SERVICE AGREEMENT

CALIFORNIA DIRECT

AXESSON
100 ENTERPRISE WAY SUITE C110 SCOTTS VALLEY CA 95066
(831)600-3750
cadirect@axesson.com

Direct Service Agreement

Service Agreement

Dear

This agreement outlines the terms of service and agreements necessary to onboard

_____("Organization") onto the California Direct program. By signing below you hereby agree to all terms and conditions as set forth.

Definitions

All definitions in the Direct Service Agreement (the "Agreement") apply to all Direct services, including California Direct.

"HISP" shall mean Health Information Service Provider (Axesson) providing delivery of health related services and support including but not limited to Direct.

"Organization" shall mean any entity and/or authorized Users registered for Direct. Organizations and authorized Users may include, but are not limited to, health care providers and employees, staff, contractors, or agents of the Organization as it relates to the care of the patient.

"CADirect Service" shall mean the California Direct services provided by Axesson wherein User(s) may send/receive information and/or Patient Data to or from other Direct Users via Direct protocols. Messages may contain Protected Health Information (PHI).

"Business Associate" shall mean any person that is a business associate of a Covered Entity User under 45 CFR § 160.103.

"Minimum Necessary" shall refer to the standard set forth at 45 CFR §164.502(b) and 164.514(d) of the HIPAA Regulations.

"Provider Directory" shall mean a database accessible to the User and its Authorized Users containing Direct addresses of the other Participating Entities and their Authorized Users, attributes of each Participating Entity and Users, and the Participating Entity of which each Authorized User is associated. The Provider Directory's purpose is to locate a user/entity with whom the User or its User desires to have PHI secure Direct communication.

"Treatment" shall have the meaning set forth at 45 CFR § 164.501 of the HIPAA Regulations.

Direct Service Authorized Use

User shall use Direct Services to send and receive Patient Data only for the purposes set forth below. User shall also ensure that its Users use Direct Services to send and receive Patient Data only for the purposes set forth below.

1. Treatment. Treatment of the individual who is the subject of the Patient Data requested or received by User.
2. Payment. Obtaining payment for health care services provided to an individual who is the subject of the Patient Data requested or received by User.
3. Health Care Operations. Health Care Operations provided that (i) the requesting User has an established Treatment relationship with the individual who is the subject of the Patient Data; (ii) the purpose of the request is for those Health Care Operations listed in paragraphs (1) and (2) of the definition of Health Care Operations in 45 CFR § 164.501 or health care fraud and abuse detection with respect to use of the System or compliance with the Agreement's and this Service Level Attachment's requirements; and (iii) the Authorized User is Requesting/accessing Patient Data for its own use. User shall only use the Minimum Necessary Patient Data for such Health Care Operations purposes.

4. Public Health. Public Health activities and reporting, but only to the extent permitted by all applicable statutes, rules and regulations of the State, as well as all applicable federal statutes, rules, and regulations.
    1. Reporting on Clinical Quality Measures. Reporting on such clinical quality measures and other measures to demonstrate "meaningful use," as specified in regulations promulgated by the Department of Health and Human Services under the American Recovery and Reinvestment Act of 2009, Sections 4101 and 4102, or other payer incentive or accreditation programs but only to the extent permitted by all applicable statutes, rules and regulations of the State of California, as well as all applicable federal statutes, rules, and regulations.

Direct Mail Limits

1. Mail Retention: California Direct is not intended to be a repository of clinical information or messages. California Direct provides the means by which you can send and receive information. For this purpose, direct messages expire 90 days from when they were received/sent by the User or Users. Messages older than 90 days will be removed automatically.
2. Mailbox Size: Each account is allocated 1GB of space.
3. The maximum attachment size is 10MB.
4. Organization is hereby authorized to perform back-up of all data transmitted through Direct Service and California Direct shall not institute any procedures or protections within the system that will interfere with such back-up. Organization may perform back-up procedure as frequently as daily.

