MedConnect

API DOCUMENTATION FOR CLIENT APPLICATION DEVELOPERS

Updated June 19, 2017

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. A developer wishing to develop an application to consume this API should contact the organization holding the data he/she wishes to access to be granted an account.

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

2. General Concepts

Application Access Requests
The API is a read-only RESTful based on standards developed by HL7 in FHIR® STU 3 Ballot Specification. Details on the FHIR specification can be retrieved from http://hl7.org/fhir/.

All requests to the API will be in a format following the pattern of [base]/[endpoint] with [base] representing a URL that will be provided to the developer by the organization who issues the access account and [endpoint] representing a combination of actions and variables supplied within this document. As a read-only API, each request will be a GET HTTP request. Requests other than GET (ie. POST, PUT, …) are no supported.
All data will be returned in JSON format.

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.

2. API Access Authentication

Authentication – Obtaining an Access Token

Client authentication will be achieved using a username, passcode, and strong password combination. 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.

The first step a client must complete before making any patient-related API requests is obtaining an Access Token by utilizing the credentials obtained from the healthcare organization. The client software must support the OAuth 2.0 authorization code grant flow as detailed in RFC 6749. The request to receive an Access Token will follow the Basic Authentication model with an additional PassCode parameter, included in the credentials supplied to the client.

Token Generation / Credential Authentication – [base]/acct/login/

Authenticate passed in credentials and returns an Access Token for API request.

Change Password / Credential Authentication – [base]/acct/cpwd/

Authenticate passed in credentials, changes account password, and returns an Access Token for API request.

Each of the above actions require a Basic Authentication header with the client's supplied username and password. The passcode parameter is also used for additional client validation. The passcode will be base64 encoded string and sent in a custom HTTP header named MC_API_OrgCode. For the change password action, the new password will also be sent as a base64 encoded string in a custom HTTP header named MC_API_NewPwd.

A valid Access Toke will be issued to the client on successful completion of either of the above actions. This Access Token will be required for any subsequent API action.

The Access Token will be included as a base64 encoded string in a custom HTTP header named MC_API_Token. This is required for ALL patient-related API requests. Failure to provide this token in the appropriate header will result in no access.

3. API Details

Patient Search – [base]/pat/srchpat/

After obtaining an Access Token, a client will need to specify the patient for data requests. This can be accomplished in two ways. Each of these will use the same action [endpoint] with the same format for the request:

> [base]/pat/srchpat?mrn=MRN&lname=LNAME&fname=FNAME&dob=DOB.
> (Note: The values in all CAPS are the parameters that refines the searching of patients. These are REQUIRED parameters but can be blank)

Method 1: View all patients
A client will be granted access to a specific set of patients at the healthcare organization's discretion. The client can use the API to view a list of all patients he/she has access to. To retrieve the full list of patients the client has access to, the API request is performed with blank parameters.

> Ex. https://[base]/pat/srchpat?mrn= &lname= &fname= &dob=
> (Searches all patients within the access list)

Method 2: Patient Search based on parameters
A client can narrow the patient results from within the specific list of patients a client has access to. To do so, include a search parameter in the patient search API request. Each parameter is required to be sent for each request – any parameters not needed must be sent with no value.

> Ex. https://[base]/pat/srchpat?mrn= &lname= TEST&fname= &dob=
> (Searches for a patient within the access list with a last name of TEST)

PARAMETER	PATIENT VALUE
MRN	Medical Record Number (exact match required)
LNAME	Last Name (partial matched permitted)
FNAME	First Name (partial matched permitted)
DOB	Date of Birth (exact match required)

(Note: The patient search is limited to the list of patients the healthcare organization has granted access to, regardless of the search method used or the parameters passed in.
All date parameters will be expected in yyyyMMdd format.)

Either method of patient search will return a general collection patient information, including a Patient Token. The Patient Token uniquely identifies that patient and is only valid for the current client account. All patient-specific API requests are expected to include this Patient Token as a base64 encode string in a custom HTTP header named MC_API_PatID. Patient-specific API request also require the Access Token as indicated above.

