



HIPAA Business Associate Agreement

This Business Associate Agreement (“**BAA**”) is entered into by and between ForgeRock US, Inc. (“**ForgeRock**”) as a Business Associate and the entity that will access the ForgeRock Identity Cloud as a Covered Entity (“**Customer**”). This BAA is incorporated into the license agreement that governs Customer’s access to the ForgeRock Identity Cloud (the “**Agreement**”) between ForgeRock and Customer. This BAA shall become effective upon the date of last signature below. This Agreement shall become effective upon the execution of an Order Form that incorporates its terms.

WHEREAS, Business Associate provides certain data processing and hosting services (“**Services**”) to Covered Entity pursuant to the Agreement;

WHEREAS, in connection with these Services, Business Associate may receive, maintain or transmit PHI from, to, or on behalf of, Covered Entity, which PHI is subject to certain protections under the HIPAA Rules; and

WHEREAS, this BAA defines the rights and responsibilities of each party with respect to PHI exchanged pursuant to this BAA and the Agreement;

NOW, THEREFORE, for good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the parties agree as follows:

1. Definitions. All capitalized term used but not defined herein shall have the meaning set forth in the HIPAA Rules. The following terms are specifically defined as follows:

1.1. “*Business Associate*” has the same meaning as the term “business associate” at 45 CFR 160.103, and in reference to the party to this BAA, shall mean ForgeRock.

1.2. “*Covered Entity*” has the same meaning as the term “covered entity” at 45 CFR 160.103, and in reference to the party to this BAA, shall mean Customer

1.3. “*HIPAA Rules*” means, with respect to the federal Health Insurance Portability and Accountability Act of 1996, Pub. Law 101-191, as amended from time to time, and the Health Information Technology for Economic and Clinical Health (“HITECH”) Act of 2009 (as applicable).

1.4. “*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 or Disclosure of Covered Entity’s electronic protected health information “ePHI.”

2. Obligations and Activities of Business Associate.

2.1 Business Associate agrees not to use or disclose PHI received or created by Business Associate except as permitted by this BAA, the Agreement, or as Required by Law.

2.2 Business Associate agrees to use appropriate safeguards, and to comply with Subpart C of 45 CFR Part 164 with respect to ePHI, to prevent use or Disclosure of PHI other than as provided for by this BAA, the Agreement, or as Required by Law.

2.3 Business Associate agrees to report to Covered Entity any use or Disclosure of PHI not provided for by this BAA of which it becomes aware, including a Breach of Unsecured PHI as required under 45 C.F.R. §164.410, and any Security Incident of which it becomes aware. Notwithstanding the foregoing, the parties acknowledge and agree that this Section 2(c) constitutes notice by Business Associate to Covered Entity of the ongoing existence and occurrence or attempts of Unsuccessful Security Incidents for which no additional notice to Covered Entity shall be required.

2.4 Business Associate agrees, in accordance with 45 CFR 164.502(e)(1)(ii) and 164.308(b)(2), if applicable, to obtain from any Subcontractor that creates, receives, maintains, or transmits PHI on behalf of Business Associate pursuant to this BAA and the Agreement, reasonable assurance that

Subcontractor will adhere to restrictions and conditions that apply to Business Associate through this BAA with respect to such PHI as required by the HIPAA Rules.

2.5 Business Associate Agrees to make amendment(s) to PHI maintained in a Designated Record Set (if any), as requested by the Covered Entity or an individual (as applicable) pursuant to 45 C.F.R. §164.526, or take other measures as reasonably necessary to enable Covered Entity to satisfy its obligations under 45 C.F.R. §164.526.

2.6 Business Associate agrees to make available, at the request of Covered Entity, PHI that is maintained in a Designated Record Set (if any) as necessary to allow Covered Entity to satisfy its obligations under 45 C.F.R. §164.524.

2.7 Business Associate agrees to maintain and make available to Covered Entity the information required to provide an accounting of Disclosures, as reasonably necessary to satisfy Covered Entity's obligations under 45 C.F.R. §164.528.

2.8 For clarity, with respect to the foregoing Sections 2.5 – 2.7 of this BAA, in no case shall Business Associate be responsible for responding directly to any Individual who submits a request to Business Associate pursuant to 45 CFR §164.524; provided that Business Associate shall promptly forward such request to Covered Entity in accordance with Sections 2.5 – 2.7 of this BAA.

2.9 To the extent that Business Associate is to carry out one or more of Covered Entity's obligation(s) under Subpart E of 45 CFR Part 164, Business Associate agrees to comply with the requirements of Subpart E that apply to Covered Entity in the performance of such obligation(s).

2.10 Business Associate agrees to make its internal practices, books, and records, regarding the use and Disclosure of PHI created or received by the Business Associate on behalf of the Covered Entity available to the Secretary for purposes of the Secretary determining compliance with the HIPAA Rules.

