

Business Associate Agreement

1. **Definitions.** Capitalized terms in this Business Associate Agreement ("BAA"), not otherwise defined, have the same meaning ascribed to those terms in the HIPAA Regulations provided, however, that:
 - A. "Business Associate" means Carestream Health, Inc. 150 Verona Street, Rochester, NY 14608 ("Carestream") and its subsidiaries, but only to the extent Carestream's access to PHI is more than incidental or limited in nature and does not occur under the control of Covered Entity or on Covered Entity's premises. Carestream does not, by agreeing to this BAA, concede that it is a business associate. Where the term "business associate" appears without an initial capital letter, it has the meaning given to such term in the HIPAA Regulations.
 - B. "Covered Entity" means [[ContractorCoName]], [[ContractorAddress]], [[ContractorCity]], [[ContractorState]], [[ContractorZip]] and, to the extent they are receiving services from Business Associate, its subsidiaries or parent and each subsidiary of its parent, as applicable.
 - C. "PHI" means Protected Health Information limited to the information Business Associate received from, or created, or received on behalf of, Covered Entity as Covered Entity's Business Associate. "ePHI" means a subset of PHI that is created or transmitted electronically.
 - D. "Underlying Agreement" means the commercial agreement(s) between Business Associate and Covered Entity pursuant to which Business Associate is providing services to Covered Entity that has given rise to the need for this BAA.
2. **Obligations of Business Associate.** With regard to its use and disclosure of PHI, Business Associate shall:
 - A. Not use or disclose PHI other than as permitted or required by the Underlying Agreement or as required by law;
 - B. Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of ePHI and use appropriate safeguards to prevent use or disclosure of PHI other than as permitted here;
 - C. Report to Covered Entity any use or disclosure of PHI not provided for by this BAA and any Security Incident of which Business Associate becomes aware;
 - D. Use reasonable commercial efforts to mitigate any harmful effect known to Business Associate of a use or disclosure of PHI by Business Associate in violation of this BAA;
 - E. Ensure that any agents and subcontractors to whom Business Associate provides PHI agree to the same restrictions and conditions that apply through this BAA to Business Associate and that such agents and subcontractors implement reasonable and appropriate safeguards with respect to such PHI;
 - F. Make available to Covered Entity any PHI maintained by Business Associate in a Designated Record Set within 20 days of receiving a written request from Covered Entity, so that Covered Entity can respond to Individual requests for access or amendments;
 - G. Incorporate amendments to any PHI maintained by Business Associate in a Designated Record Set within 40 days of receiving a written request from Covered Entity;
 - H. Document 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 and provide this accounting to Covered Entity within 40 days of receiving a written request from Covered Entity, at the address specified by Covered Entity in the request; and
 - I. Make Business Associate's internal practices, books and records relating to the use and disclosure of PHI and Business Associate's policies, procedures and documentation related to the safeguards required by the Security Rule available to the Secretary for purposes of determining Covered Entity's compliance with the HIPAA Regulations.
3. **Permitted Uses and Disclosures of PHI.** Covered Entity shall not request Business Associate to use or disclose PHI in any manner that would not be permissible under the HIPAA Regulations if done by Covered Entity, except that Business Associate may make any and all uses and disclosures of PHI necessary to perform its obligations under the Underlying Agreement, including:

Carestream [[ContractNumber]]

- A. Use PHI for its proper management and administration and to carry out the legal responsibilities of Business Associate;
- B. Disclose PHI to a third party for the purpose of Business Associate's proper management and administration or to carry out the legal responsibilities of Business Associate, provided that the disclosures are Required By Law or Business Associate obtains reasonable assurances from the third party regarding the confidential handling of such PHI as required under the HIPAA Regulations;
- C. Provide Data Aggregation services relating to the health care operations of Covered Entity; and
- D. De-identify PHI, and use de-identified data, in accordance with the de-identification provisions of HIPAA Regulations.