Data Access – General Information

All data types returned from API requests are based on classes provided with thein the FHIR standard. Clients must be able to make HTTP RESTful requests of a secure channel (https://). The following is a list of the Common Clinical Data Set (CCDS) elements and the corresponding FHIR element the data is mapped to. All data is returned in JSON format.

COMMON CLINICAL DATA SET ELEMENT	FHIRRESOURCE
Patient Name	Patient (modified)
Sex	Patient (modified)
Date of Birth	Patient (modified)
Race	Patient (modified)
Ethnicity	Patient (modified)
Preferred Language	Patient (modified)
Care Team Members	Patient (modified)
Smoking Status	CodeableConcept (modified)
Problems	CodeableConcept (modified)
Medications	CodeableConcept (modified)
Medication Allergies	CodeableConcept (modified)
Laboratory Tests	CodeableConcept (modified)
Laboratory Values Results	CodeableConcept (modified)
Vital Signs	CodeableConcept (modified)

Procedures	CodeableConcept (modified)
Immunizations	CodeableConcept (modified)
Unique Device Identifiers	CodeableConcept (modified)
Assessment and Plan	CodeableConcept (modified)
Goals	CodeableConcept (modified)
Health Concerns	CodeableConcept (modified)

Note: The FHIR classes have been used to provide general structure. Details will be provided later in this documentation to outline the exact nature of the returned data.

Data Access – General Information

All requests for patient information allows for the data to be returned either completed or filtered by date (single date or a date range). Each of the API requests that request patient information follow a similar pattern:

```
[base]/pat/[action]?sd=STARTDATE&ed=ENDDATE
```

This format supports the three ways of returning data (complete, by single date, by date range). This is accomplished based on the values that are sent for STARTDATE and ENDDATE. For a complete listing, send no value (empty string) for both STARTDATE and ENDDATE. For a single date, send the same date in both parameters. For a date range, send a different date for both values.

(Note: All date parameters will be expected in yyyyMMdd format.)

Every action for patient-related API requests will follow the above pattern. All parameters are required to be passed in. Failure to do so will result in no information returned.

Patient Demographics – [base]/pat/getPat/

Returns patient demographic information in a modified FHIR Patient class. Race, ethnicity, and care team member properties have been added to the FHIR Patient class.

Race is returned as a list of FHIR Coding elements in the following format:

```
"race": [
 {
   "code": "1006-6",
   "display": "Abenaki"
 },
  {
    "code": "1008-2",
    "display": "Algonquian"
  }
]
```

Ethnicity is returned as a list of FHIR Coding elements in the following format:

```
"ethnicity": [
  {
    "code": "2140-2",
    "display": "Castillian"
  },
  {
    "code": "2151-9",
    "display": "Chicano"
  }
]
```

Care Team Members are returned as a list of modified FHIR Coding elements in the following format:

```
"careTeam": [
  {
    "teamMember": "Smith, David MD",
    "memberType": "PRIMARY"
  }
]
```

(Note: Demographics API request does NOT accept the STARTDATE or ENDDATE parameters.)

Patient Vitals – [base]/pat/getVitals/

Returns patient vitals in a list of modified FHIR CodeableConcept class with custom FHIR Coding classes.

```
"vitalSigns": [
  {
    "resourceType": "CodeableConcept",
    "use": "Vital Signs",
    "period": "20170614",
    "coding": [
      {
        "system": "LOINC",
        "code": "8302-2",
        "display": "height",
        "value": "69",
        "unit": "in"
      },
      {
        "system": "LOINC",
          "code": "29463-7",
          "display": "weight",
          "value": "985",
          "unit": "lb"
        }
     ] }
]
```

