

# Business Associate Addendum



This Business Associate Addendum (“Addendum”) supplements and is made a part of the Base Agreement identified in the signature block, and applicable transaction document(s), between Client and International Business Machines Corporation (IBM) for the services that will be processing protected health information of individuals governed by U.S. laws and regulations (collectively, the “Agreement”). IBM and Client may be referred to individually as a “Party” or collectively as the “Parties.” Once accepted electronically, any reproduction made by reliable means (for example, electronic image, photocopy or facsimile) is considered an original.

## RECITALS

Client is a “covered entity”, as such term is defined by HIPAA (defined below).

Client and IBM are Parties to the Agreement pursuant to which IBM provides certain services to Client. In connection with those services, the Parties anticipate that it may be necessary for IBM to create, receive, maintain, transmit, use, or disclose certain Protected Health Information from, or on behalf of, Client (“Client PHI”) that is subject to protection under the privacy, security and breach notification requirements of the Health Insurance Portability and Accountability Act of 1996, as amended, including by the Health Information Technology for Economic & Clinical Health Act of the American Recovery and Reinvestment Act of 2009 (“HITECH Act”), certain regulations promulgated under HIPAA by the United States Department of Health and Human Services at 45 C.F.R. Parts 160 and 164 and certain regulations promulgated pursuant to the HITECH Act (collectively, “HIPAA”).

The purpose of this Addendum is to help facilitate the Parties’ compliance with the requirements of HIPAA, as applicable when IBM is acting as a business associate of Client.

Client acknowledges that IBM may act in a capacity other than as a business associate and that this Addendum only applies to the extent that IBM is acting as a business associate for Client. Hereinafter, however, IBM will be referred to as “Business Associate.”

NOW, THEREFORE, in consideration of the mutual promises and other consideration contained in this Addendum, the delivery and sufficiency of which is hereby acknowledged, the Parties agree as follows:

## AGREEMENT

**1. Definitions.** Unless otherwise provided in this Addendum, capitalized terms have the same meaning as set forth in HIPAA. “Applicable Law” means, in respect of any person, all provisions of constitutions, statutes, rules, regulations, and orders of governmental bodies or regulatory agencies applicable to such person, including, without limitation, HIPAA and state privacy laws and security breach notification laws, and all orders and decrees of all courts and arbitrators in proceedings or actions to which the person in question is a party or by which it or its properties are bound.

**2. Applicability.** This Addendum shall be applicable solely to Protected Health Information that is Client PHI. Client will not provide Business Associate with access to, or direct Business Associate to create, receive, maintain, transmit, use, or disclose, Client PHI unless a description of the Client PHI, its location and any requirements related to such Client PHI are mutually agreed upon in the applicable transaction document.

**3. Minimum Necessary Disclosures.** In accordance with HIPAA, Client shall limit its uses, disclosures and requests of Client PHI to Business Associate to the minimum necessary to accomplish the services Business Associate is performing for Client. Business Associate shall further limit its use, disclosures and requests of Client PHI to the minimum necessary Client PHI to perform or have performed the services Business Associate is performing for Client. In each case, Client shall exercise reasonable discretion to determine what constitutes minimum necessary Client PHI.

**4. Scope of Use of Client PHI.** Business Associate shall not create, receive, maintain, transmit, use, or disclose Client PHI for any purpose other than as permitted or required by this Addendum or as Required By Law; provided that to the extent Business Associate is to carry out Client’s obligations under the Privacy Rule as agreed by the Parties in writing, Business Associate will comply with the requirements of the Privacy Rule that apply to Client in the performance of those obligations.

**5. Permitted Uses and Disclosures.** Unless otherwise limited in this Addendum, in addition to any other uses and/or disclosures permitted or required by this Addendum, Business Associate may:

5.1 create, receive, maintain, transmit, use, and disclose Client PHI as necessary to provide the services and perform its obligations under the Agreement; and

5.2 create, receive, maintain, transmit, use, and disclose Client PHI for the proper management and administration of Business Associate, or to carry out the legal responsibilities of Business Associate, provided that, with respect to disclosures: (i) the disclosures are Required by Law; or (ii) any third party to which Business Associate discloses Client PHI provides written reasonable assurances in advance that: (a) the information will be held confidentially and used or further disclosed only for the purpose for which it was disclosed to the third party; and (b) the third party promptly will notify Business Associate of any instances of which it becomes aware in which the confidentiality of the Client PHI has been compromised.

