

## Business Associate Agreement

### 1. RECITALS

- a. Covered Entity is a covered entity under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”). Covered Entity must comply with the Administrative Simplification Provisions of HIPAA, including the Privacy Rule and Security Rule (as defined in Article 1 of this Agreement), and with the applicable provisions of the Health Information Technology for Economic and Clinical Health Act of 2009 (“HITECH”).
- b. Covered Entity has engaged Business Associate to furnish certain products and/or services to Covered Entity pursuant to the Contract, as defined below.
- c. The Parties acknowledge that pursuant to the Contract (1) Business Associate does not require access to PHI; (2) Business Associate will not collect, create, maintain, process, or transmit PHI; but (3) Business Associate may have incidental or actual access to PHI during file analysis, or as part of data that is potentially accessible by Business Associate during the performance of remote or on-site technology services.
- d. In the event Business Associate creates, receives, maintains or transmits PHI pursuant to the Contract, the purpose of this BA Agreement is to set forth the terms and conditions deemed necessary by the Parties hereto to ensure compliance with the applicable requirements under HIPAA. The Parties acknowledge and agree that this Agreement only applies to the extent that Business Associate is a business associate of Covered Entity under HIPAA.

NOW, THEREFORE, in consideration of the mutual promises below and for other good and valuable consideration, the receipt and adequacy of which are hereby acknowledged, the Parties agree as follows:

### 2. DEFINITIONS

Terms used in this Agreement that are specifically defined in HIPAA shall have the same meaning as set forth in HIPAA. A change to HIPAA which modifies any defined HIPAA term, or which alters the regulatory citation for the definition shall be deemed incorporated into this BA Agreement.

- a. **“Breach”** means the unauthorized acquisition, access, use, or disclosure of Protected Health Information, which compromises the security or privacy of such information, except where an unauthorized person to whom such information is disclosed would not reasonably have been able to retain such information. The term “breach” does not include the exceptions described in 45 C.F.R. § 164.402(1).
- b. **“Business Associate”** has the meaning given to such term under HIPAA, including, but not limited to, 45 C.F.R § 160.103.
- c. **“Contract”** shall mean the Palo Alto Networks EULA and the Palo Alto Networks EUSA between Business Associate and Covered Entity and any other underlying agreement(s) that outline the terms of the products and/or services that Business Associate agrees to provide to Covered Entity.

- d. **“Covered Entity”** means the Covered Entity, as indicated above. Where the term “covered entity” appears without an initial capital letter, it has the meaning given to such term under HIPAA, including, but not limited to, 45 C.F.R § 160.103.
- e. **“Data Aggregation”** has the meaning given to the term under the Privacy Rule, including, but not limited to, 45 C.F.R. § 164.501.
- f. **“Designated Record Set”** has the meaning given to the term under the Privacy Rule, including, but not limited to, 45 C.F.R. §164.501.
- g. **“Electronic Protected Health Information”** and/or **“EPHI”** has the same meaning as the term “electronic protected health information” in 45 C.F.R. § 160.103, and Business Associate on behalf of Covered Entity.
- h. **“HIPAA”** means the Health Insurance Portability and Accountability Act of 1996, Public Law 104-91, as amended, and related HIPAA regulations (45 C.F.R. Parts 160-164).
- i. **“HITECH”** means the Health Information Technology for Economic and Clinical Health Act, found in Title XIII of the American Recovery and Reinvestment Act of 2009, Public Law 111-005.
- j. **“Individual”** has the meaning given to the term under the Privacy Rule, including, but not limited to, 45 C.F.R § 160.103. It also includes a person who qualifies as a personal representative in accordance with 45 C.F.R. § 164.502(g).
- k. **“Privacy Rule”** means the Standards for Privacy of Individually Identifiable Health Information codified at 45 C.F.R. Part 160 and Part 164 (Subparts A, D, and E) and any other applicable provision of HIPAA and any amendments to HIPAA, including HITECH.
- l. **“Protected Health Information”** and/or **“PHI”** has the meaning given to the term under the Privacy Rule, including but not limited to, 45 C.F.R. § 164.103, and is limited to PHI provided by Covered Entity to Business Associate as well as PHI created or received by Business Associate on behalf of Covered Entity. Unless otherwise stated in this BA Agreement, any provision, restriction, or obligation in this BA Agreement related to the use of PHI shall apply equally to EPHI.
- m. **“Required By Law”** has the meaning given to the term under the Privacy Rule, including but not limited to, 45 C.F.R. § 164.103.
- n. **“Secretary”** means the Secretary of the U.S. Department of Health and Human Services or his designee.
- o. **“Security Incident”** means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system as provided in 45 C.F.R. § 164.304.

