THE INFORMATION IN THIS BOX IS NOT A PART OF THE CONTRACT AND IS FOR COUNTY USE ONLY

SAN BERNARDINO COUNTY

Contract Number 22-224

SAP Number

Arrowhead Regional Medical Center

Department Contract Representative	William L. Gilbert, Director
Telephone Number	(909) 580-6150
Contractor	California Mediterranean, LLC dba *EMR Direct*
Contractor Representative	
Telephone Number	
Contract Term	Indefinite
Original Contract Amount	Non-financial
Amendment Amount	
Total Contract Amount	
Cost Center	

Briefly describe the general nature of the contract: Non-financial Direct License Agreement with California Mediterranean, LLC dba EMR Direct, including non-standard terms, for access to direct messaging and software certifications that allow for the encrypted and secure exchange of health information in purchase amounts as authorized by County Policy for an indefinite period of time until terminated by either party.

FOR COUNTY USE ONLY

Approved as to Legal Form	Reviewed for Contract Compliance	Reviewed/Approved by Department
► Bonnie Uphold, Deputy County Counsel	►	► William L. Gilbert, Director
Date 3-9-2022	Date	Date 3/9/22

Non-Standard Contract Coversheet

Revised 3/14/19

EMR DIRECT LICENSE AGREEMENT

Updated February 5, 2018

This is a legal agreement (the "Agreement", which may also be referred to as the "License Agreement", the "phiMail Software License Agreement", or the "phiMail Developer License Agreement"), between "you" or "Subscriber" and California Mediterranean, LLC dba EMR Direct ("EMR Direct" or "Company"). BY USING THE SYSTEM (as defined below) AND/OR ACCEPTING THIS AGREEMENT, YOU ARE CONSENTING TO BE BOUND BY ITS TERMS.

1. Definitions.

As used herein: "Software" means the Interoperability Engine™ software suite, including the phiMail® and phiQuery™ software and any other software suite components provided by the Company, access to any applicable related website or network resources intended for use with the Interoperability Engine software suite or any of its components, and any other software delivered to Subscriber in connection with this Agreement, as applicable, in the form intended by Company for use by the Subscriber (i.e., in each case in object code format and/or as a user interface/user experience only), or as documented in accompanying manuals issued by the Company, and any updates or upgrades thereto provided by Company to Subscriber in Company's sole discretion; "Computer" means any computer hardware central processing unit or network server; "Documentation" means any paper documentation regarding the Software, any electronic documentation regarding the Software, any help text, autocomplete assistance or tool tips provided by the Software and any other online or other documentation that is generally made available by Company to users of 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; the Software is further described in Exhibit A attached hereto. "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. "Trust Anchor" means a security certificate that, when installed in the System's trust repository, said certificate and any subordinate certificates are trusted by the System. "Trust Bundle" means a dynamic collection of Trust Anchors that, when included in the System's trust repository, is polled by the System at prescribed intervals, as determined by Company, to update the System's trust repository to reflect the contents of said Bundle. "Authorized User" means an end user affiliated with Subscriber who has been authorized by Subscriber to use the System. "Certificate" means a digital certificate issued by Company's CA for use with the System. "System" means any Company website or network resources, Software and Documentation, Codes, Subscriber web site and management tools, Certificates, public repository materials maintained by

Company's CA, Company's PKI, and any services, programs, functions and information provided by Company to Subscriber. "Sandbox" means the portion of the System intended by Company for testing and development by Developers. "CP/CPS" means the current version of the phiCert Direct Certification Authority Certificate Policy and Certification Practices Statement, as amended from time to time, located at https://www.phicert.com/cps. Software "Hosted by Company" means that the Software used by you or your Authorized Users to send or receive data is operated on hardware that is under the control of Company. "PHI" means Protected Health Information as defined by HIPAA. "Excessive Use" means use of the Software Hosted by Company by a Subscriber or Authorized User that exceeds two times the 99th percentile of System use observed by Company for Subscribers and Authorized 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 transactions processed. You are a "phiCert Subscriber" if you or any of your Authorized Users have applied for or have been issued one or more Certificates or use the components of the System related to management of Certificates. You are a "phiMail Subscriber" if you or any of your Authorized Users uses the System to send or receive Direct messages. You are a "phiQuery Subscriber" if you or any of your Authorized Users uses the phiQuery components of the System to send or receive data through the System. You are a "Developer" if you have been issued Codes to access the Sandbox. You may be a phiCert Subscriber, a phiMail Subscriber, a phiQuery Subscriber, a Developer, or a combination thereof. You are a Health Information Service Provider ("HISP") if you hold private keys corresponding to at least one Direct Certificate issued by Company and used by you to digitally sign or decrypt Direct messages. You are a "Hosted Subscriber" if you or your Authorized Users use Software Hosted by Company to send or receive data. "Reseller" means a phiMail or phiQuery Subscriber who is Using Software Hosted by Company to send and/or receive data through the System on behalf of one or more third parties. "Reseller Customer" means an entity that has authorized Reseller to send and/or receive data through the System on its behalf. Without limitation, Reseller includes phiMail and phiQuery Subscribers who are operators of electronic medical records systems or other healthcare applications that access the System on behalf of one or more Reseller Customers. "Organizational Representative" means an authorized representative of Subscriber who has been approved by our CA.

2. License Grant.

Company grants you a non-transferable, non-exclusive, revocable, limited license for you and your Authorized Users 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.

SUBSCRIBER SHALL NOT ITSELF OR THROUGH ANY AGENT OR THIRD PARTY (AND SUBSCRIBER SHALL CAUSE ITS AUTHORIZED USERS NOT TO) 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, without limitation, Subscriber shall not itself or through any agent, or third party (and Subscriber shall cause its Authorized Users not to): (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) use any XML or

