Inpriva
Network Services Agreement

This Network Services Agreement (“Agreement”) between Inpriva, Inc., a Colorado corporation ("Inpriva") and the Client identified below ("Client") includes Exhibits A ("Services" or “HIN Services”), B ("Pricing"), C ("Business Associate Agreement") and D (“End-User Agreement) together with all Service Addendum ("Service Addendum") containing Service Orders and any Additional Terms and Conditions mutually agreed upon.

1. **Services:** Inpriva will provide the services, products, software and information, collectively known as "Services" described in the Exhibit A in accordance with the terms noted herein and as amended within any Service Addendum attached hereto.

2. **Prices and Rates:** The price for each Service is set forth in Exhibit B or Service Addendum attached hereto. Client shall pay all sales, use, gross receipts, excise, occupational, access, bypass, franchise and other federal, state and local taxes, assessments, fees, charges, and surcharges, however designated, imposed on or based upon the provision, sale, purchase and/or use of Services.

3. **Payment:** Except when separately set forth in Exhibit B or a Service Addendum, Inpriva shall invoice Client in advance for Services. All invoices are due upon delivery, subject to any additional payment terms set forth in the Service Addendum and become past due thirty (30) days later without demand or set off by Client. If any invoice is not paid to Inpriva within thirty (30) days of delivery, a late charge shall accrue on the delinquent amount at a rate of 1.5% per month, or the maximum rate permitted by law, whichever is less. Any and all dispute claims must be submitted to Inpriva within thirty (30) days of receipt of the applicable invoice. All dispute claims not submitted within said thirty (30) day period are deemed waived. Inpriva shall have the right, at its election and without obligation, in addition to all of its other rights and remedies, to immediately terminate this Agreement and/or suspend Services in the event of any overdue payment in excess of thirty (30) days or any breach or default under of this Agreement.

4. **Term, Renewal and Termination:** The term of this Agreement shall begin on the Effective Date set forth below and shall end upon the later of the completion of twelve (12) months or completion of all the terms for Service. The term for each Service shall be set forth in Exhibit A or a Service Addendum and shall not be less than twelve (12) months unless otherwise stated in the Exhibit A or the Service Addendum. During the term, Client shall pay Inpriva for each Service subject to this Agreement and accompanying Exhibits and Inpriva shall not increase such amounts during that period, but thereafter, Inpriva may increase such amounts upon 30 days prior notice. If Client cancels Service before the term of this Agreement is complete or before Service activation, then Client is responsible for the termination charges equal to the remaining balance of this Agreement. The term for each Service shall automatically renew for successive additional periods ("Extended Term") each equal to the term set forth in Service Addendum or twelve (12) months, if not specified in the Service Addendum unless either party delivers to the other party written notice of termination at least thirty (30) days prior to the end of the term or the Extended Term.

5. **Obligations of Inpriva:** Inpriva shall be responsible for providing Services consistent with industry standards, except as provided in the Exhibit A and Service Addendum. INPRIVA DISCLAIMS ALL OTHER WARRANTIES AND REPRESENTATIONS, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR USE UNLESS SPECIFIED SEPARATELY IN EXHIBITS OR SERVICE ADDENDUM.

6. **Obligations of Client:** Client shall be responsible for the manner in which Service is used, including the maintenance and security of the data retrieved, local computer network security, determination of trusted senders and recipients of Health Information Network (HIN) messages and all other matters related to the use of Service. Client shall ensure that users of the Service maintain the confidentiality of the authentication mechanisms. Client is solely responsible for ensuring that the individuals and systems accessing the Service are authorized to do so. Client shall notify Inpriva immediately if there is any unauthorized use of or any other breach in the security of its Service. Additional Obligations of Client may be specified in Exhibits or Service Addendum.

7. **Warranty:** Inpriva warrants that it owns the HIN Services, including all associated intellectual property rights, or otherwise has the right to grant Client the right and license provided in this Agreement, and that as of the date of this Agreement neither the HIN Services nor any materials supplied by Inpriva to client infringe any valid patents, copyrights, trademarks, or other proprietary rights of any other third parties.

8. **Liability Limitation:** Notwithstanding anything to the contrary contained in this agreement, neither party, nor any of its affiliated persons and entities, will be responsible for consequential, incidental, indirect, exemplary or special damages, including lost profits (even if they have been advised of the possibility or likelihood of such damages).