User Responsibilities

1. Compliance with the Agreement. User agrees to comply with the Agreement and to fulfill all of its responsibilities under the Agreement.
2. System Operating Policies and Technical Requirements for the Direct Service. Organization and its authorized Users shall comply with the System Operating Policies and Technical Requirements for the Direct Service. These requirements are as follows:
    a. Organization will be responsible for registration of the entity for participation and verification of any of its Users who register. Organization must provide a web browser. A separate account is required for each User with a username and password to login.
    b. Organization authorizes the system to encrypt Direct messages on behalf of Organization and Users to protect data when it is transmitted over the internet.
    c. Organization agrees to accurately complete its registration information and its authorized User's information in the Provider Directory as part of the registration process and maintain the accuracy of the information in the Provider Directory.
    d. Organization agrees to have its registration information checked for consistency with other information sources and understands that inconsistencies will terminate the registration process or this agreement unless corrected by the entity. Organization agrees to require that its authorized Users maintain the accuracy of the information contained in the Provider Directory.
    3. Security Practices for Computers (both desktop and portable): Organization and its authorized Users agree to avoid use of any computer to access Message Content unless the Organization/User has:
        a. Password lock activated to gain access to the given device
        b. Virus and other malware protection of the device, and
        c. File Encryption and encryption of data at rest.

4. Security Practices for Mobile Devices (and other portable electronic devices): Organization and its authorized User agree to avoid use of portable devices to access Message Content unless the Organization/User has:
    a. Password lock activated to gain access to the given device
    b. Virus and other malware protection of the device, and
    c. File Encryption and encryption of data at rest.
5. Prohibited Use: Organization and its authorized Users agree not to use the Message Content, information about Messages, or any Proprietary Information of the other party to compare referral or practice patterns, or make any other comparison without the other's explicit written permission.

Axesson Responsibilities

1. Provision of the Direct Service. Axesson will provide the Direct Service as a Web-mail client ("Mirth Mail") via a web browser for Authorized Users to utilize. Axesson will also provide general instructions and support on how to activate the Direct Service in Electronic Health Record systems that are enabled for Direct. Axesson is not responsible for technical support for specific EHRs unless contracted to do so.
2. Provision of Direct Address. Axesson will provide Users with an Axesson- issued CADirect email address that will allow Authorized Users to receive secure messages via the system.
3. Axesson has no role in verifying the accuracy of any messages sent over the Direct services.
4. Prohibited Use: Axesson, the HISP for California Direct, agrees not to use the Message Content, information about Messages, or any Proprietary Information of any party to compare referral or practice patterns, or make any other comparison without the other party's explicit written permission.

Fees/Payment

1. Non-Payment: Accounts shall be made inactive 15 days following non-receipt of payment.
2. Accounts are perpetual. Each account shall be charged 10 days prior to the renewal date to ensure no interruption in services occur. You must notify Axesson 30 days prior to your renewal date if you wish to not continue services.
3. Axesson reserves the right to increase fees at any time in the future for participation in Direct Service(s), provided that Axesson shall provide the Organization with sixty (60) days prior notice of its intent to increase such fees.
4. Fees do not include out-of-pocket expenses (including, travel and room and board) as incurred by Axesson in connection with Axesson's delivery to the Organization of the Services hereunder.
5. User Fee Changes: If Customer adds one or more accounts to its practice during the contract period, the Direct services shall be adjusted to permit such added Users to use the Services/Software/Products upon payment of additional services fee at the then-current rate, calculated at the then-current rate for additional Users, and pro-rated for the applicable portion of the year in which the user(s) is added. If Customer loses one or more Registered Users, there shall be no change in the fees until the renewal period.

Support

Call Center	831-600-3750	8am to 5pm PST Monday-Friday, excluding holidays
Support Portal	24/7 365	http://portal.axesson.sugarondemand.com
Email	support@axesson.com	24/7, auto generates a support ticket.

Direct Service Agreement

NOTE: Axesson is not responsible for issues related to Customer's computer or internal and external computer network.

Termination of Services

1. Direct Accounts are perpetual. In the event you wish to discontinue Direct services in advance of the annual renewal date, 30 days written notice must be provided to Axesson at cadirect@axesson.com.
2. Non Payment: Accounts shall be deactivated 15 days after annual renewal date for non-payment. Data will not be retrievable and the mail dashboard will become inaccessible.

