Addendum to the Spirion Software as a Service Agreement

Spirion HIPAA Business Associate Addendum

This HIPAA Business Associate Addendum ("**BAA**") is incorporated into and made part of the Spirion Software as a Service Agreement ("**SaaS Agreement**") and governs the Processing of Personal Data by Spirion as a Processor on behalf of Customer or Customer Affiliates, as applicable. Unless otherwise defined in this BAA, capitalized terms will have the meaning given to them in the Agreement.

Customer must have an existing SaaS Agreement in place for this BAA to be valid and effective. Together with the SaaS Agreement, this BAA will govern each party's respective obligations regarding Protected Health Information (defined below).

1. **Definitions.** Any capitalized terms used but not otherwise defined in this BAA will have the meaning given to them in HIPAA and the HITECH Act.

"Business Associate" has the definition given to it under HIPAA.

"Breach" has the definition given to it under HIPAA. A Breach will not include an acquisition, access, use, or disclosure of PHI with respect to which Spirion has determined in accordance with 45 C.F.R. § 164.402 that there is a low probability that the PHI has been compromised.

"Covered Entity" has the definition given to it under HIPAA.

"HIPAA" means the Health Insurance Portability and Accountability Act of 1996 and the rules and the regulations thereunder, as amended.

"HITECH Act" means the Health Information Technology for Economic and Clinical Health Act enacted in the United States Congress, which is Title XIII of the American Recovery & Reinvestment Act, and the regulations thereunder, as amended.

"Protected Health Information" or "PHI" has the definition given to it under HIPAA and for purposes of this BAA is limited to PHI within Customer Data to which Spirion has access through the Services in connection with Customer's permitted use of Services.

"Security Breach" means any Breach of Unsecured PHI or Security Incident of which Spirion becomes aware.

"Security Incident" has the definition given to it under HIPAA.

"Service Agreement(s)" means the written agreement(s) entered into between Spirion and Customer for provision of the Services; such agreement(s) may be in the form of an online terms of service.

2. **Applicability.** This BAA applies to the extent Customer is acting as a Covered Entity or a Business Associate to create, receive, maintain, or transmit PHI via the Services and to the extent Spirion, as a result, is deemed under HIPAA to be acting as a Business Associate or Subcontractor of Customer. Customer acknowledges that this BAA does not apply to, or govern, any other Spirion product, service, or feature that is not a Service.

3. **Use and Disclosure of PHI.**

(a) Except as otherwise stated in this BAA, Spirion may use and disclose PHI only as permitted or required by the SaaS Agreement(s) and/or this BAA or as Required by Law.

(b) Spirion may use and disclose PHI for the proper management and administration of Spirion's business and to carry out the legal responsibilities of Spirion, provided that any disclosure of PHI for such purposes may only occur if: (1) required by applicable law; or (2) Spirion obtains written reasonable assurances from the person to whom PHI will be disclosed that it will be held in confidence, used only for the purpose for which it was disclosed, and that Spirion will be notified of any Security Breach.

(c) Spirion may also use PHI to create de-identified information in a manner consistent with the standards stated in HIPAA, and may use or disclose such de-identified PHI for any purpose in accordance with HIPAA.

(d) Spirion has no obligations under this BAA with respect to any PHI that Customer creates, receives, maintains, or transmits outside of the Services (including Customer's use of its offline or on-premise storage tools or third-party applications) and this BAA will not apply to any PHI created, received, maintained or transmitted outside of the Services.

4. **Customer Obligations.**

(a) Customer may only use the Services to create, receive, maintain, or transmit PHI. Customer is solely responsible for managing whether Customer's end users are authorized to share, disclose, create, and/or use PHI within the Services.

(b) Customer will not request that Spirion or the Services use or disclose PHI in any manner that would not be permissible under HIPAA if done by Customer (if Customer is a Covered Entity) or by the Covered Entity to which Customer is a Business Associate (unless expressly permitted under HIPAA for a Business Associate).

(c) Customer will use controls available within the Services to ensure its use of PHI is limited to the Services. Customer acknowledges and agrees that it is solely responsible for ensuring that its use of the Services complies with HIPAA and HITECH.

(d) Customer will take appropriate measures to limit its use of PHI to the Services and will limit its use within the Services to the minimum extent necessary for Customer to carry out its authorized use of such PHI.

(e) Customer warrants that it has obtained and will obtain any consents, authorizations and/or other legal permissions required under HIPAA and/or other applicable law for the disclosure of PHI to Spirion. Customer will notify Spirion of any changes in, or revocation of, the permission by an Individual to use or disclose his or her PHI, to the extent that such changes may affect Spirion's use or disclosure of PHI. Customer will not agree to any restriction on the use or disclosure of PHI under 45 CFR § 164.522 that restricts Spirion's use or disclosure of PHI under the Agreement unless such restriction is required by law.