9. **Other Networks: Access and Cancellation at Inpriva Discretion.** Client agrees to comply with the acceptable use policies, rules and regulations, and terms and conditions of any networks accessed through Inpriva as outlined herein including any Service Addendum. Inpriva reserves the right to deny access to, or terminate Services which, in Inpriva's sole opinion, are causing, or may cause, harm to Inpriva facilities, servers or to other systems. Inpriva will make reasonable efforts to notify Client of any such Inpriva action, but is not bound by this Agreement to do so.

10. **Confidential Information:** Each party shall keep and maintain strictly secret and confidential any and all confidential or proprietary information of the other party and, except as required in connection with the performance of this Agreement or as is required by law and shall not use the same or disclose the same to any third party.

11. **Non-Solicitation:** Client shall not, directly or indirectly, do any of the following: (i) solicit any director, officer, employee, or agent of Inpriva, or encourage any such person to terminate any such relationship with Inpriva, (ii) encourage any Client, supplier or other entity having a business relationship with Inpriva to terminate or alter such relationship, whether contractual or otherwise written or oral, with Inpriva, (iii) encourage any prospective Client or supplier not to enter into a business relationship with Inpriva.

12. **Miscellaneous:** Client may not assign this Agreement or any rights or interests hereunder without the express prior written consent of Inpriva and no said assignment shall relieve Client of its obligations hereunder. This Agreement shall be binding upon and inure to the benefit of the parties and their permitted successors and assigns. This Agreement and any and all related Exhibits and Service Addendums constitute the entire agreement and understanding of the parties and supersede all prior and contemporaneous agreements and understandings between the parties with respect to the subject matter hereof. Any changes to this Agreement, or any additional or different terms in the Client Orders, Service Addendums or any other documents will not be effective unless agreed to in writing by Inpriva. The contractual relationship between Inpriva and Client for each Service shall be governed by the following order of precedence: (i) Service Addendum, (ii) Additional Terms and Conditions, (iii) Exhibits and (iv) Master Services Agreement.

13. **Governing Law:** In the event of a dispute between the Client and Inpriva arising out of this Agreement, the applicable Federal and state conflicts of law provisions that govern the operations of the parties shall determine governing law. Litigation between the Client and Inpriva concerning this Agreement or its subject matter shall be conducted exclusively in state or federal court in the state where the party being sued is located.

14. **Compliance With Laws**: Client shall not use or permit its end users to use Services in any manner that violates any applicable laws or Inpriva use policies, infringes on the rights of others or interferes with users of the Inpriva network or other networks, including, without limitation, distribution of chain letters or unsolicited bulk electronic mail (spamming), knowingly distribute or release computer worms and viruses, use a false identity, attempt to gain unauthorized entry to any site or network, distribute child pornography, obscenity or defamatory material, or infringe patents, copyrights, trademarks or other intellectual property rights.

15. **Rights not Waived:** Failure by either Client or Inpriva to insist upon compliance by the other party with the terms and conditions of this Agreement including any Service Addendum shall not constitute a waiver of any rights under this Agreement.

16. **Partial Invalidity:** If any part, term, or provision of this Agreement is determined to be invalid or unenforceable by a court, board, or tribunal of competent jurisdiction, such term or provision shall be construed in all respects as if such provision were written in a manner acceptable to said court, board, or tribunal, or, if such provision is found to be totally unacceptable to such court, board, or tribunal in any form, then as if such invalid provision were omitted altogether.

Entire Agreement: It is expressly understood that there are no oral agreements or understandings between Client and Inpriva, which will be deemed to extend, restrict, or otherwise supersede the exact terms of this agreement. If any provision of this Agreement including any Service Addendum fails to comply with applicable law, then this Agreement shall, without prior notice, be automatically modified to conform with the minimum requirements of any law or governmental regulation having application to or jurisdiction over the subject matter or the parties hereto.

EXHIBIT A

Health Information Network Services

This Exhibit provides an overview of the Health Information Network Services ("HIN Services") that may be provided by Inpriva, the respective responsibilities of Inpriva and Client, and additional terms and conditions that apply to the Health Information Network Services.

IDENTITY SERVICES

Inpriva is both an EHNAC/DirectTrust Accredited Certificate Authority and Accredited Registration Authority. Inpriva closely follows the policies and procedures required by the DirectTrust Certificate Policy and Health Information Service Provider (HISP) Policy.

Direct Domain Certificates (aka Organizational Certs)

1. Description.
   - A Direct Organizational Certificate is a digital means of authenticating a subscriber. Direct Organizational Certificates cover the subdomains of the healthcare organization (must be a distinct legal entity with a valid healthcare purpose) and all of the addresses associated with it. Direct Org certs are issued by an accredited EHNAC/DirectTrust Certification Authority, in accordance with its published Certification Practice Statement (CPS).

