Capella Services

API Documentation for External Application Access

Version 6.0

Acurus Solutions Inc, 160 South Old Springs Road, Suite 280 Anaheim Hills, CA 92808. Tel: 714-221-6311, email: capellasupport@acurussolutions.com

Contents

1. Introduction

This guide is written for third party developers, including patients, who are developing software applications for accessing Protected Health Information (PHI) based on this documentation of an open API. This documentation allows applications to query a public-facing API enabled by a data holder. Data holders wishing to publish such a public-facing API should have their Health IT vendor register as a developer integrator of EMR Direct Interoperability Engine services at https://www.emrdirect.com/subscribe-developer.

ALWAYS KEEP IN MIND THAT ONLINE DATA TRANSFER IS NOT A SUBSTITUTE FOR PERSON-TO-PERSON COMMUNICATION OF URGENT OR CRITICAL MEDICAL INFORMATION.

This documentation also contains general information and important security information. General information will be marked as "Note:" and important security information will be marked as "IMPORTANT:".

2. General Concepts

a. Application Access Requests

The API is a read-only RESTful FHIR® STU 3 Ballot API and follows the syntax described at http://hl7.org/fhir/2016Sep/http.html.

All data access requests will be in the following format, in which the [base] URL will need to be obtained from the data holder, either directly or via directory information: GET [base]/[resource-specific parameters]…

b. Connecting to the server

The server is accessed by clients through an https connection.

IMPORTANT: Local customer security policies must be in place to prevent unauthorized monitoring or eavesdropping of connections to the server.

Note: Only SSL/TLS connections (TLS 1.0 or higher) are accepted. All plaintext connections will be refused.

Note: Please limit your connection frequency to a value appropriate for your use case. Connection attempts which are more frequent than permitted by the bandwidth allocation for the data resource are not allowed.

c. Authentication – Obtaining an Access Token

Client authentication can be performed using a username and strong password. A healthcare organization may reuse existing patient portal credentials for this purpose, in which case the authenticated username map to a unique patient portal user on the resource holder's side. The end user should obtain these credentials directly from the healthcare organizations from which they wish to access data.

Prior to making API requests, the client application must obtain an Access Token from the associated Authorization Server. The client software must support the OAuth 2.0 authorization code grant flow as detailed in RFC 6749. If the client application does not have a client ID and client secret for this purpose, the client application may obtain a client ID and client secret using the dynamic client registration protocol by submitting the required client information to the registration endpoint as detailed in RFC 7591.
Each healthcare organization will have a unique base URL to access its Authorization Server. The required endpoint URLs are as follows:

ENDPOINT	URL
Authorization	https://[baseOAuthURL]/authz
Token	https://[baseOAuthURL]/token
Registration	https://[baseOAuthURL]/register

When the end user is directed to the authorization endpoint, the user will be presented with a login screen where they can enter their credentials for the healthcare organization they are accessing. If the correct credentials are supplied and the end user grants access to the client application, an authorization code will be returned to the client that the client application can use to obtain an access token through the token endpoint.
All requests to the API must include the access token transmitted in the Authorization header of the HTTP request as a bearer token as illustrated in RFC 6749. If the access token is missing, expired, or otherwise not valid for the requested operation, the API will return a 401 Unauthorized response.

3. API Details

a. Query a Specific Data Category Resource

Client software must be capable of making HTTPS RESTful requests in accordance with the FHIR specification and consuming the following FHIR Resources in order to support the Common Clinical Data Set (CCDS):

Common Clinical Data set element	Resource	Resource data element (If Applicable)
Patient Name	Patient	
Sex	Patient	
Date of Birth	Patient	
Race	Patient	
Ethnicity	Patient	
Preferred Language	Patient	
Smoking Status	Observation	
Problems	Condition	
Medications	Medication Statement	
Medication Allergies	Allergy Intolerance	
Laboratory Tests	Observation	
Laboratory Values Results	Observation	
Vital Signs	Observation	
Procedures	Procedure	
Care Team Members	Care Team	
Immunizations	Immunization	

Unique Device Identifiers	Device
Assessment and Plan	Care Plan
Goals	Goal
Health Concerns	Condition

