientIds](#)
 - {
 - "SNN": "",
 - "Birthdate": "1950-01-01",
 - "FirstName": "",
 - "LastName": "",
 - "Phone": "",
 - "Email": "someone@gmail.com",
 - "Sex": "M"
 - }

Once you have the Unique ID, all that is needed for the remaining calls is the ID Number in the API Call. In the example below "415" is the Unique ID representing a specific patient. That ID is all that is needed for any of the remaining API Category's.

415

The following syntax can be used with all of the following API Calls

```
{  
  "EndDate": "2018-10-09",  
  "PatientID": 415,  
  "StartDate": "2018-10-09"  
}
```

- [POST /Patient/GetProblems](#)
- [POST /Patient/GetProcedures](#)
- [POST /Patient/GetRiskAssessment](#)
- [POST /Patient/GetResults](#)
- [POST /Patient/GetEncounters](#)
- [POST /Patient/GetVitals](#)
- [POST /Patient/GetCarePlans](#)
- [POST /Patient/GetSocialHistory](#)
- [POST /Patient/GetMedications](#)



- [POST /Patient/GetMedicationDispense](#)
- [POST /Patient/GetMedicationAdministrered](#)
- [POST /Patient/GetAllergies](#)
- [POST /Patient/GetReferrals](#)
- [POST /Patient/GetImmunization](#)

The following API Call will return all patient data which will include all data from all API Calls.

- [POST /Patient/GetPatientAll](#)
{
- "EndDate": "2018-10-09",
- "PatientID": 415,
- "StartDate": "2017-10-09"
- }

Response Codes

200 – OK

401 – Failed Authentication

500 – Improperly Formatted Parameters

200 { "resourceType": "Bundle" } = Incorrect Patient Identifier