- p. **“Security Rule”** means the Security Standards for the Protection of Electronic Protected Health Information codified at 45 C.F.R. Part 160 and Part 164 (Subparts A and C) and any other applicable provision of HIPAA and any amendments to HIPAA, including HITECH.
- q. **“Subcontractor”** means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.
- r. **“Unsecured PHI”** shall mean PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary from time to time.

### 3. **BUSINESS ASSOCIATE’S OBLIGATIONS**

- a. Request, Use, and Disclosure of PHI. Business Associate agrees that it will use and disclose PHI only in accordance with the terms of this BA Agreement or as Required By Law. Business Associate acknowledges that it may use and disclose PHI obtained or created pursuant to the Contract only if the use or disclosure complies with each applicable requirement of the Privacy Rule found in 45 C.F.R. § 164.504(e).
- b. Permitted Requests, Uses, and Disclosures. Business Associate may use or disclose PHI for the purpose of performing its obligations to Covered Entity as described in the Contract, consistent with the requirements of HIPAA and this BA Agreement, and for other uses and disclosures permitted under this BA Agreement. Business Associate will not request, use, or disclose PHI in any manner that constitutes a violation of the Privacy Rule. To the extent that Business Associate is carrying out any of Covered Entity’s obligations under the Privacy Rule, Business Associate will comply with all requirements of the Privacy Rule that apply to a covered entity. In accordance with 45 C.F.R. § 164.504(e)(4), Business Associate may request, use, or disclose PHI: (a) as is necessary for the proper management and administration of Business Associate; or (b) to carry out the legal responsibilities of Business Associate. Business Associate may disclose PHI for these purposes, in accordance with the provisions of 45 C.F.R. § 164.504(e)(4)(ii), only if either: (i) the disclosure is Required By Law; or (ii) Business Associate obtains reasonable assurances from the person to whom Business Associate discloses the PHI that the PHI will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person and that the person will notify Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.
- c. Minimum Necessary Requirements. Business Associate will request, use, and disclose only the minimum amount of PHI necessary to perform the services for which it has been retained by Covered Entity. The Parties acknowledge that the phrase “minimum necessary” shall be interpreted in accordance with the Privacy Rule and Secretary’s guidance on what constitutes minimum necessary.
- d. Administrative, Physical, and Technical Safeguards. Business Associate will develop, implement, maintain, and use appropriate safeguards to prevent any use or disclosure of the PHI other than as provided by this Agreement. Business Associate will implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of EPHI. Business Associate acknowledges that the Security Rule provisions regarding administrative safeguards, physical safeguards, technical safeguards, and policies and procedures and documentation requirements found in 45

C.F.R. §§ 164.308, 164.310, 164.312 and 164.316 apply to Business Associate in the same manner as to Covered Entity. Business Associate will comply fully with these provisions of the Security Rule.