General specifications for FHIR resources and the associated data elements can be found at http://www.hl7.org/fhir/2016Sep/resourcelist.html. Additional information for the FHIR Resource or Data Element used to represent each data category can be found at the URLs listed in the following table:

COMMON CLINICAL DATA SET ELEMENT	RESOURCE OR DATA ELEMENT	URL FOR ADDITIONAL INFORMATION
Patient Name	Patient.name	http://hl7.org/fhir/2016Sep/patient-definitions.html#Patient.name
Sex	Patient.gender	http://hl7.org/fhir/2016Sep/patient-definitions.html#Patient.gender
Date of Birth	Patient.birthDate	http://hl7.org/fhir/2016Sep/patient-definitions.html#Patient.birthDate
Race	Patient.extension	http://hl7.org/fhir/2016Sep/extension-us-core-race.html
Ethnicity	Patient.extension	http://hl7.org/fhir/2016Sep/extension-us-core-ethnicity.html
Preferred Language	Patient.communication	http://hl7.org/fhir/2016Sep/patient-definitions.html#Patient.communication
Smoking Status	Observation	http://hl7.org/fhir/2016Sep/observation.html
Problems	Condition	http://hl7.org/fhir/2016Sep/condition.html
Medications	MedicationStatement	http://hl7.org/fhir/2016Sep/medicationstatement.html

Medication Allergies	AllergyIntolerance	http://hl7.org/fhir/2016Sep/allergyintolerance.html
Laboratory Tests	Observation.code	http://hl7.org/fhir/2016Sep/observation-definitions.html#Observation.code
Laboratory Values Results	Observation.value[x]	http://hl7.org/fhir/2016Sep/observation-definitions.html#Observation.value_x_
Vital Signs	Observation	http://hl7.org/fhir/2016Sep/observation.html
Procedures	Procedure	http://hl7.org/fhir/2016Sep/procedure.html
Care Team Members	CareTeam	http://hl7.org/fhir/2016Sep/careteam.html
Immunizations	Immunization	http://hl7.org/fhir/2016Sep/immunization.html
Unique Device Identifiers	Device.udiCarrier	http://hl7.org/fhir/2016Sep/device-definitions.html#Device.udiCarrier
Assessment and Plan	CarePlan	http://hl7.org/fhir/2016Sep/careplan.html
Goals	Goal	http://hl7.org/fhir/2016Sep/goal.html
Health Concerns	Condition	http://hl7.org/fhir/2016Sep/condition.html

Note: Authentication certificates or passwords can be reset by the data holder.

b. Patient Selection

To search for patients, the application should request a bundle of Patient resources matching suitable search criteria. To facilitate this, the following optional search parameters can be applied to the Patient resource:

RESOURCE DATA ELEMENT	SEARCH PARAMETER
Patient.name.family	family
Patient.birthDate	birthdate

For example, to retrieve a bundle of Patient resources to which the user is authorized, where the patient's last name is Smith and the patient was born on July 4, 1976, the request could be formatted as:
https://[baseURL]/Patient?family=Smith&birthdate=1976-07-04
The API will return a bundle of all patients (possibly zero) matching the search criteria. Only patients for which the user has been authorized access will be included in the results. Each patient returned in the search results is assigned a unique patient ID that can be found in the Patient.id element of the corresponding Patient resource. This patient ID can be included in subsequent requests to retrieve additional resources for that specific patient.

c. Query for a Specific Data Category

The Patient resource can be retrieved by specifying a specific patient ID or by performing a search as discussed in section 5(b). The remaining resource types listed in Section 5(a) can be accessed for a specific patient as a Bundle of resources by performing a search by resource type or by patient compartment and specifying the patient ID in the request. For example, to retrieve a bundle of Immunization resources containing all available immunization history for Patient 1234, the request could be formatted as:
https://[baseURL]/Immunization?patient=1234
or (equivalently)
https://[baseURL]/Patient/1234/Immunization
The following search terms can be used to isolate results for a single CCDS category in cases where two or more CCDS categories are represented by a single Resource type:

CCDS ELEMENT	SEARCH TERM
Health Concern	category=http://argonaut.hl7.org/extension-codes|health-concern