Patient Smoking Status – [base]/pat/getSS/

Returns patient smoking status in a list of modified FHIR CodeableConcept class with custom FHIR Coding classes.

```
  "smokingStatus": [
    {
      "resourceType": "CodeableConcept",
      "use": "Smoking Status",
      "period": "20170615",
      "coding": [
        {
          "system": "SNOMED-CT",
          "code": "230059006",
          "display": "Current Some Day Smoker",
          "since": "2014",
          "details": "12 packs per day"
        }
      ]
    }
]
```

Patient Problems – [base]/pat/getProblems/

Returns patient problems in a list of modified FHIR CodeableConcept class with custom FHIR Coding classes.

```
"problems": [
    {
      "resourceType": "CodeableConcept",
      "use": "Problem",
      "period": "20170614",
      "coding": [
        {
          "system": "SNOMED-CT",
          "code": "404684003",
          "display": "OTHER SPECIFIED HEALTH STATUS",
     "status": "Active"
    }
   ]
  }
]
```

Patient Medications – [base]/pat/getMeds/

Returns patient medications in a list of modified FHIR CodeableConcept class with custom FHIR Coding classes.

```
 "medications": [
  {
   "resourceType": "CodeableConcept",
   "use": "Medication",
   "period": "20170613",
   "coding": [
    {
     "system": "RXNORM",
     "code": "541365",
     "display": "Adderall 30 mg tablet",
     "ndc": "00555076802",
     "usage": "TAKE 1 TABLET (30 MG) BY ORAL ROUTE ONCE DAILY BEFORE BREAKFAST",
     "qty": "12"
    }
   ]
  }
]
```

Patient Allergies – [base]/pat/getAllergies/

Returns patient allergies in a list of modified FHIR CodeableConcept class with custom FHIR Coding classes.

```
 "allergies": [
  {
   "resourceType": "CodeableConcept",
   "use": "Drug Allergy",
   "period": "20170614",
   "coding": [
    {
     "status": "Active",
     "substance": "penicillamine",
     "substanceCode": "7975",
     "substanceCodeSystem": "RXNORM",
     "reaction": "(California viral encephalitis) or (Tahyna fever)",
     "reactionCode": "186588007",
     "reactionCodeSystem": "SNOMED-CT"
    }
   ]
  }
]
```

Patient Procedures – [base]/pat/getProcs/

Returns patient procedures in a list of modified FHIR CodeableConcept class with custom FHIR Coding classes.

```
 "procedures": [
  {
   "resourceType": "CodeableConcept",
   "use": "Procedure",
   "period": "20170619",
   "coding": [
    {
     "system": "CPT-4",
     "code": "52281",
     "display": "Cystoscopy With Dilation- Office"
    }
   ]
  }
]
```

Patient Lab Results – [base]/pat/getLabResults/

Returns patient lab results in a list of modified FHIR CodeableConcept class with custom FHIR Coding classes.

```
 "labResults": [
  {
   "resourceType": "CodeableConcept",
   "use": "Lab Results",
   "period": "20170619",
   "coding": [
    {
     "system": "CPT-4",
     "code": "52000",
     "display": "Cystoscopy-Office",
     "value": "We obtained AP and lateral cervical spine films in the office today.  The fusions and instrumentation
appeared to be in good position and are solid from C4 to C7."
    }
   ]
```

```
    }
]
```

Patient Immunizations – [base]/pat/getImm/

Returns patient immunizations in a list of modified FHIR CodeableConcept class with custom FHIR Coding classes.

```
  "immunizations": [
    {
      "resourceType": "CodeableConcept",
      "use": "Immunzation",
      "period": "20170501",
      "coding": [
        {
          "display": "Active DTaP",
          "status": "Completed",
          "ndc": "12345",
          "cvx": "52",
          "manufacturer": "ABBVIE",
          "lotNumber": "1345"
        }
      ]
    }
]
```

Patient Plans – [base]/pat/getPlans/

Returns patient plans in a list of modified FHIR CodeableConcept class with custom FHIR Coding classes.

```
  "plans": [
    {
      "resourceType": "CodeableConcept",
      "use": "Plan",
      "period": "20170614",
      "coding": [
        {
          "display": "Instruction",
          "value": "!Anticipatory  guidance !"
        }
      ]
    }
]
```