HTML code that is (or is produced by) the Software or any portion of the Software with any software other than a commercially available browser or software provided by or approved by Company for using such code, except that Subscriber may use any export feature of the Software as intended by Company, (iii) open or view any XML or HTML code in its form as such (as opposed to, for use in its intended user interface/user experience form) or (iv) open, view, or otherwise use any portion of the Software that is resident on any server on any single computer hardware central processing unit that is not a server intended by Company to execute such server-resident Software, (v) monitor, interfere with, or reverse engineer the technical aspects of the System, (vi) intentionally compromise the security of the System or take any action intentionally, or intentionally neglect or omit to take any action, that compromises the availability or security of the System, (vii) use the system to transmit computer viruses or other malicious content, (viii) sell, lease, license or sublicense the System or Documentation; or (ix) use the System to provide services to third parties, except as permitted by Section 12 of this Agreement. Subscriber will promptly notify Company of any unauthorized disclosure, reproduction or distribution of the System, Documentation, or any Codes, which comes to Subscriber's attention, or which Subscriber reasonably suspects. Subscriber is solely responsible for obtaining all equipment and ensuring the compatibility thereof with the System, for determining the suitability of said equipment for the purposes of operating the Software or using the System, and for paying all fees including, without limitation, all taxes, regulatory fees, and Internet access fees, necessary to use the System. Subscriber's responsibilities under the immediately preceding sentence include determining the suitability of any computers or devices, including mobile devices, browser software, network configuration and internet service, or other hardware or software used by Subscriber or any of Subscriber's Authorized Users to access PHI or other data through the use of 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 using the System. Subscriber agrees that when Hosted by Company, the System may only be used in association with email addresses, resource endpoints, and/or sub-domain names expressly approved by Company. For any DNS domain or subdomain that is not controlled by Company, Subscriber warrants that Subscriber has the right to use the domain, subdomain, or email address requested by Subscriber, and is solely responsible for delegating any applicable DNS zone under its control to Company in accordance with the Documentation. A Subscriber and its Authorized Users shall not use a Certificate or its corresponding private key (i) for any purpose other than those permitted by this agreement, (ii) for purposes inconsistent with the permitted key usage and extended key usage asserted in each certificate (iii) if the Subscriber or the Authorized User is not authorized to do so by our Certification Authority or (iv) to sign other certificates. Subscriber agrees that Subscriber will not use the System for any purpose that is unlawful or prohibited by this Agreement. If Subscriber is also an Authorized User, Reseller Customer, or HISP Customer of another party that has separately entered into a license agreement with Company, then Subscriber acknowledges that the terms of that separate agreement may also affect Subscriber's access to or use of the System.

4. HIPAA and HITECH; User Responsibilities.

A. SUBSCRIBER ATTESTS THAT SUBSCRIBER AND ITS AUTHORIZED USERS HAVE A VALID NEED TO SECURELY EXCHANGE PROTECTED HEALTH INFORMATION, AND SUSCRIBER AND ITS AUTHORIZED USERS AGREE TO HANDLE AND PROCESS SUCH INFORMATION ACCORDING TO ALL APPLICABLE LAWS. Subscriber agrees to maintain suitable facilities, management, operational, and physical controls to protect their Codes consistent with the security and privacy controls imposed by HIPAA, HITECH, and

any other applicable law or regulation, and to treat all Codes issued to them with no less care and protection than that afforded to Protected Health Information. Such protection includes but is not limited to practices such as the use of memorized, strong passwords; device- and monitor-based screen passwords; application timeouts after short periods of inactivity; and logging out of System after Use. Subscriber acknowledges and agrees that Subscriber shall use the System only as and to the extent permitted by applicable law, including any applicable import or export laws, and only for (i) applications related to the secure transport of 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 or (ii) authenticated communications with Company, including communications incidental to Certificate issuance, renewal, re-keying, and modification. Subscriber and Company acknowledge and agree that Company is not a Covered Entity and that whether Company is a Business Associate of Subscriber as defined by HIPAA or HITECH shall be determined by applicable law. Subscriber agrees that Subscriber 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. Subscriber and Company acknowledge that, even if company provides an electronic mailbox and/or resource endpoint for Subscriber's use with the Software, Company will not have access to Protected Health Information, except as permitted in Section 15 of this Agreement. Company agrees that Company will not intentionally access any unsecured Protected Health Information, and will not intentionally configure the System to allow Company or unauthorized third parties access to any unsecured Protected Health Information.

B. Additional terms for phiMail and phiQuery Subscribers. This Section 4B applies to you and your Authorized Users only if you are a phiMail and/or phiQuery Subscriber. Subscriber acknowledges that the System is a data transport tool and is not intended to serve as a medical record, and that it is the sole responsibility of the Subscriber to establish policies and procedures that ensure that any data sent or received though the System is incorporated into a patient's medical record, when applicable. Subscriber agrees to treat Protected Health Information received or transmitted through the System by Subscriber or its Authorized Users with privacy and security protections meeting or exceeding those required by HIPAA, and to allow access to PHI only to authorized parties, even if Subscriber is not bound by HIPAA. Subscriber agrees that it is Subscriber's sole responsibility to 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 through the System by Subscriber or its Authorized Users, use of their Certificate, or initiation of any transmission of data with a digital signature that may be verified by a third party relying upon Subscriber's Certificate. Subscriber agrees that it is Subscriber's sole responsibility to route any data it receives or retrieves from the System for Subscriber or any of its Authorized Users to the correct recipient and that receipt or retrieval of a Direct message by Subscriber from the System shall constitute final delivery by Company of that message. Subscriber agrees that if the System is Hosted by Company, Company has no obligation to archive or otherwise store any data that (i) has been retrieved from System by Subscriber or an Authorized User, (ii) has been delivered by System to Subscriber or an Authorized User, (iii) is transmitted through System by Subscriber or an Authorized User, (iv) is refused by System because it is received from an untrusted source, is not in a format allowed by System, would cause Subscriber's message queue size to exceed the allowable maximum permitted by Company, or for any other reason, (v) is marked for deletion by Subscriber or an Authorized User, (vi) exceeds the maximum allowable message age permitted by Company for the purchased service type, (vii) cannot be delivered to Subscriber within the maximum number of