Problem	category=http://argonaut.hl7.org/extension-codes|problem
Smoking Status	code=http://loinc.org|72166-2
Vital Signs	category=http://hl7.org/fhir/observation-category|vital-signs
Laboratory Tests & Laboratory Values/Results	category=http://hl7.org/fhir/observation-category|laboratory

For example, to retrieve the Smoking Status for Patient 1234, the request could be formatted as:
https://[baseURL]/Patient/1234/Observation?code=http://loinc.org|72166-2
Each search request will return a bundle of zero or more results meeting the search criteria.

d. Query for All Data as a CCDA document

CCDA documents can be accessed within DocumentReference resources. CCDAs are categorized as "Summary of Episode" Notes with LOINC code 34133-9. For example, to request a CCDA document covering all dates for patient 1234, the query could be formatted as:
https://[baseURL]/DocumentReference?patient=1234&type=http://loinc.org|34133-9
The Base64 encoded CCDA XML data can be found in the DocumentReference.content.attchment.data element of the returned DocumentReference resource

e. Query for a Specific Date or Date Range

The CCDS data categories or CCDA documents returned by the API may be limited by date by specifying either (1) a specific date or (2) start and/or end dates. These dates can be included as FHIR STU3 search parameters as defined at http://hl7.org/fhir/2016Sep/http.html#search. Specifying a date or date range in the request is optional. The following table lists the supported search parameters for this purpose:

RESOURCE DATA ELEMENT	SEARCH PARAMETER
AllergyIntolerance.reaction.onset	onset
CarePlan.period	date

CareTeam.period	date
Condition.onset	onset
Goal.target	targetdate
Immunization.date	date
MedicationStatement.effective	effective
Observation.effective	date
Procedure.performed	date
DocuementReference.period	period

f. Error Handling

If the access token used in the request is invalid, expired, or the user has not been authorized to access the requested Resource, the API will return a 401 Unauthorized HTTP response.

If the request cannot be processed for other reasons (temporarily unavailable, unsupported resource type, system error, etc.), the API will return a 400 Bad Request HTTP response containing an OperationOutcome Resource with additional information regarding the issue contained in the OperationOutcome.issue element.

Handling of OAuth-related errors is detailed in RFC 6749.

Handling of dynamic client registration errors is detailed in RFC 7591.

4. Frequently Asked Questions

a. How do I access production API resources with my client application?

Please obtain [base] URL resource information from a specific healthcare provider organization when you are ready to begin allowing client end users to access PHI with production credentials. Each clinical data source accessible through the API will have a unique Base URL.

b. How extensible is the Interoperability Engine API?

API resources are modeled after the HL7 FHIR Standard for Trial Use 3 (STU 3) Ballot which is in ballot stage as of this writing. This internationally-recognized API standard has been extended to include the additional data categories needed for use in systems certifying to the 2015 Edition Certification Criteria's Common Clinical Data Set requirements. The API is designed to optimally interface with client applications while being comprehensive as a 2015 Edition solution for implementers wishing to rely on EMR Direct Interoperability Engine for Application Access services. This guide will help you access the data categories enabled by 2015 Edition Application Access APIs.

c. How do end users and applications authenticate to the API?

The API is designed to support existing patient portal credentials via the OAuth 2.0 authorization framework as per RFC 6749. The OAuth server also supports dynamic client registration as per RFC 7591.

d. What data is available through the API?

The API will return all properly formatted data provided by a connected data source system in response to a submitted query. Healthcare organizations may have their own policies and/or safety best practices that will dictate what data can be sent and when data is considered complete and/or ready to be sent. Please contact a healthcare organization directly for questions related to their specific policies.

5. Terms of Use

This is a legal agreement ("Agreement") between you (as a Developer and/or User) and California Mediterranean, LLC dba EMR Direct ("EMR Direct" or "Company"). BY ACCESSING THE SYSTEM, YOU ARE INDICATING YOUR ASSENT TO ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT AND CONSENTING TO BE BOUND BY IT. IF YOU ARE ACCESSING THE SYSTEM ON BEHALF OF A BUSINESS, THAT BUSINESS IS ALSO BOUND BY THIS AGREEMENT.

