



# UNIVERSITY OF CALIFORNIA

## APPENDIX – HIPAA BUSINESS ASSOCIATE

### ARTICLE 1 – GENERAL

- A. UC and Supplier desire to protect the privacy and provide for the security of Protected Health Information (as that term is defined herein) used by or disclosed to Supplier in compliance with the Health Insurance Portability and Accountability Act of 1996 (HIPAA), the regulations promulgated thereunder by the U.S. Department of Health and Human Services (45 CFR Parts 160, 162 and 164, the HIPAA Regulations), the Health Information Technology for Economic and Clinical Health Act of 2009 (the HITECH Act), California Health and Safety Code §1280.15, California Civil Code §§1798.82 and 1798.29, and other applicable laws and regulations. The purpose of this Appendix is to satisfy certain standards and requirements of HIPAA, the HIPAA Regulations, including 45 CFR § 164.504(e), and the HITECH Act, including Subtitle D, part 1, as they may be amended from time to time.
- B. Supplier is or may be a Business Associate as defined under HIPAA. UC wishes to disclose to Supplier certain information, some of which may constitute Protected Health Information or Medical Information. UC has designated all of its HIPAA health care components as a single component of its hybrid entity and therefore this Appendix is binding on all other UC health care components (collectively, the Single Health Care Component or the SHCC). This Appendix is effective on the date of the Agreement under which Supplier provides Services to UC (Effective Date).
- C. This Appendix applies only if and to the extent Supplier is functioning as a Business Associate to the SHCC.

### ARTICLE 2 – DEFINITIONS

- A. "Agent" means persons or entities, including sub-suppliers, who have an agency relationship to Supplier and who have been approved in advance by UC.
- B. "Breach" means the unauthorized acquisition, access, use, or disclosure of PHI that 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, and shall have the meaning given to such term under HIPAA and the HIPAA regulations, including 45 CFR §164.402, as well as California Civil Code §§ 1798.29 and 1798.82.
- C. "Electronic Health Record" means an electronic record of health-related information on an individual that is created, gathered, managed, and consulted by authorized health care clinicians and staff, and shall have the meaning given to such term under the HITECH Act, including Section 13400(5).
- D. "Electronic PHI" means PHI that is transmitted by or maintained in electronic media and shall have the meaning given to such term under HIPAA and the HIPAA Regulations, including 45 CFR § 160.103. For the purposes of this Appendix, Electronic PHI includes all computerized data, as defined in California Civil Code §§ 1798.29 and 1798.82.
- E. "Information System" means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people, and shall have the meaning given to such

term under HIPAA and the HIPAA Regulations, including 45 CFR § 164.304.

- F. "Medical Information" means any individually identifiable information, in electronic or physical form, in possession of or derived from a provider of health care, health care service plan, pharmaceutical company, or contractor regarding a patient's medical history, mental or physical condition, or treatment and shall have the meaning given to such term under California Civil Code § 56.05.
- G. "PHI" means Protected Health Information and Medical Information, collectively.
- H. "Protected Health Information" means any information, including Electronic PHI, whether oral or recorded in any form or medium: (i) that relates to the past, present, or future physical or mental condition of an individual; the provision of health care to an individual; or the past, present or future payment for the provision of health care to an individual, and (ii) that identifies the individual or with respect to which there is a reasonable basis to believe the information can be used to identify the individual, and shall have the meaning given to such term under HIPAA and the HIPAA Regulations, including, but not limited to 45 CFR § 160.103. For the purposes of this Appendix, Protected Health Information includes all medical information and health insurance information as defined in California Civil Code §§ 56.05 and 1798.82.
- I. "Secretary" means the Secretary, Department of Health and Human Services, or his or her designee.
- J. "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, and shall have the meaning given to such term under HIPAA and the HIPAA Regulations, including 45 CFR § 164.304.
- K. "Unsecured PHI" means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of an Encryption or Destruction technology or methodology specified by the Secretary in guidance issued under Section 13402(h)(2) of the HITECH Act on the Health and Human Services Web site, as such guidance may be revised from time to time, and shall have the meaning given to such term under HIPAA and the HIPAA Regulations, including 45 CFR § 164.402.
  - 1. "Encryption" means a technology or methodology that utilizes an algorithmic process to transform data into a form in which there is a low probability of assigning meaning without use of a confidential process or key, and such confidential process or key that might enable decryption has not been breached, and shall have the meaning given to such term under HIPAA and HIPAA Regulations, including 45 CFR § 164.304.
  - 2. "Destruction" means the use of a technology or methodology by which the media on which the PHI is stored or recorded has been shredded, destroyed, cleared, or purged, as appropriate, such that the PHI cannot be read, retrieved, or otherwise reconstructed. Redaction is inadequate for the purposes of destruction.