2. Inpriva Responsibilities
   - Enforce the specific identity verification and other policies/procedures specified in the applicable Certification Policy and its associated CPS.
   - Provide access to an Enrollment Portal to facilitate Client registration
   - The RA shall verify the organization information submitted, in addition to the authenticity of the requesting representative and the representative's authorization to act in the name of the organization.

3. Client Responsibilities
   - Requests for organizational certificates must include the organization name, mailing address and documentation of the existence of the organization as well as the requested domain name that will appear in the certificate.
   - Client must provide documentation that the requesting organization is a HIPAA covered entity or business associate, or is a healthcare related organization which treats protected health information with privacy and security protections that are equivalent to those required by HIPAA. The requesting organization must be a distinct legal entity.
   - An authorized Client or owner of the organization must appoint the Direct Authorized Representative. This will require execution of an Affidavit with a notarized signature or verifiable digital signature. This Authorized Representative will be responsible for interacting with Inpriva in management of the organization's Direct account. The Authorized Representative must have their identity verified at the requested Level of Assurance (as defined in the applicable Certification Policy).
   - Client must agree to the terms and conditions of the Direct Subscriber Agreement or Direct Organizational Certificate Agreement.

4. License Terms and Conditions

   In the event the Agreement is terminated before the expiration of the Identity Services license, the rights of this license will survive the term of the overall Agreement. Additional terms and conditions:

   - The term of the certificate is granted for a period as specified within the individual certificate
   - Are issued in accordance with the policies of the designated Certification Policy and its associated Certification Practice Statement.
   - The license is subject to the terms and conditions of the Direct Organization Certificate End-User Agreement.

Administrative Representative Credentials

1. Description
   - Administrative Representative credentials are provided to Inpriva Registration Authority (RA's) for authentication and authorization of Direct Authorized Representatives or Direct Domain Administrators. The RA will verify this identity information as required by the applicable Certificate Policy and in accordance with the associated RPS and CPS and upon verification the CA will issue the requested certificate.
2. Inpriva Responsibilities
   - The RA shall verify an individual's identity in accordance with the process established that meets the requirements of the requested Level of Assurance.
   - Provide access to an Enrollment Portal to facilitate Identity verification.

3. Client Responsibilities
    - Requests for Direct Authorized Representative or Administrator Credentials must include the user's name, mailing address, birthdate and additional information as required for the requested Level of Assurance (LOA). In addition, verification of the authorization of the sponsoring organization.
    - Applicant must agree to the terms and conditions of the Direct End User Agreement

4. License Terms and Conditions

    In the event the Agreement is terminated before the expiration of the Direct Authorized Representative/Administrator Credential license, the rights of this license will survive the term of the overall Agreement. Additional terms and conditions:

- The term of the credential is granted for a period as specified within the individual Credential
- Are issued in accordance with the policies of the designated Certification Policy and its associated Certification Practice Statement.
- The license is subject to the terms and conditions of the Direct Subscriber Agreement or Direct Authorized Representative/Administrator Credentials End User Agreement.

DIRECT MAIL SERVICES

Direct Mailboxes

1. Description

    hDirectMail is a Direct Project-compliant secure email service that enables healthcare organizations and individual to securely send and receive patient healthcare information electronically and meet Meaningful Use requirements.

2 Inpriva Responsibilities.

Inpriva will provision addresses with client-provided names and provide Direct secure messaging service that are compliant with the specifications of the Direct Project.

3 Client Responsibilities.

Client must provide Inpriva with the user names for which the addresses will be provisioned and meet the terms and conditions of the Exhibit D End-User Agreement.

4 License Terms and Conditions

Rights for use of Inpriva Mail Services will be granted for 12 months from date of activation. This license is for individual use and not intended for use with an automated system. In the event the Agreement is terminated before the expiration of mail service, the rights of this license will survive the term of the overall Agreement.

Extended Usage

1. Description

    Extended usage refers to charges relating to the number of transactions or volume of data transferred over the amount of the original product contract.

EXHIBIT B

PRICING

See Service Addendum(s).