1. Definitions.

"Codes" means access codes, identification codes, tokens, private security keys, passwords and/or public security certificates that Company may issue to you for use with the System.

"Computer" means any computing device containing one or more central processing units, including but not limited to desktop and laptop personal computers, tablet devices and smartphones.

"Data Holder" means any third party that provides data that can be accessed through the System.

"Developer" means a person or business that produces or provides software or services through which a User can access the System.

"Documentation" means any printed documentation regarding the System, any electronic documentation regarding the System, and any other online or other documentation that is generally made available by Company to Users or Developers.

"Excessive Use" means access or use of the System by a Developer or User that exceeds two times the 99th percentile of system use observed by Company for all Developers and/or Users, or is otherwise identified as an outlier by Company, as measured by a suitable metric determined by Company, examples including but not limited to bandwidth utilized or number or size of data requests processed.

"Software" means the Open Application Programming Interface (API) of the EMR Direct Interoperability Engine software, any applicable related website or network resources intended for use with that software, and any other software provided by Company to you in connection with this Agreement, as applicable, in the form intended by Company for use by you, as documented by the Company, and any updates or upgrades thereto provided by Company in Company's sole discretion.

"System" means any Company websites or network resources, Software and Documentation, Codes, Public Key Infrastructure (PKI), and any services, programs, functions and information provided by Company to you.

"HIPAA" means the Health Insurance Portability and Accountability Act of 1996 and the regulations promulgated thereunder.

"HITECH" means the Health Information Technology for Economic and Clinical Health Act under Title XIII of the American Recovery and Reinvestment Act of 2009 and the regulations promulgated thereunder.

"PHI" means Protected Health Information as defined by HIPAA.

"User" means a person or other entity who accesses the System directly or through any software or service.

2. License Grant. Company hereby grants you a non-transferable, non-exclusive, revocable, limited license to use the System subject to the terms and conditions of this Agreement. RIGHTS NOT EXPRESSLY GRANTED HEREIN ARE RESERVED BY COMPANY.

3. License Restrictions. YOU MAY NOT, EITHER ON YOUR OWN BEHALF OR THROUGH ANY AGENT OR THIRD PARTY DECOMPILE, DISASSEMBLE, REVERSE ENGINEER, OR OTHERWISE ATTEMPT TO DERIVE SOURCE CODE FROM THE SOFTWARE COMPONENTS OF THE SYSTEM, OR MODIFY OR CREATE DERIVATIVE WORKS BASED ON THE SOFTWARE COMPONENTS OF THE SYSTEM OR ANY DOCUMENTATION. For example, but without limitation, you shall not yourself or through any agent, or third party: (i) translate any Software code, including without limitation for the purpose of reverse engineering or to discover the structure, sequence or organization of the Software or any portion thereof, (ii) monitor, interfere with, or reverse engineer the technical aspects of the System, (iii) intentionally compromise the security of the System or take any action intentionally, or neglect or omit to take, any action that compromises the security of the System, (iv) sell, lease, license or sublicense the System or Documentation except as expressly authorized under this Agreement. You are solely responsible for obtaining all equipment, developing or obtaining software to access the System, for ensuring the compatibility thereof with the System in accordance with the Documentation, for determining the suitability of said equipment and software for the purpose of using the System, and for paying all fees including, without limitation, all taxes and Internet access fees, necessary to use the System. Your responsibilities under the immediately preceding sentence include determining the suitability of any computers or devices, including mobile devices, browser software or other third party software, network configuration and internet service, or other hardware or software used by you, including but not limited to any software provided by Company, to access the System, including but not limited to the assessment of a device's or software's ability to maintain the security and privacy of your Codes and of any data, including PHI, viewed, downloaded, or otherwise accessed through the System. You shall not use Software or System for any purpose other than those permitted by this agreement. You will not use the System for any purpose that is unlawful or prohibited by this Agreement.

4. Participant Evaluations and User Submissions; HIPAA and HITECH; User Responsibilities.

A. As requested by Company, you agree to furnish Company with information describing the results of your use of the System, including (a) Developer's name and contact information and the names of any Users and other participants, and (b) reasonably comprehensive information concerning any errors, problems, difficulties, or suggestions regarding the access to or use of the System. You will also promptly respond to any reasonable questions provided by Company regarding the System. You acknowledge and agree that all information provided in accordance with this section shall be considered User Submissions and subject to the provisions for same set forth in Section 4.D. below.