delivery attempts permitted by Company because the Subscriber's receiving system rejects the message, is unavailable or unreachable, or for any other reason, (viii) is in a mailbox or message queue when Subscriber or Subscriber's authorized representative requests termination or closure of the mailbox or account, the associated codes expire or are revoked, or this Agreement terminates, or (ix) cannot be processed by the software used by Subscriber or its Authorized Users. Subscriber acknowledges that Company does not control the content of data sent or received through the System, that data accessed through the System may contain software viruses or other malicious content, that it is Subscriber's sole responsibility to protect Subscriber's computer systems from viruses, and that Company has no responsibility to protect any of Subscriber's computer systems or any patients' or doctors' or other correspondents' or data recipients' computer systems from viruses or other malware. Subscriber is solely responsible for establishing which third parties are trustworthy for exchange and for adding or, when Software is Hosted by Company, requesting that Company add one or more Trust Anchors or Trust Bundles to the System's trust repository. Company may make available one or more candidate Trust Anchors or candidate Trust Bundles issued by Company or by third parties for the convenience of Subscriber, but it is Subscriber's sole responsibility to assess each Trust Anchor or Trust Bundle to determine whether a particular anchor or bundle is suitable for addition to Subscriber's Trust Anchors. Subscriber agrees that the decision to open a message, attachment or other data from an untrusted sender, send to an untrusted recipient, or allow access to any phiQuery-enabled resources by any person or system, is at the sole discretion of Subscriber. Subscriber acknowledges that interoperation with counterparties or with software or services that are not provided by Company may involve interoperability assessment, such as negotiation of acceptable payloads and formats, and/or technical effort by Subscriber, Company, and/or counterparties, that the time required to enable or disable interoperability will vary, and that interoperability may not always be possible. Subscriber acknowledges that current certificate revocation information may not always be accessible by Company to validate the certificate status of a given counterparty certificate, and that unavailability of current revocation information may negatively impact interoperability. Subscriber agrees that Company may establish a grace period during which Company may use any previously available revocation information to validate certificate status when current revocation information is not accessible by Company for any reason. Subscriber further acknowledges that not all Trust Anchor operators provide certificate revocation information or regular updates to certificate revocation information, and not all Trust Bundle operators require the included Trust Anchor operators to provide this information, and that when a Subscriber enables trust with such a Trust Anchor or Trust Bundle, the Software will not reject an associated counterparty certificate solely because current certificate revocation information is not accessible by Company. Further, Subscribers Using Software Hosted by Company agree that Company, in its sole discretion, reserves the right not to interoperate with any particular counterparty or trust community. If Subscriber or Subscriber's Authorized Users are also end users of Interoperability Engine Open APIs, Subscriber is also subject to the terms of that service listed at https://www.interopengine.com/2017, as modified from time to time, and may also be subject to additional terms required by the developer or operator of the client application used to access the System and/or by the data holder that provides the data.

C. Subscriber and Subscriber's Authorized Users may make submissions of certain data and information to Company (the "User Submissions"), such as feedback related to the System, errors, problems, difficulties, or suggestions regarding access to or use of the System. Subscriber understands and shall ensure that Subscriber's Authorized Users understand that User Submissions are not and shall not be deemed to be confidential and/or proprietary information of Subscriber or

any Authorized User, regardless of whether any submission is marked "Confidential" and/or "Proprietary". All User Submissions of any type, whether written or oral, 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, without having any obligation or liability to Subscriber. Subscriber hereby warrants 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 and any audit log or debugging log files, to which it has or is given access in any form, to evaluate, test or improve the System or for other internal purposes related to the System or to this Agreement, or with external parties in order to troubleshoot interoperability issues, but only in accordance with HIPAA, HITECH, and any other applicable laws. Subscriber 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.

D. If 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 or Subscriber 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 or Subscriber 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 absolute 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 the consent of Subscriber or any other person or entity. If Company determines that compliance with such requirements is impossible, then this Agreement may be terminated by the Company without penalty upon five (5) business days prior written notice, or, if earlier as of the effective date upon which the Law or Action prohibits the relationship of the parties pursuant to this Agreement.

5. Authorization Codes and Certificates.

A. Company may limit the number of persons who can use the System. Subscriber may be issued one or more user identification codes or passwords, or means to create such passwords, for use in accessing the System. Subscriber may also be issued one or more private security keys and/or public security certificates for use with the System. All such user codes, including keys, certificates, or passwords, as well as any keys generated by the Subscriber for use with the System, are referred to herein as the "Codes." Subscriber is solely responsible for use and proper protection of the Codes, and agrees to take all reasonable precautions to protect the security and integrity of the Codes and to prevent their unauthorized use. Subscriber shall be responsible for all actions taken that utilize the Codes, unless such actions are taken by Company, its subcontractors or agents without Subscriber's approval.

B. Additional terms for phiCert Subscribers. This section 5B applies to you and your Authorized Users if you are a phiCert Subscriber. For the certificates we issue, Company warrants to Subscriber that to

the actual knowledge of the Company: (i) there are no material misrepresentations of fact in the Subscriber's certificate originating from Company, (ii) there are no errors in such certificate introduced by the Company as a result of a failure to exercise reasonable care in processing such certificate application or creating such certificate, (iii) their certificate meets all material requirements of the CP/CPS, (iv) revocation services and use of a repository by the Company in connection with such certificate conforms to the CP/CPS in all material respects and (v) Company has complied with all applicable laws and regulations that apply specifically to the issuance of such certificates. Subscriber warrants to Company that (a) all information supplied by the Subscriber or Subscriber's authorized representative and contained in the certificate is true, correct and complete, (b) all representations made by the Subscriber in the certificate application submitted by the Subscriber or Subscriber's agent are true, correct and complete, (c) no unauthorized person has ever had access to Subscriber's private key corresponding to the public key listed in the certificate, (d) Subscriber is an end user and is not using said private key to digitally sign any other certificate, similar security instrument, or certificate revocation list, as a Certification Authority or otherwise, (e) each digital signature created using said private key is the digital signature of the Subscriber, (f) that the corresponding certificate was valid (e.g., not expired or revoked) at the time that the digital signature was created, (g) the certificate is being used exclusively for legal and authorized purposes consistent with this agreement and the CP/CPS, and (h) Subscriber has not included trademarks in Subscriber's certificate application unless Subscriber also possesses the rights to use the respective names. Subscriber and Company agree not to escrow any private keys used with System.

C. Additional terms for phiCert Subscribers who hold private keys. This section 5C applies to you and your Authorized Users if you hold a private key corresponding to the public key in any Certificate issued by us. Subscriber acknowledges that loss or corruption of a private key held by Subscriber may result in permanent loss of access to encrypted materials as Company's Certification Authority does not archive or back up Subscriber private keys. Subscriber agrees that Subscriber is solely responsible for (i) backing up private keys in their possession to a secure offsite location in a manner and form of their choosing, and (ii) determining if private key archival is appropriate for their specific circumstances, and, if required, choosing the manner, form, and location in which their keys are archived; Subscriber agrees that all copies of private key not exclusively stored by the Company on Subscriber's behalf, including any backup or archival copies, shall be held by Subscriber in Subscriber's control and will never be stored in plaintext form outside of Subscriber's cryptographic module. Subscriber agrees to protect private keys using a suitable cryptographic module, to destroy private keys in their control when they are no longer needed, using any suitable method, and to cease use of any private signing key before the six year anniversary following such key's generation.