Service Level

PROMISES Axesson DOES NOT MAKE

1. We do not promise that Services will be uninterrupted, error-free, or completely secure. You acknowledge that there are risks inherent in Internet connectivity that could result in the loss of your privacy, confidential information and property.
2. We disclaim any and all warranties not expressly stated in the Agreement including the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. You are solely responsible for the suitability of the service you have chosen. Any services that we are not contractually obligated to provided but that we may perform for you at your request and without any additional charge are provided on an AS IS basis.
3. We do not promise to retain the data backup longer than agreed data retention period.

Certificate Authorization

DigiCert, Inc. ("**DigiCert**") issues X.509 v.3 digital certificates ("**Certificates**") to customers of the health information service provider identified on the registration document ("**HISP**"). You, as either an individual or organization that will be named in a certificate, are providing this authorization to assist HISP in performing certain digital certificate-related duties that are normally reserved for Certificate subjects, usually an entity's equipment, personnel, or agents. These tasks include managing keys, registering devices, and authenticating personnel with DigiCert and its Certificate systems and installing, configuring, and managing issued Certificates. Therefore, you hereby agree and authorize HISP and DigiCert as follows:

1. Certificates. HISP may request and approve Certificates in your name and use issued Certificates for your benefit. DigiCert may issue, refuse to issue, revoke, or restrict access to Certificates in accordance with the instructions provided by HISP and rely on these instructions as if originating from you.
2. Representations. You represent that you are a HIPAA covered entity, a HIPAA business associate, or a health-care organization that treats protected health information with privacy and security protections that are equivalent to those required by HIPAA. You represent that you will limit your use of the digital certificate for purposes required as a HIPAA Business Associated or Non-HIPAA Healthcare Entity (HE), defined as an entity that has an appropriate healthcare-related need to exchange Direct messages and which agrees to handle protected health information with privacy and security protections that are equivalent to those required by HIPAA.
3. Authorization. You explicitly appoint HISP's employees and agents as your agent for the purpose of requesting, using, and managing Certificates and corresponding private keys. HISP's employees and agents are authorized to fulfill all obligations imposed by DigiCert with respect to the Certificate, communicate with DigiCert regarding the management of key sets and Certificates, and fulfill all roles related to Certificate issuance, such as a certificate requester, certificate approver, and contract signer (as used in the CA/Browser Forum's Extended Validation Guidelines for SSL Certificates). You hereby authorize HISP and its employees to:
   (i) Request Certificates for domains and emails owned or controlled by you or your affiliates,

(ii) Request Certificates naming you or your equipment, employees, agents, or contractors as the subject, and

(iii) Accept terms and conditions related to Certificates issued on your behalf.

4. Trusted Agent. In addition, you are hereby appointed as an agent of DigiCert for the purpose of collecting documentation, verifying identities, and providing identity information to DigiCert. Any information must be verified in accordance with instructions provided by DigiCert. The requirements for identity verification are set by the applicable CP and may change without notice. Therefore, DigiCert may amend the instructions at any time.
5. Documentation. For each certificate ordered by HISP under your authorization, DigiCert must obtain a personal attestation and a copy of all documentation necessary to verify the entity's identity. DigiCert may reuse this information in some cases. DigiCert may rely solely on the information you provide or previously provided when issuing a Certificate or may elect to perform additional verification prior to issuing a Certificate. You agree to provide, at all times, provide accurate, complete, and true information to DigiCert. If any information provided to DigiCert changes or becomes misleading or inaccurate, then you agree to promptly update the information. You consent to (i) DigiCert's public disclosure of information embedded in an issued Certificate, and (ii) DigiCert's transfer of your personal information to DigiCert's servers, which are located inside the United States. DigiCert shall follow the privacy policy posted on its website when receiving and using information from you or HISP. DigiCert may modify the privacy policy in its sole discretion, but only to an extent that conforms and complies with all applicable statutory and regulatory provisions.
6. Representation. You represent that you have the authority to execute this authorization and bind your organization (if applicable) by its terms. By submitting documentation to DigiCert, you represent to DigiCert that (i) you have verified any named individual's name, address, email address, telephone number, birthdate, and any other information required by DigiCert and in accordance with any instructions provided by DigiCert, (ii) you have examined any relied upon documents for modification or falsification and believe that the documents are legitimate and correct, and (iii) you are unaware of any information that is reasonably misleading or that could result in a misidentification of the verified entity. These representations survive termination of this appointment until all Certificates that rely on the documentation expire.
7. Duration. This authorization lasts until revoked by you, and you are responsible for all Certificates requested by HISP on your behalf until after DigiCert receives a clear email message revoking the authorization at legal@digicert.com. Even after revocation, all representations and obligations herein survive until all Certificates issued under this authorization expire or are revoked in accordance with DigiCert's agreement with HISP. DigiCert may require that you periodically renew this authorization by resubmitting a copy of this authorization to DigiCert.
8. Certificate Revocation and Termination. DigiCert will revoke any Certificate issued to HISP on your behalf after receiving notice from you and after verifying the legitimacy of the revocation request. DigiCert may also revoke a Certificate issued to HISP on your behalf for any reason and without notice.
9. Notices**.** You must send all notices (i) in writing, (ii) with delivery confirmation via first class mail, commercial overnight delivery service, facsimile transmission, email, or by hand, and (iii) addressed to Axesson Attn: Direct , 100 Enterprise Way C110 Scotts Valley CA 95066 cadirect@axesson.com Fax: 831 465 7893. All notices are effective on receipt. DigiCert will deliver notices to you by delivering the notice to HISP. Notices are effective when sent to HISP in accordance with DigiCert's agreement with HISP.
10. Intended Beneficiaries**.** HISP and DigiCert are express and intended beneficiaries of your obligations and representations under this agreement.