B. YOU ATTEST THAT YOU ARE AUTHORIZED TO ACCESS ANY PHI THAT YOU REQUEST THROUGH THE SYSTEM, AND YOU AGREE TO HANDLE AND PROCESS SUCH INFORMATION ACCORDING TO ANY AND ALL APPLICABLE LAWS. You acknowledge and agree that you shall use the System only as and to the extent permitted by applicable law, including any applicable import or export laws, and only for applications related to the secure access to health information over the Internet, in a manner compliant with the security and privacy rules of HIPAA, HITECH, and any other

applicable law or regulation. You acknowledge and agree that Company is not a Covered Entity. You agree that you will not intentionally submit to Company or otherwise share with Company any Protected Health Information and will not provide Company with access to any Protected Health Information except as required for you to use the System. You acknowledge and agree that Company only acts as a conduit to transfer Protected Health Information or any other data between you and a Data Holder. You and Company agree that you and Company do not intend to become each other's Business Associate by virtue of entering into this Agreement or your use of the System. As a result, this Agreement is not intended to serve as a Business Associate Agreement between you and Company.

C. You acknowledge that the System is a data transport tool and is not intended to serve as a medical record, and that it is your sole responsibility to ensure that the content of any data accessed through the System is incorporated into a patient's medical record, when applicable. You agree that it is your sole responsibility to provide or obtain any and all necessary consents and to fulfill any and all obligations that are required by HIPAA, HITECH, or other governmental statute or regulation, including but not limited to entering into any required Business Associate Agreement, prior to use, disclosure, or transmission of any Protected Health Information or other data accessed through the System. You agree that Company has no obligation to archive or otherwise store any PHI or other data transferred through the System. You acknowledge that the data you request may not be accessible through the System when (i) you are denied access by Data Holder to any or all of the data requested or the Data Holder does not respond to your request for any reason, (ii) your request or the data provided by a Data Holder is not in a format recognized by the System, (iii) your request would cause transfer size or frequency to exceed the allowable maximum permitted by Company, (iv) the Codes you use to access the System are invalid, (v) this Agreement terminates, or (vi) for any other reason. You are solely responsible for obtaining any Codes or other credentials needed to use the System or access PHI or other data through the System. You acknowledge that Company does not control the content of data accessed through the System, that data accessed through the System may contain software viruses or other malicious content, that it is your sole responsibility to protect your computer system from viruses, and that Company has no responsibility to protect your computer system from viruses or other malware. You agree that Company, in its sole discretion, reserves the right not to enable Software or System for any particular Developer or User, should Company determine, in its sole discretion, that use by the Developer or User is a threat to Company's systems or negatively impacts the use of the System by other Users.

D. You may make submissions of certain data and information to Company (the "User Submissions"), such as feedback related to the System. You understand that User Submissions are not and shall not be deemed to be your confidential and/or proprietary information, regardless of whether any submission is marked "Confidential" and/or "Proprietary". All User Submissions of any type, and the responses of Company or any other entity, if any, and all intellectual property rights therein, including any derivatives, modifications, updates and improvements thereto, shall be owned solely by Company, and you hereby irrevocably assign to Company all such rights in the User Submissions. You hereby warrant that the User Submissions are and will be in compliance with all applicable laws and regulations, and will not contain Protected Health Information. Company has a right to use User Submissions, to which it is given access in any form, to evaluate, test or improve the System or for other lawful

purpose. You will make User Submissions and will provide Company access to Software-generated data only in accordance with HIPAA/HITECH, applicable state privacy laws and other applicable laws.