## **ARTICLE 3 –SUPPLIER’S RESPONSIBILITIES**

- A. Permitted Uses and Disclosures of PHI. Supplier may use, access, and/or disclose PHI received by Supplier solely for the purpose of performing a function or activity for or on behalf of UC. To the extent Supplier carries out one or more of UC’s obligations under Subpart E of 45 CFR Part 164, Supplier must comply with the requirements of Subpart E that apply to UC in the performance of such obligation(s).
  - 1. Minimum Necessary. With respect to the use, access, or disclosure of PHI by Supplier as permitted under this Article 3, Supplier shall limit such use access, or disclosure, to the extent practicable, to the minimum necessary to accomplish the intended purpose of such use, access, or disclosure. Supplier shall determine what constitutes the minimum necessary to accomplish the intended purpose in accordance with HIPAA, HIPAA Regulations and any applicable guidance issued by the Secretary.

2. Documentation of Disclosures. With respect to any disclosures of PHI by Supplier as permitted under this Article 3, Supplier shall document such disclosures including, but not limited to, the date of the disclosure, the name and, if known, the address of the recipient of the disclosure, a brief description of the PHI disclosed, and the purpose of the disclosure.
  3. Modification of PHI. Except as permitted under Article 5.B, Supplier shall not modify any existing data to which it is granted access other than to correct errors, or derive new data from such existing data. Supplier shall record any modification of data and retain such record for a period of seven (7) years.
  4. Electronic Transaction Standards. Where applicable, Supplier shall adhere to the transaction standards as specified in 45 CFR §§ Parts 160 and 162.
- B. Other Permitted Uses and Disclosures of PHI. Supplier may, if necessary and only to the extent necessary, use PHI (i) for the proper management and administration of Supplier's business, (ii) to provide data aggregation services relating to UC's health care operations, or (iii) to carry out Supplier's legal responsibilities, subject to the limitation in Article 3.C. Supplier shall obtain reasonable assurances from the person to whom the PHI is being disclosed that, as required under this Appendix BAA, the PHI will be held confidentially and used or further disclosed only as required by law or for the purpose for which it was disclosed. Supplier shall require that any Breaches or Security Incidents be immediately reported to Supplier. Supplier shall then report the Breach or Security Incident to UC in accordance with Article 3.G.
- C. Nondisclosure of PHI. Supplier is not authorized and shall not use or further disclose UC's PHI other than as permitted or required under any agreement it has with UC, including this Appendix, or as required by law or regulation.
1. Disclosures Required by Law. In the event Supplier is required by law to disclose PHI, Supplier shall promptly notify UC of such requirement. Supplier shall give UC sufficient opportunity to oppose such disclosure or take other appropriate action before Supplier discloses the PHI.
  2. Legal Process. In the event Supplier is served with legal process or a request from a governmental agency that may potentially require the disclosure of PHI, Supplier shall promptly, and in any case within two (2) business days of its receipt of such legal process or request, notify UC. Supplier shall not disclose the PHI without UC's consent unless pursuant to a valid and specific court order or to comply with a requirement for review of documents by a governmental regulatory agency under its statutory or regulatory authority to regulate the activities of either party.
- D. Prohibition on Sale of PHI for Remuneration. Subject to the limitations set forth in Section 13405(d)(2) of the HITECH Act, Supplier shall not directly or indirectly receive remuneration in exchange for any of UC's PHI unless Supplier first obtains authorization from UC. UC shall not grant such authorization unless the subject of the PHI has granted UC a valid authorization that includes a specification of whether the PHI can be further exchanged for remuneration by the entity receiving the individual's PHI.
- E. Security Standards. Supplier shall take appropriate security measures (i) to protect the confidentiality, integrity and availability of UC's Electronic PHI information that it creates receives, maintains, or transmits on behalf of UC and (ii) to prevent any use or disclosure of UC's PHI other than as provided by the Agreement and this Appendix. Appropriate security measures include the implementation of the administrative, physical and technical safeguards specified in Subpart C of 45 CFR Part 164 of the HIPAA Security Rule.
- F. Security Documentation. Supplier shall maintain the policies and procedures implemented to comply with Article 3.E in written form (paper or electronic). If an action, activity or assessment is required to be documented, Supplier shall maintain a written record (paper or electronic) of the action, activity, or assessment, shall retain the documentation for six (6) years from the date of its creation or the date when

it last was in effect, whichever is later, make documentation available to those persons responsible for implementing the procedures to which the documentation pertains, and review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the PHI.