**6. Safeguards for the Protection of Client PHI.** Business Associate shall: (i) use safeguards that are designed to appropriately prevent the use or disclosure (other than as provided for by this Addendum) of Client PHI; and (ii) implement administrative, physical and technical safeguards that are designed to reasonably and appropriately protect the confidentiality, integrity and availability of Electronic Client PHI. If Business Associate agrees at the request of Client to provide customized safeguards, such safeguards shall be documented in applicable statements of work or in comparable contract documents describing the services to be performed. In all cases, Business Associate shall comply with the Security Rule requirements for business associates in 45 C.F.R. Parts 160 and 164 (Subparts A & C).

**7. Reporting of Unauthorized Uses or Disclosures.** In compliance with HIPAA Business Associate shall report to Client:

7.1 any use or disclosure of Client PHI of which Business Associate becomes aware that is not provided for or permitted in this Addendum.;

7.2 any Security Incident of which Business Associate becomes aware; provided, however, that the Parties acknowledge and agree that no additional notice is required by Business Associate to Client for the ongoing existence and occurrence of Unsuccessful Security Incidents. "Unsuccessful Security Incidents" means, without limitation, pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denial of service attacks, and any combination of the above, so long as no such incident results in unauthorized access, use, disclosure, modification or destruction of Client PHI or intentional interference with system operations in an information system that contains Client PHI; and

7.3 any Breach of Unsecured Client PHI of which Business Associate becomes aware, without unreasonable delay and in no case later than 30 days following the discovery by Business Associate of such Breach. Business Associate shall provide Client with written notification of Breach in accordance with 45 C.F.R. § 164.410.

**8. Use of Subcontractors.** Business Associate shall cause each Subcontractor of Business Associate (including, without limitation, a Subcontractor that is an agent under Applicable Law) that creates, receives, maintains, transmits, uses, or discloses Client PHI on behalf of Client to sign a written agreement with Business Associate satisfying the requirements of 45 C.F.R. §§ 164.504(e) and 164.314(a)(2) and containing at least as restrictive provisions and conditions related to the protection of Client PHI as those that apply to Business Associate under this Addendum.

**9. Authorized Access to and Amendment of Client PHI.** Only to the extent that Business Associate maintains Client PHI in Designated Record Sets, Business Associate shall: (i) within 30 business days of a written request by Client for access to Client PHI about an Individual contained in any Designated Record Set of Client maintained by Business Associate, make available to Client in accordance with 45 C.F.R. § 164.524, all such Client PHI held by Business Associate, including electronic access to Client PHI maintained by Business Associate in electronic form; and (ii) within 30 business days of a written request by Client to amend Client PHI, incorporate any amendments Client makes to Client PHI in accordance with 45 C.F.R. § 164.526. In the event that Business Associate receives a request for access to Client PHI directly from an Individual, Business Associate shall direct the Individual to contact Client directly.

**10. Accounting of Disclosures of Client PHI.** Business Associate shall keep records of disclosures of Client PHI made by Business Associate (the "Disclosure Accounting") during the term of this Addendum in accordance with 45 C.F.R. § 164.528. Business Associate shall provide the Disclosure Accounting to Client within 45 days of receiving a written request therefor from Client. Business Associate shall comply with, and assist Client in compliance with, additional requirements of 42 U.S.C. § 13405(c), if and when applicable. In the event that Business Associate receives a request for a Disclosure Accounting of Client PHI directly from an Individual, Business Associate shall direct the Individual to contact Client directly.