EXHIBIT C

BUSINESS ASSOCIATE AGREEMENT

A. Pursuant to the terms of a Master Services Agreement and associated Service Addendums, Inpriva, Inc., ("Business Associate"), provides services for Covered Entity (the "Service Arrangement") pursuant to which Covered Entity will disclose Protected Health Information ("PHI") to Business Associate in order to enable Business Associate to perform one or more functions for Covered Entity related to Treatment, Payment or Health Care Operations, and

B. Covered Entity and Inpriva desire to comply with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") and the Final Rule for Standards for Privacy of Individually Identifiable Health Information adopted by the United States Department of Health and Human Services and codified at 45 C.F.R. part 160 and part 164, subparts A & E (the "Privacy Rule"), the HIPAA Security Rule, codified at 45 C.F.R. Part 164 Subpart C (the "Security Rule") and Subtitle D of the Health Information Technology for Economic and Clinical Health Act ("HITECH") including 45 C.F.R. Sections 164.308, 164.310, 164.312 and 164.316.

The parties to this Agreement hereby agree as follows:

1. Definitions. Terms used, but not otherwise defined, in this Agreement shall have the same meaning as those terms in 45 C.F.R. §§ 160.103, 164.103, and 164.304, 164.501 and 164.502.

2. Obligations and Activities of Business Associate.

a. Business Associate agrees to not use or further disclose PHI other than as permitted or required by this Agreement, as required by Law or as permitted by law, provided such use or disclosure would also be permissible by law by Covered Entity.

b. Business Associate agrees to use appropriate safeguards to prevent use or disclosure of the PHI other than as provided for by this Agreement. Business Associate agrees to implement Administrative Safeguards, Physical Safeguards and Technical Safeguards ("Safeguards") that reasonably and appropriately protect the confidentiality, integrity and availability of PHI as required by the "Security Rule".

c. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement, or of any Security Incident of which it becomes aware.

d. Business Associate agrees to report to Covered Entity any use or disclosure for the PHI not provided for by this Agreement.

e. Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides PHI; received from, created by, or received by a Business Associate on behalf of Covered Entity, agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

f. Business Associate agrees to provide access, at the request of Covered Entity and in the time and manner designated by Covered Entity, to PHI in a Designated Record Set, to Covered Entity or, as directed by Covered Entity, to an Individual in order to meet the requirements under 45 C.F.R. § 164.524.

g. Business Associate agrees to make any amendment(s) to PHI in a Designated Record Set that Covered Entity directs or agrees to pursuant to 45 C.F.R. §164.526 at the request of Covered Entity or an Individual, and in the time and manner designated by Covered Entity.

h. Business Associate agrees to make internal practices, books, and records relating to the use and disclosure of PHI received from, created by, or received by a Business Associate on behalf of Covered Entity available to Covered Entity, or at the request of Covered Entity to the Secretary of HHS, in a time and manner designated by Covered Entity or the Secretary, for the purposes of the Secretary determining Covered Entity's compliance with the Privacy Rule and Security Rule.

i. Business Associate agrees to document such disclosures of PHI and information related to such disclosures as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. §164.528.

j. Business Associate agrees to provide to Covered Entity or an Individual, in a time and manner designated by Covered Entity, information collected in accordance with this Agreement, to permit Covered Entity to respond to a request by an individual for an accounting of disclosures for PHI in accordance with 45 §C.F.R. 164.528.

k. If Business Associate accesses, maintains, retains, modifies, records, stores, destroys, or otherwise holds, uses, or discloses Unsecured Protected Health Information (as defined in HITECH), it shall, following the discovery of a breach of such information, promptly notify Covered Entity of such breach. Such notice shall include: a) the identification of each individual whose Unsecured Protected Health Information has been, or is reasonably believed by Business Associate to have been accessed, acquired or disclosed during such breach; b) a brief description of what happened, including the date of the breach and discovery of the breach; c) a description of the type of Unsecured PHI that was involved in the breach; d) a description of the investigation into the breach, mitigation of harm to the individuals and protection against further breaches; e) the results of any and all investigation performed by Business Associate related to the breach; and f) contact information of the most knowledgeable individual for Covered Entity to contact relating to the breach and its investigation into the breach.

3. Permitted Uses and Disclosures by Business Associate.

   a. Except as otherwise limited to this Agreement, Business Associate may use or disclose PHI to perform functions, activities, or services for, or on behalf of, Covered Entity as specified in the Service Arrangement, provided that such use or disclosure would not violate the Privacy Rule if done by Covered Entity or the minimum necessary policies and procedures of Covered Entity required by 45 C.F.R. §164.514(d).

   b. Except as otherwise limited in this Agreement, Business Associate may use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

   c. Except as otherwise limited in this Agreement, Business Associate may disclose PHI for the proper management and administration of the Business Associate, provided that disclosures are Required By Law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as Required By Law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

   d. Except as otherwise limited in this Agreement, Business Associate may use PHI to provide Data Aggregation services to Covered Entity as permitted by 45 C.F.R. §164.504 (e)(2)(i)(B).

   e. Business Associate may use PHI to report violations of law to appropriate Federal and State authorities, consistent with 45 C.F.R. §164.502(j) (1).