D. If Subscriber becomes aware of any unauthorized access or use of the System or any other part thereof, Subscriber shall immediately notify Company. If Company determines in its sole discretion that Subscriber is or may be using a certificate issued by Company for purposes other than those allowed by this agreement, Company may, in its sole discretion, revoke the Subscriber certificate. For certificates issued by Company for use by a device operated by Subscriber, with an Authorized User acting as device sponsor, Subscriber agrees that if the device sponsor changes, the new sponsor shall review the status of each device to ensure that it is still authorized to use the issued certificates, that the new sponsor is authenticated according to the requirements of Company's CA, and that the new sponsor is an Authorized User. Subscriber agrees that all required fees shall be paid by Subscriber to Company prior to issuance of any new, re-keyed, renewed, or modified certificates, or the use of any

associated private keys. Following issuance of a certificate, Subscriber has seven (7) days to accept or reject the certificate. Any use of certificate by Subscriber shall be deemed acceptance whether or not notice of rejection has been sent to the Company. After seven (7) days have passed, the certificate will be deemed to have been accepted by Subscriber unless notice of rejection has been given through the Company's secure Subscriber website in the manner described below. Subscriber may reject the certificate only if the certificate has not been used and contains information that is incorrect or incomplete when compared with the information submitted by Subscriber and verified by Company prior to issuance. Rejection of a certificate must be done through Company's secure Subscriber website pursuant to the express instructions for "Certificate Rejection" located at https://www.emrdirect.com/phimail/accountmanagement.php. Unpaid or overdue accounts are subject to certificate and/or software license revocation at Company's sole discretion and without prior notice. Company may also revoke any unexpired certificate if this license agreement terminates. Subscriber agrees that they have read, understood, and agree with the terms of the CP/CPS. If the CP/CPS is updated, the new CP/CPS will apply to any certificates issued, renewed, re-keyed or modified after the effective date of the updated version. Subscriber agrees to the conditions under which certificate renewal, re-keying, and modification are permitted as outlined in the CP/CPS. Company may modify a Certificate issued to Company or to a Subscriber 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 Trust Bundle in which Company participates or intends to participate, or that Company or Subscriber do not meet or cease to meet the inclusion requirements for a trust community or Trust Bundle. Subscriber will cease use of all private key(s), certificates and Codes at the end of Subscriber's subscription period, or following expiration or revocation of the corresponding certificate or of the license granted hereunder, will promptly notify Company if any information in Subscriber's certificate is inaccurate or has changed, and will protect Subscriber's private keys and other Codes from unauthorized access. If a Subscriber discovers, or has reason to believe that Subscriber's private key or other Code has been compromised, or that information contained in their certificate is inaccurate or has changed, Subscriber agrees to promptly notify Company to request revocation or modification of the certificate, and to promptly notify any person or organization that may reasonably be expected to rely on Subscriber's certificate or any digital signature verifiable with reference to the Subscriber's certificate. Subscriber agrees that a certificate issued to Subscriber shall be revoked if any of the following circumstances exists: (i) the identifying information or affiliation attributes of any names in the certificate become invalid, (ii) the private key (or its password) associated with the certificate has been compromised or is suspected of compromise, (iii) Subscriber ceases to have a valid need to securely exchange health information, (iv) Subscriber has violated any of the terms of this Agreement, (v) Subscriber is no longer using the certificate for a purpose permitted by this Agreement, (vi) this Agreement expires without being renewed or is otherwise terminated, (vii) Subscriber requests that the certificate be revoked, or (viii) any other circumstances exist that require revocation under the CP/CPS. Subscriber agrees to request revocation immediately through the Company's secure website located at https://www.emrdirect.com/phimail/accountmanagement.php if any of the circumstances in (i)-(vi) exist. There is no grace period for revocation. Subscriber agrees to request revocation of any certificate issued to them as soon as the need for revocation comes to their attention. Without limiting the last sentence of Section 7, this Section 5 will survive any termination of this Agreement.

6. Proprietary Rights and Audits.

A. 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, and 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. Subscriber will, upon expiration or termination of this Agreement, whichever occurs earlier, or upon any request by Company, immediately return or destroy, to the extent requested by the Company, any other Company Information (and all portions and copies thereof), in each case as directed by Company, and if requested by Company, certify in writing as to the destruction or return of such Company Information.

B. Additional terms for phiMail Subscribers when the Software is not Hosted by Company. This Section 6B applies to you and your Authorized Users only if you are a phiMail Subscriber and you are not a Hosted Subscriber. At Company's request and upon reasonable notice, Subscriber will grant Company or its auditors reasonable access to each facility, site or location where any copy of the System is installed (including physical access to each such location for the purpose of examining the actual Computers and applicable non-Computer servers at such facilities) for the purpose of verifying Subscriber's compliance with the terms of this Agreement.

7. Term and Termination.

The term of this license shall begin on the date of Subscriber's acceptance of this Agreement, first use of the System, or upon issuance of Codes to Subscriber by Company, whichever occurs earliest. This license will automatically terminate without notice to Subscriber upon expiration or revocation of all Codes issued to Subscriber by Company or upon the termination of this Agreement as provided herein, whichever occurs earlier. Either party may terminate this Agreement for their convenience upon sixty (60) days prior written notice to the other party through the Company's secure website. This Agreement will also terminate immediately upon written notice through the Company's secure website to Subscriber if Subscriber fails to comply with any of its terms. If you are a Hosted Subscriber, Company may also terminate this Agreement without notice at the conclusion of the service term purchased by Subscriber if applicable renewal fees are not received by Company on or before the service renewal date. Upon any termination, all rights and licenses granted to Subscriber under this Agreement shall immediately terminate and, if Subscriber or Subscriber's employees or consultants have been issued any Code(s), Subscriber shall destroy and discard (or cause to be destroyed or discarded) all copies of any Code(s). Upon any termination, Company may, in its sole discretion, also revoke any digital credentials issued to Subscriber under this Agreement. 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. SUBSCRIBER ACKNOWLEDGES AND AGREES THAT THE SYSTEM AND ANY CONTENT ARE PROVIDED TO SUBSCRIBER "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 SUBSCRIBER OR ANY THIRD PARTY. COMPANY DISCLAIMS ANY LIABILITY FOR ANY DAMAGES TO SUBSCRIBER'S COMPUTER OR ANY THIRD PARTY'S COMPUTER OR OTHER PROPERTY CAUSED BY OR ARISING FROM SUBSCRIBER'S USE OF THE SYSTEM, WHETHER DUE TO INFECTION BY A SOFTWARE VIRUS OR OTHER MALWARE OR OTHER CAUSE. Subscriber agrees that Company and Subscriber are independent contractors and that neither has any fiduciary responsibility to the other. In furtherance of the immediately preceding sentence, each of Company and Subscriber agree to never assert for its own benefit that the other has any fiduciary duties and to the extent permitted by applicable law, Subscriber and Company hereby disclaim any fiduciary relationship between Company on one hand and Subscriber on the other hand. Subscriber further acknowledges that some content, including but not limited to any 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. Subscriber acknowledges 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, routers, domain name system (DNS) servers (including DNS servers or DNS records under your control), mail servers, directory servers, certificate status servers, electronic health record systems, client software applications, and HISP systems serving counter parties to message exchange with Subscriber, and Subscriber agrees that Company is not responsible for the reliability or availability of those systems.