BY SIGNING THE SERVICE AGREEMENT, YOU ACKNOWLEDGE THAT YOU HAVE READ THIS AUTHORIZATION, THAT YOU UNDERSTAND IT, AND THAT YOU AGREE TO IT. IF YOU DO NOT ACCEPT THIS SERVICE AGREEMENT OR DO NOT WISH TO APPOINT HISP (Axesson) AS YOUR CERTIFICATE AGENT, DO NOT SIGN THE SERVICE AGREEMENT. IF YOU HAVE ANY QUESTIONS, PLEASE E-MAIL AXESSON AT cadirect@axesson.com or CALL 831.600.3750.

Direct Service Agreement

Customer agrees to all terms and conditions including the general terms and conditions as provided via website: www.californiadirect.org /generaltermsconditions. IN WITNESS WHEREOF, the parties have caused this Agreement to be executed by their duly authorized representatives.

Customer	**Axesson**
Signature: _____	Signature: _____
By: _____	By: _____
Title: _____	Title: _____
Date: _____	Date: _____

Direct Service Agreement

This Business Associate Agreement is entered into by and between Axesson**, a** California LLC **located at**

100 Enterprise Way #C110 Scotts Valley CA 95066 **("Business Associate") and**

_____, a _____(business type),

located at _____

("Covered Entity"), which is a covered entity under the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"). The parties are entering into this agreement to assist the Covered Entity in complying with HIPAA, and to set forth Business Associate's obligations under the Health Information Technology for Economic and Clinical Health Act of 2009 (the "HITECH Act"), and 45 CFR Parts 160 and 164, Subpart C (the "Security Rule"), Subpart D (the "Data Breach Notification Rule"), and Subpart E (the "Privacy Rule") (collectively, the "HIPAA Regulations"). Terms used in this Agreement have the meanings given them in the HIPAA Regulations. This agreement applies to any Protected Health Information Business Associate receives from Covered Entity, or creates, receives or maintains on behalf of Covered Entity, under its agreements with Covered Entity (the "Principal Agreements").]

AGREEMENT

1. Business Associate may use and disclose Covered Entity's Protected Health Information to provide Covered Entity with the goods and services contemplated by the Principal Agreements. Except as expressly provided below, this agreement does not authorize Business Associate make any use or disclosure of Protected Health Information that Covered Entity would not be permitted to make.

2. Business Associate will:

(a) Not use or further disclose Covered Entity's Protected Health Information except as permitted by the Principal Agreements or this Agreement, or as required by law;

(b) Use appropriate safeguards, and comply, where applicable, with the HIPAA Security Rule with respect to electronic protected health information, to prevent use or disclosure of Covered Entity's Protected Health Information other than as provided for by the Principal Agreements or this Agreement;

(c) Security Practices for Computers (both desktop and portable): User agrees to avoid use of any computer to access Message Content unless the User has:(i) Password lock activated to gain access to the given device; (ii) Virus and other malware protection of the device, and (iii) File Encryption and encryption of data at rest.