E. If the Company (i) determines that a statute or regulation, including any interpretation thereof (e.g., an advisory opinion) (collectively referred to in this subsection as a "Law") to become effective as of a certain date which, if or when implemented, would have the effect of subjecting the Company to civil or criminal prosecution under state and/or federal laws, or any other material adverse proceeding on the basis of such party's participation herein, or (ii) receives notice of an actual or threatened decision, finding or action by any governmental or private agency or party or court (collectively referred to in this subsection as an "Action"), which, if or when implemented, would have the effect of subjecting Company to civil or criminal prosecution under state and/or federal laws, or any other material adverse proceeding on the basis of such party's participation herein, then Company shall amend this Agreement to the minimum extent necessary, as determined reasonably by the Company, in order to comply with such Law or to avoid the Action, as applicable and Company shall have the power to amend this Agreement for this purpose without your consent or the consent of any other person or entity. If the Company determines that compliance with such requirements is impossible, then this Agreement may be terminated by the Company without penalty and without prior written notice.

5. Codes.

A. Company may limit the number of Users who can use the System at any given time. You warrant to Company that (a) all information supplied by you is true, correct and complete, (b) no unauthorized entity has ever had access to your Codes, and (c) you have not included trademarks in your token request unless you also possess the rights to use the respective names, nor have you otherwise misrepresented the identity of your legal organization or software. You are solely responsible for use and proper protection of your Codes, and agree to take all reasonable precautions to protect the security and integrity of the Codes and to prevent their unauthorized use. You acknowledge and agree that you are solely responsible for all actions taken that utilize your Codes, unless such actions are taken by Company, its subcontractors or agents without your approval.

B. If Company determines in its sole discretion that you are or may be using a Code issued by Company for purposes other than those allowed by this agreement, Company may, in its sole discretion, revoke the Code. Company may modify a Code or its metadata issued to you if Company determines, in its sole discretion, that such modification is required to meet the initial or ongoing inclusion or interoperability requirements of a trust community or equivalent in which Company participates or intends to participate, or that Company or Developer do not meet or have ceased to meet the inclusion requirements for a trust community or equivalent. You will cease use of all Codes following expiration or revocation of the corresponding Code or of the license granted hereunder. You will promptly notify Company if any information in your Code or its associated metadata is inaccurate or has changed. You will protect all Codes to which you have access from unauthorized access. Without limiting the last sentence of Section 7, this Section 5 will survive any termination of this Agreement.

6. Proprietary Rights and Audits. The Software, System, Documentation and all content and all information with regard thereto or contained therein including, but not limited to, data, evaluation and test results, any reports, questionnaires or other documentation provided to Company under this Agreement (the "Company Information") and any User Submissions, including any compilations of any participant information that are created in connection with or as part of the System are proprietary products of Company and its licensors and are protected under various intellectual property laws. Except for the rights expressly granted pursuant to Section 2 above, Company and its licensors retain all right, title, and interest in and to the System and Documentation, all other Company Information and the User Submissions, including all intellectual property rights therein. Company may modify the Software and Documentation at any time and from time to time and the definitions of Software or Documentation shall be deemed to also include such modifications and such Software and Documentation as modified.

7. Term and Termination. The term of this Agreement shall begin on the date of your acceptance of this Agreement, first use of the System, or upon issuance of Codes to you, whichever occurs earliest. This license will automatically terminate without notice to you upon expiration of Codes issued to you or upon the termination of this Agreement as provided herein, whichever occurs earlier. Upon any termination, all rights and licenses granted to you under this Agreement shall immediately terminate and, if you have been issued any Code(s) from Company, you shall destroy and discard (or cause to be destroyed or discarded) and cease use of all copies of such Code(s). The terms of this Agreement that give the parties rights beyond termination of this Agreement will survive any termination of this Agreement.