B. Additional terms for phiMail and phiQuery Subscribers. This Section 8B applies to you and your Authorized Users only if you are a phiMail or phiQuery Subscriber. Subscriber acknowledges that the System is designed to facilitate secure delivery of health content over the Internet. Subscriber acknowledges and agrees that each user's needs and data are unique, and that Subscriber's inputs and information and Subscriber's use to generate customized reports and outputs or other data based on Subscriber's own needs and data, may cause Subscriber's experience to differ from other users and that Subscriber assumes the entire risk of Subscriber's reliance on the System and any reports, information or any other content generated thereby. Subscriber is solely responsible for tracking and maintaining logs of any data transmitted through the system to or from Subscriber or its Authorized Users. Subscriber acknowledges that the transmission of data through System may require data to pass through other systems that are not controlled by Company, and Subscriber agrees that Company is not responsible for the timeliness or reliability of delivery or receipt of data, including message disposition notifications, through the System. Subscriber and its Authorized Users are solely responsible for properly accessing the System in accordance with the Documentation, including, as applicable, performing regular polling for incoming messages and status notifications, maintaining active connections to respond to any incoming queries, and/or any other client requirements described in the Documentation. Subscriber agrees that Subscriber and Subscriber's Authorized Users 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. Subscriber 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, OR FOR ANY LIABILITY (II) ARISING FROM INFORMATION IN A CERTIFICATE, UNLESS THE FAULT IN THE INFORMATION IS DUE TO FRAUD OR WILLFUL MISCONDUCT OF THE COMPANY, (III) ARISING FROM THE USAGE OF A CERTIFICATE THAT IS NOT VALID OR HAS NOT BEEN USED IN CONFORMANCE WITH THIS AGREEMENT, (IV) ARISING FROM COMPROMISE OF A SUBSCRIBER'S PRIVATE KEY OR OTHER CODE, OR (V) FOR ANY MATTER OUTSIDE THE COMPANY'S CONTROL INCLUDING, WITHOUT LIMITATION, IF COMPANY CANNOT EXECUTE THE REVOCATION OF A CERTIFICATE 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 SUBSCRIBER UNDER THIS AGREEMENT IN THE TWELVE MONTHS PRECEDING THE FIRST CLAIM MADE BY SUBSCRIBER AGAINST THE COMPANY, REGARDLESS OF THE NUMBER OF TRANSACTIONS OR CAUSES OF ACTION ARISING OUT OF OR RELATED TO ANY SERVICES PROVIDED BY 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. Subscriber agrees that Subscriber is solely responsible for any loss or damage resulting from Subscriber failing to meet the requirements of this agreement and of the CP/CPS for the protection of their private keys and other Codes.

10. Indemnification.

Subscriber agrees 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 use of the System by Subscriber or Subscriber's Authorized Users, 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.emrdirect.com/privacy.html.

12. Resellers.

This Section 12 applies to you and your Authorized Users only if you are a Reseller. Reseller attests that Reseller has identified itself to Company as a Reseller and agrees that Reseller shall not exchange health information through the System on behalf of a Reseller Customer until approved to do so in writing by Company. Reseller attests that Reseller is authorized by each Reseller Customer to

exchange health information on behalf of each Reseller Customer, and that, where required by HIPAA or other regulation, Reseller has entered into a suitable Business Associate Agreement with each Reseller Customer that permits Reseller to exchange Protected Health Information on behalf of each Reseller Customer through the System. Reseller and Company agree that it is the sole responsibility of Reseller to (a) deliver received data to Reseller Customer once Reseller acknowledges receipt of data through an approved interface to the System, (b) provide any accounting of Disclosures of Protected Health Information to Reseller Customers, (c) provide any accounting of other metrics or user-based auditing to Reseller Customers as may be required by Reseller Customer to meet obligations under applicable law, regulation, or other standard, and (d) if Reseller provides access to System to Reseller Customers through Reseller's application or interface, provide obvious visual indicators to alert Reseller Customers as to the potential access to Protected Health Information through such application or interface, and the privacy and security requirements of such access. Reseller agrees to protect the Codes of Reseller Customers, and to maintain an accounting of all Reseller Customers with access to Codes, including when access to Codes was established and terminated. Reseller further agrees that Reseller is solely responsible for authenticating each Reseller Customer using an authentication method approved by Company prior to accessing the System on Reseller Customer's behalf, that Reseller must maintain an accounting of which Authorized User has access to Codes or to the System at any given time sufficient to determine which Authorized User exchanged health information through the System at a given time for all transactions, and will provide the name of the Authorized User associated with a specific transaction to Company upon Company's request. Reseller will maintain such an accounting of access for the time periods required by HIPAA, HITECH, and other applicable laws. Reseller agrees that each Reseller Customer is an Authorized User of Reseller. Reseller agrees to enter into suitable contracts with each Reseller Customer that bind Reseller Customers to the applicable terms of this Agreement, and that Reseller will make these contracts available to Company upon request. Reseller agrees not to access System on behalf of a Reseller Customer if such a contract is not in place, has expired, or has otherwise been terminated. Company may also require each Reseller Customer to enter into a separate phiMail Software License Agreement or other similar Agreement with Company prior to Reseller's use of System on behalf of that Reseller Customer. Reseller agrees to access System on behalf of Reseller Customers only through interfaces approved by Company, and further agrees not to provide direct access to the System interfaces to a Reseller Customer without written consent of Company. Reseller agrees that Reseller is responsible for all fees charged by Company related to System Use, certificate issuance, renewal, re-keying, or modification of a certificate issued by Company to a Reseller Customer at Reseller's request, and acknowledges that Reseller Customer certificates and Codes may be revoked or disabled by Company if fees are not paid. Company agrees that Reseller may charge or choose not to charge, as Reseller sees fit, fees to Reseller Customer for any use of the System by Reseller on Reseller Customer's behalf.