4. Obligations of Covered Entity

   a. Covered Entity shall notify Business Associate of any limitation(s) in its notice of privacy practices of Covered Entity in accordance with 45 C.F.R. § 164.520, to the extent that such limitation may affect Business Associate's use or disclosure of PHI.

   b. Covered Entity shall notify Business Associate of any changes in, or revocation of, permission by an Individual to use or disclose PHI to the extent that such changes may affect Business Associate's use or disclosure of PHI.

   c. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI that Covered Entity has agreed to in accordance with 45 C.F.R. §164.522, to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

5. Permissible Requests by Covered Entity

   Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the Privacy Rule if done by Covered Entity, provided that, to the extent permitted by the Service Arrangement, Business Associate may use or disclose PHI for Business Associate's Data Aggregation activities or proper management and administrative activities.

6. Term and Termination.

   a. The term of this Agreement shall begin as of the effective date of the Service Arrangement and shall terminate when all of the PHI provided by Covered Entity to Business Associate, or created or received by Business Associate on behalf of Covered Entity, is destroyed or returned to Covered Entity, or, if it is infeasible to return or destroy PHI, protections are extended to such information, in accordance with the termination provisions of this Section.

   b. Upon Covered Entity's knowledge of a material breach by Business Associate, Covered Entity shall either:

      i. Provide an opportunity for Business Associate to cure the breach or end the violation and terminate this Agreement and the Service Arrangement if Business Associate does not cure the breach or end the violation within the time specified by Covered Entity.

      ii. Immediately terminate this Agreement and the Service arrangement if Business Associate has breached a material term of this Agreement and cure is not possible; or

      iii. If neither termination nor cure is feasible, Covered Entity shall report the violation to the Secretary.

   c. Except as provided in paragraph (d) of this Section, upon any termination or expiration of this Agreement, Business Associate shall return or destroy all PHI received from Covered Entity, or created or received by Business Associate on behalf of Covered Entity. This provision shall apply to PHI that is in the possession of subcontractors or agents of Business Associate. Business Associate shall retain no copies of the PHI.

d. In the event that Business Associate determines that returning or destroying the PHI is infeasible, Business Associate shall provide to Covered Entity notification of the conditions that make return or destruction infeasible. Upon Covered Entity's written agreement that return or destruction of PHI is infeasible, Business Associate shall extend the protections of this Agreement to such PHI and limit further uses and disclosures of such PHI to those purposes that make the return or destruction infeasible, for so long as Business Associate maintains such PHI.

7. Miscellaneous.

a. A reference in this Agreement to a section in the Privacy Rule or Security Rule means the section as in effect or as amended.

b. The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Covered Entity to comply with the requirements of HIPAA, the Privacy and Security Rules and HITECH.

c. The respective rights and obligations of Business Associate under Section 6 (c) and (d) of this Agreement shall survive the termination of this Agreement.

d. Any ambiguity in this Agreement shall be resolved to permit Covered Entity to comply with HIPAA and HITECH.

e. Business Associate is solely responsible for all decisions made by Business Associate regarding the safeguarding of PHI.

f. Nothing express or implied in this Agreement is intended to confer, nor shall anything herein confer upon any person other than Covered Entity, Business Associate and their respective successors and assigns, any rights, remedies, obligations or liabilities whatsoever.

g. Modification of the terms of this Agreement shall not be effective or binding upon the parties unless and until such modification is committed to writing and executed by the parties hereto.

h. This Agreement shall be binding upon the parties hereto, and their respective legal representatives, trustees, receivers, successors and permitted assigns.

i. Should any provision of this Agreement be found unenforceable, it shall be deemed severable and the balance of the Agreement shall continue in full force and effect as if the unenforceable provision had never been made a part hereof.

j. This Agreement and the rights and obligations of the parties hereunder shall in all respects be governed by, and construed in accordance with, the laws of the State of Colorado, including all matters of constructions, validity and performance.

k. All notices and communications required or permitted to be given hereunder shall be sent by certified or regular mail, addressed to the other part as its respective address as shown on the signature page, or at such other address as such party shall from time to time designate in writing to the other party, and shall be effective from the date of mailing.

l. This Agreement, including such portions as are incorporated by reference herein, constitutes the entire agreement by, between and among the parties, and such parties acknowledge by their signature hereto that they do not rely upon any representations or undertakings by any person or party, past or future, not expressly set forth in writing herein.