3. Permitted Uses and Disclosures by Business Associate.

3.1 Business Associate may not use or disclose PHI in a manner that would violate Subpart E of 45 C.F.R. Part 164 if done by Covered Entity.

3.2 Business Associate may use and disclose PHI:

- (i) To perform the Services set forth in the Agreement and as otherwise set forth in this BAA;
- (ii) As Required by Law, including to report violations of law to appropriate Federal and State authorities;
- (iii) For the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate;
- (iv) To provide Data Aggregation services to Covered Entity; and
- (v) To de-identify the PHI in accordance with 45 CFR 164.514(a)-(c), (after which the information shall not longer be considered PHI and shall not be subject to the terms of this BAA).
- (vi) Any permitted use or Disclosure under Section 3.2(i)-(iv) shall be consistent with the minimum necessary requirements set forth in the HIPAA Rules.

4. Obligations of Covered Entity.

4.1 During the Term of this BAA, Covered Entity shall:

- (i) Provide Business Associate with a copy of its Notice of Privacy Practices;
- (ii) Notify Business Associate of any limitations in its Notice of Privacy Practices, to the extent that such limitation may affect Business Associate's use or Disclosure of PHI;
- (iii) 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;
- (iv) Not request Business Associate to use or disclose PHI in any manner that would not be permissible under HIPAA if done by Covered Entity (other than as permitted pursuant to Section 3.2(iii-iv)); and
- (v) Comply with all HIPAA requirements applicable to Covered Entity.

5. Term and Termination.

5.1 Term. The Term of this BAA shall commence as of the effective date and, except for the rights and obligations set forth in this BAA specifically surviving termination, shall terminate upon the termination or expiration of the Agreement, unless otherwise earlier terminated for cause in accordance with this Section 5.

5.2 Termination by Covered Entity. In addition to any termination provisions set forth in the applicable Agreement, Covered Entity may terminate this BAA if Covered Entity determines, in good faith and after reasonable investigation, that Business Associate has violated a material term of this BAA, and Business Associate has failed to cure such material breach or end the violation within thirty (30) days of notice by Covered Entity of such alleged breach.

5.3 Termination by Business Associate. In addition to and notwithstanding any termination provisions set forth in the applicable Agreement, Business Associate may terminate this BAA if Business Associate determines, in good faith and after reasonable investigation, that Covered Entity has violated a material term of this BAA, and Covered Entity has failed to cure such material breach or end the violation within thirty (30) days of notice by Business Associate of such alleged breach.

5.4 Effect of Termination. Upon termination or expiration of this BAA for any reason, Business Associate, with respect to any PHI received from Covered Entity or created, maintained, or received by Business Associate on behalf of Covered Entity, shall:

- (i) Retain only that PHI which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities (if any);
- (ii) Return to Covered Entity or destroy, at Covered Entity's expense, the remaining PHI that the Business Associate still maintains in any form that is not necessary to carry out Section 5(d)(i);
- (iii) Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 with respect to ePHI to prevent use or Disclosure of the PHI, other than as provided for in this Section 5.3, for as long as Business Associate retains the PHI;
- (iv) Not use or disclose the PHI retained by Business Associate other than for the purposes for which such PHI was retained and subject to the same conditions set out at Section (ii) which applied prior to termination; and
- (v) Return to Covered Entity or destroy the PHI retained by Business Associate when it is no longer needed by Business Associate for its proper management and administration, or to carry out its legal responsibilities.

6. Miscellaneous.

This BAA is governed by, and will be construed in accordance with, the governing law of the Agreement. Any action relating to this BAA must be commenced within two years after the date upon which the cause of action accrued. This BAA may only be assigned in connection with an assignment of the Agreement, if any. If any part of a provision of this BAA is found illegal or unenforceable, it will be enforced to the maximum extent permissible, and the legality and enforceability of the remainder of that provision and all other provisions of this BAA will not be affected. All notices relating to the parties' legal rights and remedies under this BAA will be provided in writing to a party, will be sent to its address set forth in the Agreement, or to such other address as may be designated by that party by notice to the sending party, and will reference this BAA. This BAA may be modified, or any rights under it waived, only by a written agreement executed by the authorized representatives of the parties. The parties agree to take such action as is necessary to amend this BAA from time to time as is necessary for the parties to comply with the requirements of applicable law. This BAA is the complete and exclusive agreement between the parties with respect to the subject matter hereof, superseding and replacing all prior agreements, communications, and understandings (written and oral) regarding its subject matter. Any ambiguity in this BAA shall be resolved in favor of the meaning that permits the parties to comply with applicable law and any current regulations promulgated thereunder. Any failure of a party to exercise or enforce any of its rights under this BAA will not act as a waiver of such rights.