13. Health Information Service Providers.

This Section 13 applies to you and your Authorized Users only if you are a HISP. HISP shall appoint at least one Information Systems Security Officer (each an "ISSO" and, collectively, the "ISSOs"). HISP shall require each ISSO to perform all ISSO duties in accordance with this Agreement and the CP/CPS. Each ISSO will be approved by Company only after he or she has been successfully identity proofed by Company in accordance with the CP/CPS. HISP agrees that all private keys corresponding to any public key listed in a Certificate issued to HISP or to any end user or organization serviced by HISP (the "HISP Customers") shall be secured and managed exclusively by approved ISSOs, and shall never be

provided to any other party. HISP shall require each HISP Customer to agree to the terms of this Agreement as a phiCert Subscriber, and to authorize HISP ISSOs to exclusively secure and manage private keys and certificates on behalf of the HISP Customer, such agreement and authorization to be made in writing and provided to Company at the time of application for a Certificate. HISP agrees that each ISSO shall restrict the use of private keys only to Authorized Users of the corresponding Certificate. HISP, HISP ISSOs, HISP Customers and their Authorized Users are phiCert Subscribers as defined in this agreement. All requests for issuance, renewal, modification, re-keying or revocation of certificates issued to HISP or HISP Customers must be made by an ISSO. HISP is solely responsible for any fees charged by Company in conjunction with any such request. HISP agrees to maintain an access control list for private keys corresponding to each certificate issued by Company and managed by HISP ISSOs, including an accounting of which Subscriber(s) had access to use each Private Key at any time and when such access was granted or terminated, and to provide the current access control list to Company within seven (7) days upon Company's request. HISP ISSOs may delegate management of such access control list to a HISP Customer, but HISP is solely responsible for collecting any list managed by a HISP Customer when needed, ensuring the accuracy thereof, and submitting the list to Company within the seven (7) day time frame. HISP acknowledges, and will require any HISP Customer to whom list management is delegated to acknowledge, that failure to supply the information required is a violation of this Agreement and the CP/CPS and may result in immediate revocation of any associated Certificate.

14. Fees and Refund Policy.

All fees are due prior to the start of service and prior to any applicable annual renewal date. Certificates may be corrected prior to acceptance, as defined in Section 5, at no additional fee. After acceptance or after activation of services, whichever is earlier, refunds are not available. Fees will not be prorated for use for a period of less than a year or for any other circumstance. In the case of Excessive Use of the System by Subscriber or one of Subscriber's Authorized Users, Company, in its sole discretion, may limit access to System, require payment of additional fees by Subscriber as a condition of allowing ongoing Use, or terminate this Agreement. Additional fees will also apply for modification, re-keying or renewal of certificates issued by Company or for modification of previously activated services. A current fee schedule is available upon request from Company. Fees are subject to change without notice. Notwithstanding the preceding sentence, if this Agreement includes an attached fee schedule as Exhibit B, then the fee schedule in Exhibit B shall apply for the services included therein during the effective period specified therein, or for the 12 month period starting with the beginning of the term of this Agreement if Exhibit B does not specify an effective period.

15. Business Associate Agreement.

This Section 15 (the "BAA") applies to you and your Authorized Users only if you are a Hosted Subscriber (the acceptance date of the associated Certificate by Subscriber or first use of the System by Subscriber or any of Subscriber's Authorized Users, whichever is earliest, is the beginning of the "BAA Term"), and, further this BAA applies only for the validity period of such Codes (the expiration date or revocation date of the associated Certificate or deactivation of Subscriber's services, whichever is earliest, is the last day of the corresponding "BAA Term"). If you are not a Hosted Subscriber and your subscription status is changed so that you become a Hosted Subscriber, this BAA will apply to you during the time you are a Hosted Subscriber; if you are a Hosted Subscriber and your subscription

status changed so that you are not a Hosted Subscriber, this BAA will terminate. Notwithstanding the above, this BAA shall not apply to you if you are a Reseller Customer of a Reseller who has entered into a Business Associate Agreement with us and you and your Authorized Users only access the System through software or services provided by the Reseller. Notwithstanding the above, section 15C(ii)-(iii) shall apply to all Subscribers.

A. Definitions. Catch-all definition: The following terms used in this BAA (or alternate forms or conjugations thereof) shall have the same meaning as those terms in the HIPAA Rules: Breach, Designated Record Set, Disclosure, Protected Health Information, Required By Law, Secretary, Security Incident, Subcontractor, Unsecured Protected Health Information, and Use. Specific definitions: "Company as Business Associate" shall generally have the same meaning as the term "business associate" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean Company, when Company meets the definition of Business Associate under HIPAA. "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 CFR 160.103, and in reference to the party to this agreement, shall mean a Subscriber who is a Covered Entity or a Business Associate and who is a Hosted Subscriber. "HIPAA Rules" shall mean the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Part 160 and Part 164.

B. Obligations and Activities of Company as Business Associate. Company as Business Associate agrees to: (i) not Use or Disclose Protected Health Information other than as permitted or required by this Agreement or as Required By Law; (ii) employ appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 with respect to electronic Protected Health Information, to prevent Use or Disclosure of Protected Health Information other than as provided for by this Agreement; (iii) report to Covered Entity any Use or Disclosure of Protected Health Information not provided for by this Agreement of which it becomes aware, including Breaches of Unsecured Protected Health Information as required at 45 CFR 164.410, and any Security Incident of which it becomes aware; (iv) in accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, ensure that any Subcontractors that create, receive, maintain, or transmit Protected Health Information on behalf of the Company as Business Associate agree to the same restrictions, conditions, and requirements that apply to the Company as Business Associate with respect to such information; (v) make available to Covered Entity the information required to assist Covered Entity in providing an accounting of Disclosures as necessary to satisfy Covered Entity's obligations under 45 CFR 164.528; Specifically, Company as Business Associate will make available to Covered Entity through Company's approved interfaces status information relating to messages transmitted by Covered Entity, as specified in the Documentation. It is the sole responsibility of Covered Entity, however, to retrieve this information, to provide accounting of Protected Health Information disclosed by Covered Entity in each disclosure made by Covered Entity, including the recipient, the date of transmission, and the data included in each transmission as well as any other information Required By Law, and to update this accounting information as applicable with the status information made available by Company; (vi) to the extent the Company as Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 CFR Part 164, comply with the requirements of Subpart E that apply to the Covered Entity in the performance of such obligation(s); and (vii) make its internal practices, books, and records available to the Secretary for purposes of determining compliance with the HIPAA Rules.