(d) Security Practices for Mobile Devices (and other portable electronic devices): User agrees to avoid use of portable devices to access Message Content unless the User has: (i) Password lock activated to gain access to the given device; (ii) Virus and other malware protection of the device, and (iii) File Encryption and encryption of data at rest.

(e) Report to Covered Entity within 15 days of discovery any use or disclosure of Covered Entity's Protected Health Information not provided for by the Principal Agreements or this Agreement of which it becomes aware, including breaches of unsecured protected health information as required by the Data Breach Notification Rule (45 CFR § 164.410), and any security incident of which Business Associate becomes aware.

(f) Mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of protected health information by Business Associate in violation of this Agreement or the HIPAA Regulations;

(g) Ensure that any of Business Associate's subcontractors that create, receive, maintain, or transmit protected health information on behalf of the Business Associate agree in writing to the same restrictions and conditions

that apply to Business Associate with respect to such information, including compliance with the HIPAA Security Rule with respect to electronic protected health information;

(h) Make any Protected Health Information in a designated record set available to Covered Entity to enable Covered Entity to meet its obligation to provide access to the information in accordance with 45 CFR § 164.524;

(i) Make any Protected Health Information in a designated record set available for amendment and incorporate any amendments to Protected Health Information as directed by Covered Entity pursuant to 45 CFR § 164.526;

(j) Make available to Covered Entity the information concerning disclosures that Business Associate makes of Covered Entity's Protected Health Information required to enable Covered Entity to provide an accounting of disclosures in accordance with 45 CFR § 164.528;

(k) To the extent that Business Associate carries out Covered Entity's obligations under the Privacy Rule, comply with the requirements of the Privacy Rule that apply to Covered Entity in the performance of such obligations;

(l) Make Business Associate's internal practices, books, and records relating to Business Associate's use and disclosure of Protected Health Information received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity, available to the Secretary of the United States Department of Health and Human Services for purposes of determining Covered Entity's compliance with the HIPAA Regulations, and to the Covered Entity for purposes of determining Business Associate's compliance with this Agreement;

(m) Limit its requests for and uses and disclosures of Covered Entity's Protected Health Information to the minimum necessary, and comply with any minimum necessary policies and procedures that covered entity provides to Business Associate;

(n) Upon termination of the Principal Agreements, return or destroy all Covered Entity's Protected Health Information that Business Associate still maintains in any form and retain no copies of such information or, if return or destruction is not feasible, extend the protections of this agreement to that information and limit further use and disclosure to those purposes that make the return or destruction of the information infeasible.

3. Business Associate may use Covered Entity's Protected Health Information for the management and administration of Business Associate's company and to carry out Business Associate's own legal responsibilities, and Business Associate may disclose the information for these purposes if Business Associate is required to do so by law, or if Business Associate obtains reasonable assurances from the recipient of the information (1) that it will be held confidentially, and used or further disclosed only as required by law or for the purpose for which it was disclosed to the recipient, and (2) that the recipient will notify Business Associate of any instances of which the recipient is aware in which the confidentiality of the information is breached.

4. Business Associate may use Covered Entity's Protected Health Information for data aggregation, as permitted by the Privacy Rule in accordance with 45 CFR § 164.501.

5. Business Associate may de-identity Covered Entity's Protected Health Information, and use and disclosed the de-identified information as permitted by the Privacy Rule in accordance with 45 CFR § 164.514.

6. Cover entities agree not to use the Message Content, information about Messages, or any Proprietary Information of the other party to compare referral or practice patterns, or make any other comparison without the other's explicit written permission.

7. If Covered Entity determines that Business Associate has violated a material term of this agreement, and if Business Associate fails to cure such violation within 30 days of delivery of written notice thereof, Covered Entity may immediately terminate the Principal Agreements. This Agreement shall remain in effect as long as Business Associate maintains or has access to Covered Entity's Protected Health Information, regardless of the termination of the Principal Agreements.

8. This agreement is to be interpreted in accordance with HIPAA, the HITECH Act, and the regulations promulgated thereunder, as amended from time to time.

Covered Entity:	**Business Associate:**
_____	Axesson _____
Name	**Name**
_____	_____
Signature	**Signature**
_____	William Beighe / General Manager__
Name and title	**Name and title**
_____	_____
Date	**Date**