- e. Agents and Subcontractors. Prior to making any permitted disclosures, Business Associate will ensure that any subcontractors that create, receive, maintain, or transmit PHI on its behalf agree in writing to be bound by the same privacy and security restrictions and conditions that apply to Business Associate under this Agreement, including but not limited to those conditions relating to termination of the contract for improper disclosure. Further, Business Associate shall implement and maintain sanctions against agents and subcontractors, if any, that violate such restrictions and conditions. Business Associate shall terminate any agreement with an agent or subcontractor, if any, who fails to abide by such restrictions and obligations.
- f. Reporting of Illegal, Unauthorized, or Improper Uses or Disclosures. Business Associate will report to Covered Entity's designated contact any illegal, unauthorized, or improper use or disclosure of PHI, Security Incident, or Breach of Unsecured PHI (collectively, "Known Misuse") by Business Associate or its agents or subcontractors within thirty (30) business days of obtaining knowledge of the Known Misuse. In the case of a Breach of Unsecured PHI, the initial notification, to the extent feasible, will include the identification of individuals whose Unsecured PHI has been or is reasonably believed to have been accessed, acquired, disclosed, or used during the Breach. As requested, Business Associate will provide Covered Entity with additional information in its possession to allow Covered Entity to comply with its notification obligations for Breaches of Unsecured PHI. Business Associate will implement a reasonable system for discovery of Breaches of Unsecured PHI.
- g. This section constitutes notice to Covered Entity of the ongoing existence and occurrence of attempted but Unsuccessful Security Incidents (as defined below) for which no additional notice to Covered Entity is required. "Unsuccessful Security Incidents" include, but are not limited to, pings and other broadcast attacks on Business Associate's firewall, port scans, unsuccessful log-on attempts, denials of service, and any combination of the above, so long as no such incident results in unauthorized access, use, or disclosure of PHI.
- h. Mitigation of Harmful Effect. Business Associate will take commercially reasonable actions to mitigate any harmful effect of a Known Misuse that is known to Business Associate and adopt additional or improve existing safeguards to prevent recurrence.
- i. Access to PHI. Business Associate will make PHI contained in Designated Record Sets that are maintained by Business Associate or its agents or subcontractors, if any, available to Covered Entity for inspection and copying to enable a Covered Entity to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 C.F.R. § 164.524. Business Associate will make PHI available for these purposes within ten (10) business days of a request by Covered Entity.
- j. Amendments to PHI. Within ten (10) business days of receipt of a request from Covered Entity for an amendment of PHI or a record about an Individual contained in a Designated Record Set, Business Associate or its agents or subcontractors, if any, shall make such PHI available to Covered Entity for amendment and shall incorporate any such amendment to enable Covered Entity to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 C.F.R. § 164.526. If one Individual requests an

amendment of PHI directly from Business Associate or its agents or subcontractors, if any, Business Associate will notify Covered Entity in writing within ten (10) business days of the request. Any approval or denial of an amendment of PHI maintained by Business Associate or its agents or subcontractors, if any, shall be the responsibility of Covered Entity. Upon the approval of Covered Entity, Business Associate shall appropriately amend the PHI maintained by it or its agents or subcontractors.

k. Accountings of Disclosures of PHI.

i. Business Associate agrees to maintain necessary and sufficient documentation of disclosures of PHI as would be required for Covered Entity to respond to a request by an Individual for an accounting of disclosures as necessary to fulfill Covered Entity's obligations under the Privacy Rule, including, but not limited to, 45 C.F.R. §164.528. Notwithstanding Section 4.3 below, Business Associate and any agents or subcontractors shall continue to maintain the information required for purposes of complying with this Section 2.10 for a period of six (6) years after termination of the Agreement.

ii. Within ten (10) business days of notice by Covered Entity of a request for an accounting of disclosures of PHI, Business Associate and any agents or subcontractors shall make available to Covered Entity the information required to provide an accounting of disclosures to enable Covered Entity to fulfill its obligations under the Privacy Rule, including, but not limited to, 45 C.F.R. §164.528. If a request for an accounting is made directly to Business Associate or its agents or subcontractors, Business Associate will notify Covered Entity of the request within ten (10) business days of having received the request. Business Associate will make available to Covered Entity the information required to provide the requested accounting of disclosure. Business Associate will not make any accounting of disclosures directly to an Individual, unless required to do so by law.

l. Internal Practices, Books, and Records. Business Associate will make its internal practices, books, and records relating to the use and disclosure of PHI available to the Secretary for purposes of determining Covered Entity's and Business Associate's compliance with the Privacy Rule. Business Associate will notify Covered Entity regarding any PHI that Business Associate provides to the Secretary concurrently with providing the requested PHI to the Secretary. Upon request by Covered Entity, Business Associate will provide Covered Entity with a duplicate copy of the requested PHI. Notwithstanding this provision, no attorney-client, accountant-client or other legal privilege or immunity will be deemed waived by Business Associate or Covered Entity as a result of this section.