Patient Implantable Devices – [base]/pat/getImpDevs/

Returns patient implantable devices in a list of modified FHIR CodeableConcept class with custom FHIR Coding classes.

```
 "implantableDevices": [
  {
    "resourceType": "CodeableConcept",
    "use": "Implantable Device",
    "coding": [
      {
        "manufacturer": "Vivorte, Inc",
        "lotNumber": "000000000000XYZ123",
        "location": "Cheek teeth (body structure)",
        "locationCode": "62708002",
        "locationCodeSystem": "SNOMED-CT",
        "deviceDescription": "Cadaveric-donor/synthetic mineral bone graft",
        "deviceId": "W4146EB0010T0475",
        "model": "10 cc",
        "serial": "000025",
        "udi": "=/W4146EB0010T0475=,000025=A99971312345600=>014032=}013032&,1000000000000XYZ123",
        "implantDate": "12/6/2016"
      }
    ]
  }
]
```

Patient CCDA – [base]/pat/getCCDA/

Returns patient CCDA as a URL Token Encoded string (.NET HttpServerUtility.UrlTokenEncode)

```
"ccdaUTEnc": “CCDA XML as URLTokenEncoded string (not shown)”
```

4. Error Handling

All requests that are sent to the proper endpoints will receive an HTTP Status of 202 – Accepted. Any error that is encounter while attempting to complete an API request will be returned with the 202 status as a JSON object will a details error message detailing the error:

```
"ErrMsg": “Detailed error message”
```

The following is a list of errors that may be encountered when executing API requests:

ERROR	MEANING
The supplied token is invalid	The Access Token passed in wasn’t located and couldn’t be validated.
The supplied token is expired.	The Access Token expired.
The supplied token is disabled.	The Access Token has been marked disabled by a system administrator.
The associated account is locked.	The account associated with the passed in Access Token has been marked locked by a system administrator.
The associated account is disabled.	The account associated with the passed in Access Token has been marked disabled by a system administrator.
The associated account is inactive.	The account associated with the passed in Access Token has been marked inactive by a system administrator.
Unable to validate credentials.	The username, user password, and passcode combination wasn’t validated.
Unable to validate credentials. Password was not changed.	The username, user password, and passcode combination wasn’t validated during a password change request.
No ABC retrieved.	Indicates the requests resource wasn’t retrieved for the patient, with ABC being the resource (ex. Vitals)
Access has not been granted for the selected patient.	The Patient Token supplied identified a patient that the client account doesn’t have access to.
Patient not specified.	Patient Token missing or invalid.
An error has occurred while processing the request.	Generic error. Verify all parameter required are passed in and in the proper format.

Any HTTP Status other than 202 – Accepted indicates an error that is outside the control of the API developer. If such an error occurs, verify [base] URL, endpoint usage, and general connectivity to the API URL.

5. 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. Ensure an account is also requested and credentials received from the healthcare organization.

b. 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. Additional, non-patient portal accounts can also be assigned at the discretion of the healthcare organization. Authentication is based on standard Basic Authentication with an additional PassCode for additional security.

c. 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.

Any additional questions can be directed to the healthcare organization that granted an API access account. Issues of a technical nature will be directed by the healthcare organization to the developers of the MedConnect API.