8. Disclaimers.

A. YOU ACKNOWLEDGE AND AGREE THAT THE SOFTWARE, DOCUMENTATION, SYSTEM AND ANY OTHER MATERIALS OR CONTENT ARE PROVIDED TO YOU "AS-IS," WITH NO WARRANTY WHATSOEVER, EITHER EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, ANY WARRANTY OF NON-INFRINGEMENT, OR ANY WARRANTY THAT THE OPERATION OF THE SYSTEM WILL BE UNINTERRUPTED OR ERROR FREE. COMPANY DISCLAIMS ANY LIABILITY FOR UNAUTHORIZED THIRD PARTY ACCESS, OR RELIANCE ON THE SYSTEM BY YOU OR ANY THIRD PARTY. COMPANY DISCLAIMS ANY LIABILITY FOR ANY DAMAGES TO YOUR COMPUTER OR ANY THIRD PARTY'S COMPUTER OR OTHER PROPERTY CAUSED BY OR ARISING FROM YOUR USE OF THE SYSTEM, WHETHER DUE TO INFECTION BY A SOFTWARE VIRUS OR OTHER MALWARE OR OTHER CAUSE. COMPANY DISCLAIMS ANY LIABILITY RESULTING FROM ANY UNAUTHORIZED ACCESS TO DATA ARISING FROM OR RELATED TO YOUR USE OF THE SYSTEM, INCLUDING BUT NOT LIMITED TO LIABILITY FOR COSTS, DAMAGES, ATTORNEYS' FEES, OR ANY LIABILITY ARISING FROM OR RELATING TO ANY REGULATORY ACTION BY ANY STATE OR FEDERAL AGENCY. You agree that you and the Company are independent contractors and that neither has any fiduciary responsibility to the other. In furtherance of the immediately preceding sentence, each of you and the Company agree to never assert for its own benefit that the other has any fiduciary duties and to the extent permitted by applicable law, you and Company hereby disclaim any fiduciary relationship between Company on one hand and you on the other hand. You further acknowledge that some content, including but not limited to any health data or directory information, has been supplied by third parties and that Company makes no warranty whatsoever with respect to such content. Company has not

attempted to nor has it verified the accuracy or completeness of such content, nor does Company have any obligation to update or correct any such content. You acknowledge that use of the System may require that data is supplied by or passes through systems that are not controlled by Company, including, without limitation, internet service providers, third party applications, routers, domain name system (DNS) servers, and systems run by Developers, Data Holders, or other third parties, and you agree that Company is not responsible for the timeliness, reliability or availability of those systems.

B. You acknowledge that the System is designed to facilitate secure delivery of health content over the Internet. You acknowledge and agree that each user's needs and data are unique, and that your inputs and information and your use to generate customized reports and outputs or other data based on your own needs and data, may cause your experience to differ from that of other users and that you assume the entire risk of your reliance on the System and any reports, information or any other content generated thereby. You acknowledge and agree that you will never use the System in urgent, critical, emergency, life-threatening, time sensitive or mission critical scenarios, and instead shall communicate in such circumstances directly and orally. You shall never use the system as a substitute for direct oral person-to-person communication in urgent, critical, emergency, life-threatening, time-sensitive, or mission-critical situations, including for communication of critical medical results in such circumstances.

9. Limitation of Liability. IN NO EVENT AND UNDER NO CIRCUMSTANCES SHALL COMPANY OR ITS AFFILIATES, EMPLOYEES, OFFICERS OR LICENSORS BE LIABLE UNDER THIS AGREEMENT, WHETHER WITH RESPECT TO THE SYSTEM OR DOCUMENTATION PROVIDED HEREUNDER OR OTHERWISE, (I) FOR ANY INDIRECT, SPECIAL, INCIDENTAL, CONSEQUENTIAL, EXEMPLARY, RELIANCE OR PUNITIVE DAMAGES OR LOSS OF PROFITS, LOSS OF BUSINESS, LOSS OF REVENUE, LOSS OF DATA, LOSS OF GOODWILL, LOSS OF BUSINESS OPPORTUNITIES, OR BUSINESS INTERRUPTION, HOWEVER CAUSED AND UNDER ANY THEORY OF LIABILITY, INCLUDING BUT NOT LIMITED TO CONTRACT, TORT (INCLUDING PRODUCTS LIABILITY, STRICT LIABILITY AND NEGLIGENCE), STATUTORY OR OTHERWISE, WHETHER OR NOT COMPANY WAS OR SHOULD HAVE BEEN AWARE OR ADVISED OF THE POSSIBILITY OF SUCH DAMAGE, (II) FOR ANY LIABILITY ARISING FROM INFORMATION INCLUDED IN OR EXCLUDED FROM DATA ACCESSED BY YOU THROUGH THE SYSTEM, UNLESS THE FAULT IN THE INFORMATION IS DUE TO FRAUD OR WILLFUL MISCONDUCT OF THE COMPANY, (III) ARISING FROM THE USAGE OF A CODE THAT IS NOT VALID OR HAS NOT BEEN USED IN CONFORMANCE WITH THIS AGREEMENT, (IV) ARISING FROM COMPROMISE OF YOUR CODES, OR (V) FOR ANY MATTER OUTSIDE THE COMPANY'S CONTROL INCLUDING, WITHOUT LIMITATION, IF COMPANY CANNOT REVOKE A CODE OR TERMINATE ACCESS TO DATA FOR ANY REASON OUTSIDE OF COMPANY'S CONTROL. IN NO EVENT SHALL COMPANY'S OR ITS LICENSORS' AGGREGATE LIABILITY ARISING OUT OF THIS AGREEMENT EXCEED THE NET AMOUNT COMPANY HAS ACTUALLY RECEIVED FROM YOU TO ACCESS THE SYSTEM AS A DEVELOPER OR USER IN THE TWELVE MONTHS PRECEDING THE FIRST CLAIM MADE BY YOU AGAINST THE COMPANY. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. THE FOREGOING LIMITATIONS SHALL APPLY NOTWITHSTANDING THE FAILURE OF ESSENTIAL