G. Notification of Breaches and Security Incidents. Supplier shall notify UC in writing as soon as possible, but in no event more than two (2) business days, after Supplier becomes aware of any Breach or Security Incident involving UC's PHI. Supplier shall be deemed to be aware of any Breach or Security Incident as of the first day on which such Breach or Security Incident is known or reasonably should have been known to its officers, employees, agents or subcontractors. Supplier shall identify as soon as practicable each individual whose unsecured PHI has been, or is reasonably believed by Supplier to have been, accessed, acquired, or disclosed during such Breach or Security Incident. Supplier shall cooperate in good faith with UC in the investigation of any Breach or Security Incident.

H. Prompt Corrective Actions. In addition to the notification requirements in Article 3.G, and with prior notice to UC, Supplier shall take (i) prompt corrective action to remedy any Breach or Security Incident, (ii) mitigate, to the extent practicable, any harmful effect of a use or disclosure of PHI by Supplier, and (iii) take any other action required by applicable federal and state laws and regulations pertaining to such Breach or Security Incident.

1. Notification of Corrective Action and Provision of Policies. Supplier shall provide written notice to UC as soon as possible but no later than twenty (20) calendar days after discovery of the Breach or Security Incident of (i) the actions taken by Supplier to mitigate any harmful effect of such Breach or Security Incident and (ii) the corrective action Supplier has taken or shall take to prevent future similar Breaches or Security Incidents. Upon UC's request, Supplier will also provide to UC a copy of Supplier's policies and procedures that pertain to the Breach or Security Incident involving UC's PHI, including procedures for curing any material breach of this Appendix.

2. Lost or Indecipherable Transmissions. Supplier agrees to make reasonable efforts to trace lost or translate indecipherable transmissions. Supplier shall bear all costs associated with the recreation of incomplete, lost or indecipherable transmissions if such loss is the result of an act or omission of Supplier.

I. Indemnity by Supplier. Supplier will defend, indemnify, and hold harmless UC, its officers, employees, and agents, from and against all losses, expenses (including, without limitation, reasonable attorneys' fees and costs), damages, and liabilities of any kind resulting from or arising out of the Agreement, including the performance hereunder of Supplier, its officers, employees, or agents, in proportion and to the extent that such losses, expenses, damages and liabilities are due or claimed to be due to the negligent acts or omissions of Supplier, its officers, employees, or agents. UC agrees to provide Supplier with prompt notice of any such claim or action and to permit Supplier to defend any claim or action, and that UC will cooperate fully in such defense. UC retains the right to participate in the defense against any such claim or action, and the right to consent to any settlement, which consent will not unreasonably be withheld. This Indemnity supersedes the Indemnity provision in the UC Terms and Conditions for Services or UC Terms and Conditions for Goods and Services, as the case may be.

J. Right of UC to Accounting or Audit. Within fifteen (15) calendar days of UC's request, Supplier shall provide, at Supplier's expense, an audit or written accounting of the uses and disclosures of UC's PHI made by Supplier and its agents, if: (i) UC receives credible information that there has been a Breach or Security Incident involving UC's PHI, or (ii) if UC determines in its sole discretion that the written notice provided in Article 3.H.1 does not provide sufficient assurances that the Breach or Security Incident involving UC's PHI has been remedied.

K. UC's Right to Terminate. If Supplier fails to provide the accounting or audit in a timely manner, or if UC is not satisfied that the corrective action is sufficient to reasonably prevent similar Breaches or Security Incidents in the future, UC may terminate its applicable agreements with Supplier in accordance with

Article 7, below.