C. Permitted Uses and Disclosures by Company as Business Associate

(i) Company as Business Associate may, in the course of troubleshooting system issues, encounter incidental occasional exposure to Protected Health Information, and may use this Protected Health Information for the purpose of troubleshooting the System. Covered Entity acknowledges that when Covered Entity or one of its Authorized Users uses the System to transmit or receive data, the Company as Business Associate is agnostic as to the content of the data sent to or received by Covered Entity and serves merely as a conduit for transmission of Protected Health Information to and from Covered Entity, and that any temporary storage of Protected Health Information by Company as Business Associate in the process of sending or receiving data is only incidental to such transmission. Covered Entity agrees that use of the System by Covered Entity or one of its Authorized Users to send data to a recipient is a Disclosure of any included Protected Health Information by Covered Entity to the specified recipient, and is not a Disclosure by Company as Business Associate to the recipient.

(ii) Company as Business Associate may use or disclose Protected Health Information as required by law, regulation, legal process or enforceable governmental request.

(iii) Company as Business Associate agrees to make Uses and Disclosures and requests for Protected Health Information only as required to fulfill items (i) and (ii) immediately above.

(iv) Company as Business Associate may not Use or Disclose Protected Health Information in a manner that would violate Subpart E of 45 CFR Part 164 if done by Covered Entity.

D. Term and Termination

(i) BAA Term. Each BAA Term will continue for so long as provided in the first paragraph of this BAA, and shall terminate early, if applicable, on the expiration date of Covered Entity's certificate(s) or, if earlier, on the date Covered Entity terminates this BAA for cause as authorized in paragraph (ii) of this Section, whichever is sooner. Simultaneously with any termination of this BAA, Subscriber shall be deemed not a Hosted Subscriber.

(ii) Termination for Cause. Company as Business Associate authorizes termination of the BAA term by Covered Entity, if Covered Entity determines Company as Business Associate has violated a material term of this BAA and Company as Business Associate has not cured the breach or ended the violation within the time specified by Covered Entity, or, if longer, within five business days after notice to the Company through Company's secure website.

(iii) Obligations of Company as Business Associate Upon Termination. Upon termination of this BAA for any reason, Company as Business Associate, with respect to Protected Health Information which may be in Covered Entity's account, shall: Retain only that Protected Health Information which is necessary for Company as Business Associate to continue its proper management and administration or to carry out its legal responsibilities; Destroy the remaining Protected Health information that Company as Business Associate still maintains in any form; Continue to use appropriate safeguards and comply with subpart C of 45 CFR Part 164 with respect to electronic Protected Health Information to prevent Use or Disclosure of the Protected Health Information, other than as provided for in this Section, for as long as Company as Business Associate retains the Protected Health Information; Not Use or Disclose the Protected Health Information retained by Company as Business Associate other than as required by law; and Destroy the Protected Health Information retained by Company as Business

Associate when it is no longer needed by Company as Business Associate for its proper management and administration or to carry out its legal responsibilities.

(iv) Survival. The obligations of Company as Business Associate under this Section shall survive the termination of this BAA.

E. Miscellaneous. Any ambiguity in this Agreement shall be interpreted to permit compliance with HIPAA, HITECH, and other rules and laws.

16. Trusted Agents.

If you are a phiCert Subscriber, you accept the role of "Trusted Agent" of Company for the purpose of verifying identities in accordance with the CP/CPS. You may designate one or more of your employees or agents (each a "Verifier") to perform these identity verification duties. You acknowledge that you are fully responsible for ensuring that each Verifier complies with the terms of this Agreement and with the requirements of the CP/CPS. You further agree that: (a) you will remove from the role of Verifier any person who ceases to be your employee or agent or who otherwise fails to meet the requirements of this Agreement; (b) Verifiers shall gather, document, and record all identification and authentication materials and data (the "Verification Records") in accordance with this Agreement and the CP/CPS; (c) you shall retain the Verification Records for the period specified in the CP/CPS, even if this period extends beyond the term of this Agreement; (d) you will make any Verification Records requested by Company during the retention period specified in the CP/CPS available to Company within a reasonable timeframe; and (e) you will submit information required by this Agreement to Company only through Company's secure administrative website or other secure channel in a manner approved by Company. For each person that you verify as Trusted Agent, you attest that sufficient Verification Records exist to substantiate that the identity of that person has been verified in accordance with the requirements of the CP/CPS at the required Level of Assurance. You agree that you shall only grant access to use a Certificate issued to you (or its corresponding private key) to your employees and agents whose identities have been successfully verified at or above the Level of Assurance of such Certificate in accordance with this Agreement, either by Company or by you as Trusted Agent, and that you will terminate such access if a person ceases to be your employee or agent. You acknowledge that failure to provide Verification Records to Company in the timeframe specified by Company and meeting the identity proofing requirements of the CP/CPS, as determined in Company's sole discretion, may result in immediate revocation of any associated Certificates issued by Company and termination of Trusted Agent status and/or this Agreement.

17. Directories.

A. Company may choose to provide directory information to certain Authorized Users in one or more formats, such as through directory search tools. Company may obtain directory information from its own databases and/or from other sources. Company is not responsible for any errors or omissions in the directory information provided. You agree that you and your Authorized Users will use directory information only for the purpose of identifying the Direct address or API endpoint of an intended exchange partner included in the directory, and will not (i) provide directory information obtained from Company to any third party HISP or permit a third party HISP to acquire or create a copy of directory information, (ii) sell, disclose or make available directory information to any third party that

is not an Authorized User of Software Hosted by Company, (iii) provide and/or use directory information to solicit business, to distribute surveys or advertisements, for spamming messages or mass mailings, for direct marketing, database marketing, telemarketing, marketing analysis, or research purposes, or to support Direct messaging or HISP services provided by any party other than Company, (iv) retain local copies of directory information other than those directory results matching intended recipients of Direct messages identified by Authorized Users. You acknowledge that if Company receives a complaint from a recipient that you or one of your Authorized Users has sent one or more unsolicited messages, or a request to block transmissions from any Direct address associated with you or your Authorized Users, or if Company determines, in our sole discretion, that you or any of your Authorized Users are using directory information for purposes prohibited by this agreement, Company may impose restrictions upon the associated account or accounts, revoke the associated certificate(s), require you to remove a recipient address from your records, and/or immediately terminate this Agreement.