PURPOSE OF ANY LIMITED REMEDY STATED IN THIS AGREEMENT. You agree that you are solely responsible for any loss or damage resulting from your failing to meet the requirements of this agreement for the protection of your Codes.

10. Indemnification. You agree to indemnify, defend, and hold Company, its subsidiaries, officers, employees, agents, contractors, and licensors harmless from and against all claims, damages, and expenses ("Claims") arising out of or related to your use of the System, other than those Claims arising out of or related to the Company's gross negligence, willful misconduct or fraud in providing the System.

11. Privacy. Company privacy policy can be found at http://www.interopengine.com/privacy.html.

12. Miscellaneous. No waiver or modification of the Agreement shall be valid unless made in writing signed by each party, except Company may modify the terms of this Agreement without written notice by posting the modified Agreement on this website. Your continued use of the System after such modification shall constitute acceptance of the modified Agreement. The waiver of a breach of any term hereof shall in no way be construed as a waiver of any other term or breach hereof. This Agreement is governed by the laws of the State of California without reference to conflict of laws principles. All disputes arising out of this Agreement shall be subject to the exclusive jurisdiction of the state and federal courts located in San Diego, California, and the parties agree and submit to the personal and exclusive jurisdiction and venue of these courts. Notwithstanding the foregoing, Company shall have the right to pursue protection of its intellectual property rights in any court of competent jurisdiction. You may not assign this Agreement or any rights or obligations hereunder without the prior written consent of Company. You must give any required notice to the Company via certified mail. Company may give notices to you through this website or in the sole discretion of the Company through any other method reasonably calculated and intended to provide actual notice to you, provided that any notice from Company received by you or your representative or agent shall be effective, and you shall be deemed to have received any notice that Company attempts to give using means reasonably calculated and intended to provide actual notice to you. Subject to the foregoing, this Agreement will inure to the benefit of and be binding upon the parties and their respective successors and permitted assigns. Any attempted assignment in violation of this section shall be null and void. If any provision of this Agreement shall be held by a court of competent jurisdiction to be contrary to law, the remaining provisions of this Agreement shall remain in full force and effect. Nonperformance of Company shall be excused to the extent that performance is rendered impossible by strike, fire, flood, earthquake or other natural disaster, failure of any electrical, communication, or other system over which Company has no control, acts of war or terrorism, acts of God, governmental acts or restrictions or for any other reason when failure to perform is beyond the reasonable control of Company whether or not the Company could have taken precautions to provide for backup or an alternate data center in another geographic location or otherwise. This Agreement constitutes the entire understanding and agreement with respect to its subject matter, and supersedes any and all prior or contemporaneous representations, understandings and agreements whether oral or written between the parties relating to the subject matter of this Agreement, all of which are merged in this Agreement, except that (if applicable) any prior confidentiality agreement executed and signed by both you and Company shall be effective through the Effective Date and any confidential information of Company thereunder will continue to be protected as Proprietary Information hereunder.