EXHIBIT D

End-User License Agreement

I. RESPONSIBILITIES OF END-USER

1. This End-User License Agreement (“End User Agreement”) applies to any means through which an End-User orders or accesses the HIN Services including, without limitation, system-to-system, personal computer or the Internet.
2. For the purposes of this End User Agreement, the term "Authorized User" means a Client employee or other affiliated person that has had their identity properly verified and whom the Client has authorized to order or access the HIN Services and who is trained on Client's obligations under this End-User License Agreement with respect to the ordering and use of the HIN Services and Inpriva Information.
3. Each Direct Address has a healthcare or healthcare-associated organization, person or device bound to it as reflected in an associated Direct Digital Certificate. This License, which grants access to the HIN Services is expressly conditioned upon compliance by the End-User with the terms and conditions of the Direct Digital Certificates, including those related terms and conditions specified in the DirectTrust Certificate Policy, those specified in the DirectTrust HISP Policy, and those related to management of the HIN Services.
4. Client shall ensure that only Authorized Users can order or have access to the HIN Services.
5. Client shall take all necessary measures to prevent unauthorized ordering of or access to the HIN Services by any person other than an Authorized User for permissible purposes, including, without limitation, limiting the knowledge of the Client security codes, member numbers, User IDs, and any passwords Client may use (collectively, "Security Information"), to those individuals with a need to know.
6. Client shall monitor compliance with the obligations of this End-User Agreement, and immediately notify Inpriva if Client suspects or knows of any unauthorized access or attempt to access the HIN Services.
7. If Client uses a Service Provider to establish access to the HIN Services, Client shall be responsible for the Service Provider's use of Security Information, and ensure the Service Provider safeguards such Security Information through the use of security requirements that are no less stringent than those applicable to Client under this End-User Agreement,
8. Client shall use commercially reasonable efforts to assure data security when disposing of any individually identified personal information obtained from Inpriva. Such efforts must include the use of those procedures issued by the federal regulatory agency charged with oversight of Client's activities (e.g. the Office of Civil Rights) applicable to the handling of such information or records.
9. Client shall use commercially reasonable efforts to secure Inpriva Information when stored on servers.
10. Client is responsible for ensuring that Users are properly qualified to use the HIN Services and use them for appropriate purposes. It is the Client's responsibility to review the access auditing reports for individual Users if that is deemed by Client to be important for their HIPAA compliance.
11. Client is responsible for establishing a trust policy to be used by the HIN Services to determine which recipients Users can send messages to and which senders the User can receive messages from. Client is responsible for the completion of registration forms and agreements required for enrollment to use the HIN Services, including those establishing the identity of the Client and the Client's Representative.
12. Client agrees to accurately complete its registration information as part of the registration process and maintain the accuracy of the information in an "Identity Registry" provided by Inpriva. Client agrees to have this registration information checked for consistency with other information sources by Inpriva and understand that inconsistencies may result in termination of HIN Services unless and until corrected by the Client. Client agrees to require that its Users maintain the accuracy of the information contained in the Identity Registry.
13. Client acknowledges that information provided by the Client and its Users may be included in Provider/Direct directories accessible to other organizations or persons having Direct addresses, unless the Client notifies Inpriva otherwise.
14. Client agrees to comply fully with all requirements (including but not limited to requirements regarding individuals receiving access to the HIN Services, and requirements regarding identity proofing of those individuals) that are set forth on these web pages relating to registration, enrollment and management of the HIN Services and for the HIN Services generally. The Participant further understands that such requirements may be updated by Inpriva from time to time in its sole discretion, and that it is the responsibility of the Client to review the requirements on an ongoing basis and to ensure the Client's continued compliance with those requirements.
15. If Inpriva reasonably believes that Client has violated this End-User Agreement, Inpriva may, in addition to any other remedy authorized by this End-User Agreement, with reasonable advance written notice to Client, conduct, or have a third party conduct on its behalf, an audit of Client's network security systems, facilities, practices and procedures to the extent Inpriva reasonably deems necessary, including an on-site inspection, to evaluate Client's compliance with the data security requirements of this End-User Agreement.