#### 4. **COVERED ENTITY OBLIGATIONS**

a. Notification of Limitations in Notice of Privacy Practices. Covered Entity shall notify Business Associate of any limitation(s) in Covered Entity's required notice of privacy practices to the extent that such limitation may affect Business Associate's use or disclosure of PHI.

b. Notification of Restrictions on PHI Use or Disclosure. Covered Entity shall notify Business Associate of any restriction to the use or disclosure of PHI or of any request for confidential communication in the use or disclosure of PHI that Covered Entity has agreed to or must comply with in accordance with 45 C.F.R.

§ 164.522 and 42 U.S.C. § 17935(a) to the extent that such restriction may affect Business Associate's use or disclosure of PHI.

- c. Notification of Changes or Revocations of Permission. Covered Entity shall provide Business Associate with notice of any grant of, change to, or revocation of permission by Individual to use or disclose PHI within a reasonable period of time after Covered Entity becomes aware of such occurrence to the extent that such event may affect Business Associate's permitted uses or disclosures of PHI.
- d. Compliance with HIPAA. Covered Entity warrants that Covered Entity, its directors, officers, subcontractors, employees, affiliates, agents, and representatives (i) shall comply with the Privacy Rule in its use or disclosure of PHI; (ii) shall not use or disclose PHI in any manner that violates applicable federal and state laws; (iii) shall not request Business Associate to use or disclose PHI in any manner that violates applicable federal and state laws if such use or disclosure were done by Covered Entity; and (iv) may request Business Associate to disclose PHI directly to another party only for the purposes allowed by the Privacy Rule. The provisions of this section shall survive the termination of this BA Agreement.

## 5. TERMINATION

- a. Term and Survival. The term of this BA Agreement shall be effective as of the Effective Date of this BA Agreement and continue until terminated by Covered Entity or any underlying Contract expires or is terminated. Any provision related to the use, disclosure, access, or protection of EPHI or PHI or that by its terms shall survive termination of this BA Agreement.
- b. Termination for Breach.
  - i. Covered Entity may immediately terminate this BA Agreement if Covered Entity determines that Business Associate, or any of Business Associate's agents or subcontractors, has breached a material term of this BA Agreement, including by engaging in a pattern of activity or practice that constitutes material breach of this BA Agreement or by violating Business Associate's obligations under this BA Agreement. Alternatively, Covered Entity may choose to provide Business Associate with written notice of the material breach and terminate this BA Agreement if Business Associate has not cured the breach within thirty (30) calendar days of receiving written notice from Covered Entity.
  - ii. Business Associate may immediately terminate this BA Agreement if it determines that Covered Entity has breached a material term of this BA Agreement, including by engaging in a pattern of activity or practice that constitutes material breach of this Agreement or by violating Covered Entity's obligations under this Agreement. Alternatively, Business Associate may choose to provide Covered Entity with written notice of the material breach. At its discretion, Business Associate may terminate this Agreement if Covered Entity has not cured the breach within thirty (30) calendar days of receiving written notice from Business Associate.
- c. Return or Destruction of PHI. Upon termination of this Agreement for any reason, Business Associate shall destroy or, at Covered Entity's request, return all PHI received from Covered Entity or created or received by Business Associate on behalf of Covered Entity that Business Associate still maintains in any form. If

Business Associate destroys the PHI, Business Associate shall certify in writing to Covered Entity that such PHI has been destroyed. This provision applies to PHI that is in the possession of agents or subcontractors of Business Associate. Notwithstanding the foregoing, the parties acknowledge and agree that it is not feasible for Business Associate to return or destroy PHI due to the nature of Business Associate's products and services. Business Associate will retain the PHI, subject to all of the protections of this Agreement, and limit further uses and disclosures of the PHI to those purposes that make the return or destruction of the PHI infeasible for so long as Business Associate maintains the PHI.