- L. **Costs Related to Inappropriate Use, Access or Disclosure of PHI.** If Supplier fails to adhere to any of the privacy, confidentiality, and/or data security provisions set forth in this Appendix or any other agreement it has with UC or if there is a Security Incident or Breach of PHI in Supplier's possession and, as a result, PHI or any other confidential information is unlawfully accessed, used or disclosed, Supplier agrees to pay and reimburse UC for any and all costs, direct or indirect, incurred by UC associated with any Security Incident or Breach notification obligations. Supplier also agrees to pay for any and all fines and/or administrative penalties imposed for such unauthorized access, use or disclosure of confidential information or for delayed reporting if it fails to notify UC of the Breach or Security Incident as required by this Appendix. To the extent that this provision conflicts with the Indemnity provision above, this provision shall control.
- M. **Regulatory Compliance.** Supplier shall make its internal practices, books and records relating to the use, disclosure or security of PHI received from UC (or created or received by Supplier on behalf of UC) available to any state or federal agency, including the U.S. Department of Health and Human Services, for purposes of determining UC's and/or Supplier's compliance with federal/state privacy and security laws and regulations.
- N. **Inspection of Records.** Within thirty (30) calendar days after UC's written request, Supplier shall make available to UC and its authorized agents, during normal business hours, all facilities, systems, procedures, records, books, agreements, policies and procedures relating to the use and/or disclosure of UC's PHI for purposes of enabling UC to determine Supplier's compliance with federal and state privacy and security laws and regulations.
- O. **Compliance with Law.** In connection with all matters related to this Appendix, Supplier shall comply with all applicable federal and state laws and regulations, including, but not limited to, HIPAA, the HIPAA Regulations, 45 CFR §§ Parts 160, 162 and 164, and the HITECH Act, Subtitle D, part 1, California Civil Code §1798.29 and California Health and Safety Code §1280.15, as they may be amended from time to time.

## **ARTICLE 4 –UC'S RESPONSIBILITIES**

- A. **Indemnity by UC.** UC will defend, indemnify, and hold harmless Supplier, its officers, employees, and agents, from and against all losses, expenses (including, without limitation, reasonable attorneys' fees and costs), damages, and liabilities of any kind resulting from or arising out of the Agreement, including the performance hereunder of UC, its officers, employees, or agents, in proportion and to the extent that such losses, expenses, damages and liabilities are due or claimed to be due to the negligent acts or omissions of UC, its officers, employees, or agents. Supplier agrees to provide UC with prompt notice of any such claim or action and to permit UC to defend any claim or action, and that Supplier will cooperate fully in such defense. Supplier retains the right to participate in the defense against any such claim or action, and the right to consent to any settlement, which consent will not unreasonably be withheld.

## **ARTICLE 5 - Parties' Responsibilities with Respect to Rights of Individuals**

A. **Individual's Right to Request Restrictions of PHI.** Supplier shall notify UC in writing within five (5) business days after receipt of any request by individuals or their representatives to restrict the use and disclosure of the PHI Supplier maintains for or on behalf of UC. Upon written notice from UC that it agrees to comply with the requested restrictions, Supplier agrees to comply with any instructions to modify, delete or otherwise restrict the use and disclosure of PHI it maintains for or on behalf of UC.

B. **Individual's Request for Amendment of PHI.** Supplier shall inform UC within five (5) business days after receipt of any request by or on behalf of the subject of the PHI to amend the PHI that Supplier maintains for or on behalf of UC. Supplier shall, within twenty (20) calendar days after receipt of a written request,

make the subject's PHI available to UC as may be required to fulfill UC's obligations to amend PHI pursuant to HIPAA and the HIPAA Regulations, including, but not limited to, 45 CFR § 164.526. Supplier shall, as directed by UC, incorporate any amendments to UC's PHI into copies of such PHI maintained by Supplier.

C. Individual's Request for an Accounting of Disclosures of PHI. Supplier shall document all disclosures of PHI and, within twenty (20) calendar days after receipt of a written request, make available to UC, and, if authorized in writing by UC, to the subject of the PHI, such information maintained by Supplier or its agents as may be required to fulfill UC's obligations to provide an accounting for disclosures of UC's PHI pursuant to HIPAA, the HIPAA Regulations, including, but not limited to, 45 CFR § 164.528, and the HITECH Act, including, but not limited to Section 13405(c).