B. You agree that, unless you have opted out, Company may publish certain information about you and your Authorized Users, including your company logo, the names of persons and organizations, business addresses, NPI numbers, specialties, telephone and fax numbers, Direct addresses, API endpoints and other related metadata, any information listed in NPI or other public records or in a public certificate, as well as any additional information submitted by you specifically for directory inclusion. If you have not opted out, you agree to keep this information up to date. Company may choose, in its sole discretion, which directory or directories in which to publish or stop publishing this information, including directories operated by Company or by third parties. If you opt out, Company will remove the corresponding entries from the directory information that Company publishes. You acknowledge that opting out does not guarantee that your information will be removed from directories published by other parties, and that your information may still appear in directory information obtained from other sources. Requests by an organization or by an Authorized User to opt out of directory listing must be made by an Organizational Representative and submitted through Company's secure website.

18. Developer use of the Sandbox

This Section 18 applies to you and your Authorized Users only if you are a Developer. YOU ACKNOWLEDGE THAT ACCESS TO THE SANDBOX IS GRANTED BY COMPANY FOR TESTING AND EVALUATION PURPOSES ONLY. YOU AGREE THAT THE SANDBOX MUST NOT BE USED BY YOU OR YOUR AUTHORIZED USERS TO SEND OR RECEIVE PROTECTED HEALTH INFORMATION. YOU AGREE THAT ABSOLUTELY NO PROTECTED HEALTH INFORMATION MAY BE USED WITH THE SANDBOX. You may only use properly de-identified data or other test data with the Sandbox. You acknowledge that access to the Sandbox is provided as a convenience to you intended to expedite your testing and development of software and services that can be used with the System, and you agree to use the Sandbox solely for your internal testing and evaluation purposes and not for the benefit of any third party. During the term of this Agreement, Company may decide not to (i) make the Sandbox available, (ii) continue developing the Sandbox, or (iii) offer Sandbox features outside the Sandbox, and, in each case, you agree that Company will have no liability as a result of any such decision. You agree that Company has access to, and may utilize, any and all information processed by or through the Sandbox, for improvement of the System, management of the Sandbox, or any other purpose. Company reserves the right to restrict and/or terminate access to the Sandbox at any time and from

time to time in its sole discretion. Performance testing or benchmark testing of the Sandbox System is prohibited. Notwithstanding anything to the contrary in this Agreement, you agree to notify all third parties with whom you intend to exchange data through the Sandbox as to the status of the Sandbox as a software testing environment for developers and not for use with Protected Health Information or in urgent or mission critical scenarios.

19. Confidentiality

A. Confidential Information. "Confidential Information" means all information disclosed by Company to you either before or during the term of this Agreement and which (a) is marked as "Confidential" at or before the time of disclosure, or (b) a reasonable person in the circumstances would know is confidential or proprietary information of the party disclosing such information. Without limiting or expanding the foregoing, the Software, Documentation, User Submissions, and any pricing information or fee schedules will be considered Confidential Information of Company.

B. Exceptions. Notwithstanding anything to the contrary, Confidential Information does not include information to the extent that such information: (i) is or becomes generally known to the public by any means other than a breach of your obligations hereunder; (ii) was previously known to you at the time of Company's communication thereof to you; (iii) is rightly received by you from a third party who is not under an obligation of confidentiality; (iv) is independently developed by you without reference to or use of the Confidential Information which such independent development can be established by evidence that would be acceptable to a court of competent jurisdiction; or (v) is Protected Health Information subject to the terms of Section 15 of this Agreement.

C. Confidential Treatment. You agree: (i) to maintain the Confidential Information in confidence and to take all reasonable steps, which shall be no less than those steps you take to protect your own confidential and proprietary information, to protect the Confidential Information from unauthorized use, disclosure, copying or publication; (ii) not to use the Confidential Information other than in the course of exercising your rights or performing your obligations under this Agreement; (iii) not to disclose or release such Confidential Information except to the extent required by applicable law or during the course of or in connection with any litigation, arbitration or other proceeding based upon or in connection with the subject matter of this Agreement, provided that you shall first give reasonable notice to Company prior to such disclosure so that Company may obtain a protective order or equivalent and provided that you shall comply with any such protective order or equivalent; (iv) not to disclose or release such Confidential Information to any third person without the prior written consent of Company, except to your authorized employees or agents who have a need to know such information for the purpose of performance under this Agreement and exercising your rights under this Agreement, and who are bound by confidentiality obligations at least as protective of the Confidential Information as this Agreement; and (v) to take such actions as may be reasonably necessary to enforce your agreements with your employees and agents, including commencing legal proceedings.

D. Obligations Upon Termination. Upon expiration or termination of this Agreement, whichever occurs earlier, or upon any request by Company, you will, at your option, either immediately return or destroy, to the extent requested by Company, any Confidential Information (and all portions and copies thereof), in each case as directed by Company, and if requested by Company, certify in writing

as to the destruction or return of such Confidential Information. The obligations set forth in this section shall apply to all Confidential Information during the term of this Agreement and thereafter as follows: (i) for any trade secrets, the obligations shall survive expiration or termination of the Agreement for as long as such information shall remain a trade secret under applicable law; and (ii) for other Confidential Information, the obligations shall continue for seven (7) years after the expiration or termination of this Agreement.

20. 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 to Subscriber by posting the modified Agreement on Company's website; Subscriber's 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. Subscriber may not assign this Agreement or any rights or obligations hereunder without the prior written consent of Company. Subscriber must give notices to the Company through the Company's secure website. The Company may give notices to the Subscriber through the Company's secure website or in the sole discretion of the Company through any other method reasonably calculated and intended to provide actual notice to Subscriber, provided that any notice from Company received by Subscriber or any representative or agent of Subscriber shall be effective, and Subscriber shall be deemed to have received any notice that Company attempts to give using means reasonably calculated and intended to provide actual notice to Subscriber. 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 Subscriber and Company shall be effective through the start date of the term of this Agreement and any confidential information of Company thereunder will continue to be protected as Proprietary Information hereunder.

Exhibit A. The "Software" includes without limitation the following components: (1) The object code, system and/or program shortcuts, configuration files, example code, and installers or any related components; (2) The user interface and user experience, including the methods of creating, processing, sending, receiving, transforming, and exporting secure messages and associated content, and associated graphics, logos, trade names, and icons; (3) The underlying system architecture; (4) The structure of any log files generated; (5) Any Internet email address, domain name, API endpoint, private or public keys or access codes, or digital certificate provided to Subscriber by Company; (6) The concept and implementation of each of the foregoing in the context of the industries in which the Software may be used. These components, and all other parts of the Software, are proprietary to Company. Subscriber agrees to use the Software only as intended by Company.

Trademark Notice: phiMail is a registered trademark and phiCert, phiQuery, and Interoperability Engine are trademarks of EMR Direct.

EMR Direct
858-367-0770
support@emrdirect.com

CONTACT US