## 6. MISCELLANEOUS

- a. References to Privacy Rule or Security Rule. A reference in this Agreement to a section in the Privacy Rule or Security Rule means the section as in effect or as amended.
- b. Compliance with Laws. Business Associate will comply with all appropriate federal and state security and privacy laws to the extent that such laws apply to Business Associate and are more protective of Individual privacy than are the HIPAA laws.
- c. Changes in Law. If any modification to this BA Agreement is Required By Law or required by HITECH or any other federal or state law affecting this BA Agreement, or if Covered Entity reasonably concludes that an amendment to this Agreement is needed because of a change in federal or state law or changing industry standards, Covered Entity shall notify Business Associate of such proposed modification(s) ("Legally-Required Modifications"). The Parties will negotiate in good faith to address any such Legally Required Modifications.
- d. Amendment. Except as permitted by Section 5.3 above, this Agreement shall not be amended, altered, or modified except by an instrument in writing duly executed by the Parties to this Agreement.
- e. Waiver. No delay or failure of either party to exercise any right or remedy available hereunder, at law or in equity, shall act as a waiver of such right or remedy, and any waiver shall not waive any subsequent right, obligation, or default. No modification of, addition to, or waiver of any right, obligation, or default shall be effective unless in writing and signed by the party against whom the same is sought to be enforced.
- f. Remuneration in Exchange for PHI. Business Associate will not directly or indirectly receive remuneration in exchange for any PHI of an Individual unless Covered Entity has received a valid authorization from the Individual or the exchange is otherwise permitted by law. As permitted by law, Covered Entity may provide remuneration to Business Associate for activities involving the exchange of PHI that Business Associate undertakes on behalf of and at the specific request of Covered Entity pursuant to an agreement.
- g. Limitations on Benefits of this Agreement. Nothing express or implied in this BA Agreement is intended to confer, nor shall anything herein confer, upon any person other than Covered Entity, Business Associate, or their respective successors or assigns, any rights, remedies, obligations, or liabilities whatsoever.
- h. Independent Contractors. The Parties are independent contractors and nothing in this BA Agreement shall be deemed to make them partners or joint-venturers.

- i. Notices. All notices which are required or permitted to be given pursuant to this BA Agreement shall be in writing and shall be sufficient in all respects if delivered personally, by electronic mail (with a confirmation by registered or certified mail placed in the mail no later than the following day), or by registered or certified mail, postage prepaid, addressed to a party as indicated below:

If to Business Associate:  
Palo Alto Networks  
Attn: General Counsel  
3000 Tannery Way  
Santa Clara, CA 95054

If to Covered Entity:  
Enter Company Name  
Attn: Enter Attention To  
Enter Company Street name and City  
Enter Company State, Postal Code and Country

Notice shall be deemed to have been given upon transmittal thereof as to communications which are personally delivered or transmitted by electronic mail and, as to communications made by United States mail, on the third (3rd) day after mailing. The above addresses may be changed by giving notice of such change in the manner provided above for giving notice.

- j. Severability. If any provision of this BA Agreement is determined by a court of competent jurisdiction to be invalid, void, or unenforceable, the remaining provisions hereof shall continue in full force and effect.
- k. Entire Agreement. This BA Agreement contains the entire understanding between the Parties hereto and shall supersede any other oral or written agreements, discussions, and understandings of every kind and nature, including any provision in any Contract.
- l. Interpretation. Any ambiguity in this BA Agreement shall be resolved in favor of a meaning that permits the Parties to comply with the applicable requirements of the Privacy Rule and Security Rule and any other requirements imposed by HIPAA or HITECH. Any conflict between a provision of the Contract and this BA Agreement regarding the subject matter of this BA Agreement shall be resolved in favor of this BA Agreement.
- m. Governing Law. This BA Agreement shall be governed by California law and applicable Federal law, without respect to its conflict of law principles.