4. Termination.

- A. If Covered Entity learns of a material breach by Business Associate, Covered Entity shall either provide an opportunity for Business Associate to cure such breach or to end such violation, as applicable. If Business Associate does not cure or cease the violation, or if a cure is not possible, Covered Entity shall either (a) terminate the Underlying Agreement if, in Covered Entity's sole discretion, it is feasible; or, (b) if neither termination nor cure is feasible, report the violation to the Secretary.
- B. With the exception of incidental elements of PHI required to maintain US Food and Drug Administration Quality Systems records, upon termination of the Underlying Agreement for any reason, Business Associate shall return or destroy all PHI in Business Associate's possession or in the possession of Business Associate's subcontractors or agents. Business Associate shall retain no copies of returned or destroyed PHI. If return or destruction is not feasible, Business Associate shall provide Covered Entity with notification of the conditions that make the return or destruction of such PHI not feasible. Any PHI retained by Business Associate will remain subject to all of the protections of this BAA, and Business Associate shall make no further use of such PHI. The rights and obligations of Business Associate under this subsection survive termination of the Underlying Agreement.

5. HITECH.

- A. Business Associate acknowledges that HITECH requires Business Associate to adhere to the administrative, physical, and technical safeguards, and policy, procedure, and documentation requirements of the HIPAA Administrative Simplification Security Rule in the same manner that such sections apply to Covered Entity, and Business Associate shall so comply.
- B. As required by HITECH, if Business Associate commits or discovers a breach involving unsecured protected health information, Business Associate shall notify Covered Entity in accordance with the provisions in HITECH.
- C. To the extent Business Associate is responsible for a breach involving unsecured protected health information, Business Associate shall reimburse Covered Entity for direct costs, such as postage, printing and media fees, that Covered Entity expends to meet its notification obligations under HITECH. If the breach was discovered by Covered Entity through its own investigation, as opposed to Business Associate self-reporting, then Business Associate shall also reimburse Covered Entity for reasonable investigative costs to the extent of Business Associate's culpability. In addition, prior to Covered Entity sending out notification to individuals affected by that breach, Business Associate and Covered Entity shall meet and agree on: (a) a mitigation plan for those affected individuals, and (b) allocation of costs related to that plan. Business Associate's obligation to reimburse or assume costs under this section is limited to Business Associate's comparative liability for the breach which gave rise to those costs and is subject to the Remedies section in the Underlying Agreement.

6. Miscellaneous.

- A. The parties intend that any ambiguities, or any conflict between the terms of this BAA and the Underlying Agreement, be resolved in favor of permitting the parties to comply with the HIPAA Regulations. If the HIPAA Regulations are materially amended, the parties agree to amend this BAA solely as needed for the parties to comply with the HIPAA Regulations.
- B. This BAA does not confer upon any person other than the parties and their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.

7. **LIMITATION OF LIABILITY:** NOTWITHSTANDING ANY CONTRARY TERMS, THE PARTIES EXPRESSLY AGREE THAT NEITHER PARTY SHALL BE LIABLE FOR INCIDENTAL, CONSEQUENTIAL, PUNITIVE, OR EXEMPLARY DAMAGES, REGARDLESS OF WHETHER THE PARTY IN BREACH WAS ADVISED OF, OR OTHERWISE SHOULD HAVE BEEN AWARE OF, THE POSSIBILITY OF SUCH DAMAGES. NOTWITHSTANDING ANY CONTRARY TERMS, THE PARTIES EXPRESSLY AGREE THAT THE TOTAL AGGREGATE LIABILITY OF EACH PARTY UNDER THIS AGREEMENT SHALL NOT EXCEED THE TOTAL FEES PAYABLE UNDER THE UNDERLYING AGREEMENT.

The Parties are entering into this BAA on [[ContStartDt]].

By their signature below, the parties acknowledge that this agreement supersedes all prior or contemporaneous representations, agreements, understandings or commitments, whether written or oral, relating to the subject matter of this agreement. The invalidity of any provision of this agreement does not affect the validity of the remaining provisions and the parties shall construe this agreement as if such invalid provision had been omitted. No provision of this agreement may be terminated, modified or waived except in a written agreement executed by the parties.

Carestream Health, Inc.

[[ContractorCoName]]

Signature		Signature
	Name	
	Title	