6. Terms of Use

This is a legal agreement ("Agreement") between "you" (a "Developer" or “User”) and MedConnect, Inc ("Company"). BY USING THE SYSTEM AND/OR ACCEPTING THIS AGREEMENT, YOU ARE CONSENTING TO BE BOUND BY ITS TERMS. WHEREAS, Company is willing to supply the System (as defined below) to you; WHEREAS, you desire to have access to the System, and are aware of the purpose of the System; NOW THEREFORE, in consideration of the foregoing and the mutual covenants hereinafter set forth, the parties hereby agree:

1. Definitions.

As used herein: "Software" means the MedConnect, Inc Application Programming Interface (API) software, access to any applicable related website or network resources intended for use with the 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 website or network resources, Software and Documentation, “Codes”, Company's Public Key Infrastructure (PKI), and any services, programs, functions and information provided by Company to you. "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. "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. "User" means an end user (a person and/or other entity) who Uses the System directly or through a third party software product or service. You are a “Developer” if you produce or provide software or services through which a User or Users can Use the System. "Use" means when you access the System. 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. "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. “Data Holder” means any third party organization that provides data that can be accessed through the System. "Excessive Use" means 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 processed.

2. License Grant.

Company grants Developer and their Users 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 SHALL NOT ITSELF 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 intentionally 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 documented here. You are solely responsible for obtaining all equipment, developing or obtaining software, and obtaining Codes used to access PHI or other data through the System, for ensuring the compatibility thereof with the System, for determining the suitability of said equipment and software for the purposes 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 a Developer or by

Company, to access PHI or other data through the System, including but not limited to the assessment of a device's or software's ability to maintain the security and privacy 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 may 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 other participants, and (b) any errors, problems, difficulties, or suggestions regarding the access to or use of the System. You agree that Company will own and has the right to use, transfer and license all suggestions and improvements, whether written or oral, furnished by you without having any obligation or liability to you. You will also promptly respond to any reasonable questions provided by Company regarding the System.

B. YOU ATTEST THAT YOU ARE AUTHORIZED TO ACCESS THE PHI YOU ARE REQUESTING THROUGH THE SYSTEM, AND YOU AGREE TO HANDLE AND PROCESS SUCH INFORMATION ACCORDING TO ANY AND ALL APPLICABLE LAWS. If you are a Developer, you agree to maintain suitable facilities, management, operational, and physical controls to protect PHI and any Codes consistent with the security and privacy controls imposed by HIPAA, HITECH, and any other federal, state, and local laws, where applicable, and to treat all Codes with no less care and protection than that afforded to Protected Health Information. 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.

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 establish policies and procedures that 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 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 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 the 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 we determine, in our 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. Each Developer or User may also 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 user, if any, and all intellectual property rights therein, including any derivatives, modifications, updates and improvements thereto, shall be owned solely by Company. 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 internal purposes related to the System. 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 persons who can use the System. You may be issued one or more identification codes or tokens. You may also be issued one or more private security keys and/or public security certificates for use with the System. All such user codes, keys, certificates, tokens, or passwords issued by Company are referred to herein as the "Codes." If you are a Developer, 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 you become aware of any unauthorized access or use of the System or any other part thereof, you shall immediately notify Company. 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 a Developer if Company determines, in its sole discretion, that such modification is required for Company 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 cease 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. If you are a Developer, 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. If you discover, or have reason to believe that your Codes have been compromised, or that information contained in your Code or its associated metadata is inaccurate or has changed, you agree to promptly notify Company to request a new Code, and to promptly notify any person or organization that may reasonably be expected to rely on your Code. Without limiting the last sentence of Section 7, this Section 5 will survive any termination of this Agreement.

6. Proprietary Rights and Audits.

The 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.

7. Term and Termination.

The term of this license shall begin on the date of your acceptance of this Agreement, first use of the System, or upon issuance of Codes to you by Company, whichever occurs earliest. This license will automatically terminate without notice to you upon expiration of Codes issued to you by Company 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 SYSTEM AND ANY 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. 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 Data Holders, 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 other users and that you assume the entire risk of their reliance on the System and any reports, information or any other content generated thereby. You acknowledge that the access to health information through System may require data to pass through other systems that are not controlled by Company, and you agree that Company is not responsible for the timeliness or reliability of delivery or receipt of data through the System. 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 HEREUNDER OR WITH RESPECT TO THE SYSTEM OR DOCUMENTATION PROVIDED HEREUNDER (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.