5. **Appropriate Safeguards.** Spirion and Customer will each use appropriate safeguards designed to prevent against unauthorized use or disclosure of PHI, and as otherwise required under HIPAA, with respect to the Services.

6. **Reporting.**

(a) Subject to Section 6(d), Spirion will promptly notify Customer following Spirion's Discovery of a Security Breach in accordance with HIPAA and in the most expedient time possible under the circumstances, consistent with the legitimate needs of applicable law enforcement and applicable laws, and after taking any measures Spirion deems necessary to determine the scope of the Security Breach and to restore the reasonable integrity of Spirion's systems.

(b) To the extent practicable, Spirion will use commercially reasonable efforts to mitigate any further harmful effects of a Security Breach caused by Spirion.

(c) Spirion will send any applicable Security Breach notifications to the notification email address provided by Customer in the SaaS Agreement or via direct communication with the Customer.

(d) Notwithstanding Section 6(a), this Section 6(d) will be deemed as notice to Customer that Spirion periodically receives unsuccessful attempts for unauthorized access, use, disclosure, modification or destruction of information, or interference with the general operation of Spirion's information systems and the Services. Customer acknowledges and agrees that even if such events constitute a Security Incident as that term is defined under HIPAA, Spirion will not be required to provide any notice under this BAA regarding such unsuccessful attempts other than this Section 6(d).

7. **Subcontractors.** Spirion will take appropriate measures to ensure that any Subcontractors used by Spirion to perform its obligations under the SaaS Agreement that require access to PHI on behalf of Spirion are bound by written obligations that provide the same material level of protection for PHI as this BAA. To the extent Spirion uses Subcontractors in its performance of obligations hereunder, Spirion will remain responsible for their performance as if performed by Spirion.

8. **Access and Amendment.** Customer acknowledges and agrees that Customer is solely responsible for the form and content of PHI maintained by Customer within the Services, including whether Customer maintains such PHI in a Designated Record Set within the Services. Spirion will provide Customer with access to Customer's PHI via the Services so that Customer may fulfill its obligations under HIPAA with respect to Individuals' rights of access and amendment, but will have no other obligations to Customer or any Individual with respect to the rights afforded to Individuals by HIPAA with respect to Designated Record Sets, including rights of access or amendment of PHI. Customer is responsible for managing its use of the Services to appropriately respond to such Individual requests.

9. **Accounting of Disclosures.** Spirion will document disclosures of PHI by Spirion and provide an accounting of such disclosures to Customer as and to the extent required of a Business Associate under HIPAA and in accordance with the requirements applicable to a Business Associate under HIPAA.

10. **Access to Records.** To the extent required by law, and subject to applicable attorney-client privilege, Spirion will make its internal practices, books, and records concerning the use and

disclosure of PHI received from Customer, or created or received by Spirion on behalf of Customer, available to the Secretary of the U.S. Department of Health and Human Services (the "Secretary") for the purpose of the Secretary determining compliance with this BAA.

11. **Expiration and Termination.**

(a) This BAA will terminate on the earlier of (i) a permitted termination in accordance with Section 11(b) below, or (ii) the expiration or termination of all SaaS Agreements under which Customer has access to a Service.

(b) If either party materially breaches this BAA, the non-breaching party may terminate this BAA on 10 days' written notice to the breaching party unless the breach is cured within the 10-day period. If a cure under this Section 11(b) is not reasonably possible, the non-breaching party may immediately terminate this BAA, or if neither termination nor cure is reasonably possible under this Section 11(b), the non-breaching party may report the violation to the Secretary, subject to all applicable legal privileges.

(c) If this BAA is terminated earlier than the SaaS Agreement, Customer may continue to use the Services in accordance with the SaaS Agreement, but must delete any PHI it maintains in the Services and cease to further create, receive, maintain, or transmit such PHI to Spirion.

12. **Return/Destruction of Information.** On termination of the SaaS Agreement, Spirion will return or destroy all PHI received from Customer, or created or received by Spirion on behalf of Customer; provided, however, that if such return or destruction is not feasible, Spirion will extend the protections of this BAA to the PHI not returned or destroyed and limit further uses and disclosures to those purposes that make the return or destruction of the PHI infeasible.

13. **Miscellaneous.**

(a) Survival. Section 12 (Return/Destruction of Information) will survive termination or expiration of this BAA.

(b) Counterparts. The parties may execute this BAA in counterparts, including facsimile, PDF or other electronic copies, which taken together will constitute one instrument.

Effects of Addendum. To the extent this BAA conflicts with the remainder of the SaaS Agreement(s), this BAA will govern. This BAA is subject to the "Choice of Law" section in the SaaS Agreement(s). Except as expressly modified or amended under this BAA, the terms of the SaaS Agreement(s) remain in full force and effect.