**11. Health and Human Services.** Business Associate shall make its internal practices, books and records related to the use and disclosure of Client PHI under the Agreement and this Addendum available to Secretary of the Department of Health and Human Services for the purpose of determining Client's compliance with 45 C.F.R. § 164.500 et seq.

**12. Client Responsibilities.** Client warrants that it has obtained and will obtain any consents, Authorizations, and/or other legal permissions required under HIPAA and other Applicable Law for the disclosure of Client PHI to Business Associate. Client shall notify Business Associate 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 Business Associate's use or disclosure of Client PHI under this Addendum. Client shall not agree to any restriction on the creation, receipt, maintenance, transmission, use, or disclosure of PHI under 45 C.F.R. § 164.522 that restricts Business Associate's creation, receipt, maintenance, transmission, use, or disclosure of Client PHI under this Agreement unless such restriction is Required By Law or Business Associate grants its written consent to such restriction, which consent shall not be unreasonably withheld.

**13. Future Protections of Client PHI.** Upon the expiration or earlier termination of this Addendum for any reason, if feasible, Business Associate shall return to Client, or, at Client's direction, destroy, all Client PHI in any form. If Business Associate determines that such return or destruction is not feasible, Business Associate shall extend the protections of this Addendum to the Client PHI and shall limit further creation, receipt, maintenance, transmission, use, or disclosure to those purposes that make the return or destruction of the Client PHI infeasible.

**14. Termination.** Either Party (the "Non-Breaching Party") may terminate this Addendum upon 30 days' prior written notice to the other party (the "Breaching Party") in the event that the Breaching Party materially breaches this Addendum and such breach is not cured to the reasonable satisfaction of the Non-Breaching Party within such 30-day period. In the event of termination of this Addendum, either Party may terminate those portions of the Agreement, and only those portions of the Agreement, that require Business Associate to create, receive, maintain, transmit, use, or disclose Client PHI, in accordance with and subject to any rights to cure and payment obligations specified in the Agreement.

**15. Effect on Agreement.** This Addendum is not intended to, nor shall it be construed to, reduce or diminish any of Business Associate's or Client's obligations under the Agreement. Accordingly, except as set forth in section entitled "Termination" or to the extent expressly inconsistent with this Addendum, all other terms of the Agreement shall remain in full force and effect and shall not be modified, diminished, or reduced hereby. In the event of a conflict between this Addendum and the Base Agreement, including applicable transaction document, with respect to the privacy and security of Client PHI or compliance with HIPAA, the terms more protective of Client PHI shall control. In all other cases, the terms of the Agreement shall control.

**16. No Intended Third Party Beneficiaries.** There are no intended third party beneficiaries under this Addendum.

**17. Independent Contractor Status.** The Parties acknowledge and agree that Business Associate is at all times acting as an independent contractor of Client and not as an agent or employee of Client under this Addendum.

**18. Assignment.** Neither Party may assign this Addendum, in whole or in part, without the prior written consent of the other. Any attempt to do so is void. Neither Party will unreasonably withhold such consent. The assignment of this Addendum, in whole or in part, to any majority-owned subsidiary in the United States or to a successor organization by merger or acquisition does not require the consent of the other. It is not considered an assignment for Business Associate to divest a portion of its business in a manner that similarly affects all of its Clients.

**19. Future Amendments.** Any future amendments to HIPAA affecting the required provisions of business associate agreements are hereby incorporated by reference into this Addendum as if set forth in this Addendum in their entirety, effective on the later of the effective date of this Addendum or such subsequent date as may be specified by HIPAA. No other amendment to this Addendum shall be valid unless agreed to in writing by both Parties.

---

Each Party accepts the terms of this Business Associate Addendum by signing this Addendum (or another document that incorporates it by reference) by hand or electronically.

Agreed to:

**Client Company Name:**

Agreed to:

**International Business Machines Corporation**

By \_\_\_\_\_

Authorized signature

By \_\_\_\_\_

Authorized signature

Title:

Name (type or print):

Title:

Name (type or print):

Date:

Date:

Client number:

Base Agreement number:

Enterprise number:

Client address:

IBM address: