SPAM STOPS HERE®

SpamStopsHere
HIPAA Compliance Addendum

In order to comply with the federal Standards for Privacy of Individually Identifiable Health Information, located at 45 C.F.R. parts 160 and 164 ("HIPAA" or the "Privacy Rule"), the following terms are incorporated into the general Confidentiality Agreement:

Whereas Client is a “Covered Entity” under HIPAA and SpamStopsHere (SSH) is a “Business Associate” providing “spam filtering” email services to Client,

Whereas the Privacy Rule requires that covered entities receive adequate assurances from Business Associates that they will comply with certain obligations with respect to Protected Health Information (“PHI”) (individually identifiable health information transmitted in any form) subject to protection under the Privacy Rule, and

Whereas the purpose of this Agreement is to comply with the requirements of the Privacy Rule,

A. Purposes for which PHI May Be Disclosed to SSH. In connection with the services provided by SSH, Client will not be providing PHI to SSH, other than that which may flow through SSH’s servers as part of email messages. SSH is not providing any services relating to medical care, billing, or other services in which record sets or PHI are used as an integral part of SSH’s services, and SSH will not be maintaining any Designated Record Sets.

B. Obligations of Client. If deemed applicable by Client, Client shall:

1. provide SSH a copy of its Notice of Privacy Practices ("Notice") produced by Client in accordance with 45 C.F.R. 164.520 as well as any changes to such notice;
2. provide SSH with any changes in, or revocation of, authorizations by Individuals relating to the use and/or disclosure of PHI, if such changes affect SSH's permitted or required uses and/or disclosures;
3. notify SSH of any restriction to the use and/or disclosure of PHI to which Client has agreed in accordance with 45 C.F.R. 164.522;

C. Obligations of SSH. SSH agrees to comply with applicable federal and state confidentiality and security laws, specifically the provisions of the Privacy Rule applicable to Business Associates (as defined by the Privacy Rule), including:

1. Use and Disclosure of PHI. Except as otherwise permitted by this Agreement or applicable law, SSH shall not use or disclose PHI except as necessary, in its sole discretion, to provide spam filtering and related email services, and shall not use or disclose PHI that would violate the Privacy Rule if used or disclosed by Client. Provided, however, SSH may use and disclose PHI as necessary for the proper management and administration of SSH and to carry out its spam filtering operations on Client’s behalf. SSH shall in such cases:

    (a) provide information to members of its workforce using or disclosing PHI regarding the confidentiality requirements of the Privacy Rule and this Agreement;

(b) obtain reasonable assurances from the person or entity to whom the PHI is disclosed that: (a) the PHI will be held confidential and further used and disclosed only as Required by Law or for the purpose for which it was disclosed to the person or entity; and (b) the person or entity will notify SSH of any instances of which it is aware in which confidentiality of the PHI has been breached; and

(c) agree to notify the designated Privacy Officer of Client of any instances of which it is aware in which the PHI is used or disclosed for a purpose that is not otherwise provided for in this Agreement or for a purpose not expressly permitted by the Privacy Rule.

2. De-identified Information. SSH may use and disclose de-identified health information, if (i) the use is disclosed to Client and permitted by Client in its sole discretion and (ii) the de-identification is in compliance with 45 C.F.R. §164.502(d), and the de-identified health information meets the standard and implementation specifications for de-identification under 45 C.F.R. §164.514(a) and (b).
3. Safeguards. SSH shall maintain appropriate safeguards to ensure that PHI is not used or disclosed other than as provided by this Agreement or as required by Law.
4. Minimum Necessary. SSH shall attempt to ensure that uses and disclosures of PHI are subject to the principle of "minimum necessary use and disclosure," i.e., that only PHI that is the minimum necessary to accomplish the intended purpose of the use, disclosure, or request is used or disclosed.
5. Disclosure to Agents and Subcontractors. If SSH discloses PHI received from Client, or created or received by SSH on behalf of Client, to agents, consultants, or subcontractors, SSH shall require such persons to agree to the same restrictions and conditions as apply to SSH under this Agreement.
6. Individual Rights Regarding Designated Record Sets. It is not anticipated that SSH will maintain any records subject to an Individual's right to access and copy records, make corrections to records, etc. In the event that this changes, the parties agree to modify this agreement to deal with procedures for a amendment to records, etc., as required by HIPAA. In the event that any PHI is disclosed to any party, SSH agrees to maintain documentation of the information required to provide an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.538, and to make this information available to Client upon Client's request, in order to allow Client to respond to an Individual's request for accounting of disclosures.
7. Internal Practices and Policies and Procedures. Except as otherwise specified herein, SSH shall make available its internal practices and policies and procedures relating to the use and disclosure of PHI received from or on behalf of Client to the Secretary or his or her agents for the purpose of determining Client's compliance with the Privacy Rule. Records requested that are not protected by an applicable legal privilege will be made available in the time and manner specified by Client or the Secretary. If it is necessary for SSH to invoke and defend the attorney-client privilege, Client shall agree to pay the cost for such defense.
8. Notice of Privacy Practices. If Client's Notice of Privacy Practices ("Notice") specifically affects SSH's use or disclosure of PHI, Client shall inform SSH of the specific limitations. SSH shall abide by the limitations of Client's Notice that affect its use or disclosure of PHI of which it has been specifically informed. Any use or disclosure permitted by this Agreement may be amended by changes to Client's Notice if Client specifically informs SSH of the amendment; provided, however, that the amended Notice shall not affect permitted uses and disclosures on which SSH relied prior to receiving notice of such amended Notice.

D. Term and Termination.

1. Term. This Agreement shall be effective as of the Effective Date and shall be terminated when all PHI provided to SSH by Client, or created or received by SSH on behalf of Client, has been destroyed or returned to Client.
2. Termination for Breach. If Client determines that SSH has breached the requirements of this Agreement, it may terminate this Agreement on a date specified by Client.
3. Effect of Termination. Upon termination of this Agreement for any reason, SSH agrees to return or destroy all PHI received from Client, or created or received by SSH on behalf of Client, maintained by SSH in any form. If SSH determines that the return or destruction of PHI is not feasible, SSH shall inform Client in writing of the reason thereof, and shall agree to extend the protections of this Agreement to such PHI and limit further uses and disclosures of the PHI to those purposes that make the return or destruction of the PHI not feasible for as long as SSH retains the PHI.

E. Miscellaneous.

1. No Third Party Beneficiaries. Nothing in this Agreement shall be considered or construed as conferring any right or benefit on a person not party to this Agreement nor imposing any obligations on either Party hereto to persons not a party to this Agreement.
2. Mitigation. If SSH violates this Agreement or the Privacy Rule, SSH agrees to attempt to mitigate any damage caused by such breach.
3. Notices. Any notices pertaining to this Agreement shall be given in writing and shall be deemed duly given when personally delivered to a Party or a Party's authorized representative as listed below or sent by means of a reputable overnight carrier, or sent by means of certified mail, return receipt requested, postage prepaid. A notice sent by certified mail shall be deemed given on the date of receipt or refusal of receipt.