D. Electronic Health Records. If Supplier, on behalf of UC, uses or maintains Electronic Health Records with respect to PHI, UC may provide an individual, upon the individual's request, with the name and contact information of Supplier so that the individual may make a direct request to Supplier for an accounting of disclosures made by Supplier during the three (3) years prior to the date on which the accounting is requested or as otherwise provided under the HITECH Act Section 13405(c)(4)(A) or Section 13405(c)(4)(B).

E. Access to PHI by the Individual. If UC determines that an individual's PHI is held solely by Supplier or if Supplier is acting on behalf of UC to provide access to or a copy of an individual's PHI, Supplier shall, within five (5) calendar days after receipt of a written request, make available to UC, and, if authorized in writing by UC, to the subject of the PHI, such information as may be required to fulfill UC's obligations to provide access to or provide a copy of the PHI pursuant to HIPAA and the HIPAA Regulations, including, but not limited to, 45 CFR § 164.524.

F. Access to Certain Information in Electronic Format. If Supplier uses or maintains Electronic Health Records with respect to PHI on behalf of UC, Supplier shall, upon request of UC, provide UC with the requested Electronic Health Record in an electronic format.

## **ARTICLE 6 – Supplier's Agents**

- A. Other than as expressly authorized herein, Supplier will provide UC's PHI only to persons or entities who are Agents. Supplier will provide PHI to Agents solely for the purposes of carrying out the Agreement.
- B. Supplier shall require such Agents to agree to the same restrictions and conditions that are imposed on Supplier by this Appendix, and to provide written assurance of such agreement, including, but not limited to, Articles 3.E (Security Standards), 3.F (Security Documentation) and 3.G (Notification of Breaches and Security Incidents).

## **ARTICLE 7 – TERMINATION AND OTHER REMEDIES**

- A. Material Breach. A breach by either party of any material provision of this Appendix shall constitute a material breach of any agreements between UC and Supplier. Either party, upon written notice to the other party describing the breach, may take any of the following actions:
  - 1. Terminate all applicable agreements, including this Appendix, immediately if the other party has breached a material term of this Appendix.
  - 2. Terminate the applicable agreements, including this Appendix, unless the other party, within five (5) business days, provides a plan to cure the breach and, within fifteen (15) business days, cures the breach;
  - 3. In the case of a material breach of the Appendix, if termination is not feasible, upon the non-breaching

party's request, the breaching party shall:

(a) at its expense, provide a third-party review of the outcome of any plan implemented under Article 7.A.2. to cure the breach;

(b) at its expense, submit to a plan of monitoring and reporting to demonstrate compliance with the Appendix.

- B. **Effect of Termination - Return or Destruction of PHI held by Supplier or Supplier's Agents.** Upon termination, expiration or other conclusion of the Appendix for any reason, Supplier shall return or, at UC's option, provide for the Destruction of all PHI received from UC, or created and received by Supplier on behalf of UC in connection with the Appendix, that Supplier and/or Supplier's agents and sub-suppliers still maintain in any form, and shall retain no copies of such PHI. Within thirty (30) calendar days after the termination of this Appendix, Supplier shall both complete such return or Destruction and certify in writing to UC that such return or Destruction has been completed.
- C. **Return or Destruction Not Feasible.** If Supplier represents to UC that return or Destruction of UC's PHI is not feasible, Supplier must provide UC with a written statement of the reason that return or Destruction by Supplier or its agents is not feasible. If UC determines that return or Destruction is not feasible, this Appendix shall remain in full force and effect and shall be applicable to any and all of UC's PHI held by Supplier or its agents.
- D. **Other Remedies.** Notwithstanding the foregoing rights to terminate the Agreement, UC shall have such other remedies as are reasonably available at law or equity, including injunctive relief.
- E. **Civil and Criminal Penalties.** Supplier understands and agrees that it is subject to civil or criminal penalties applicable to Supplier for unauthorized use, access or disclosure of PHI in accordance with the HIPAA Regulations and the HITECH Act.

## **ARTICLE 8 – CHANGES TO THIS APPENDIX**

- A. **Compliance with Law.** The parties acknowledge that state and federal laws and regulations relating to electronic data security and privacy are rapidly evolving and that additional obligations and responsibilities may be imposed on Supplier to ensure compliance with the new laws and regulations. The parties specifically agree to comply with all applicable laws and regulations and take such action as may be necessary to implement the standards and requirements of HIPAA, the HIPAA Regulations, the HITECH Act, and other applicable state and federal laws and regulations relating to the security or confidentiality of PHI, without need to amend or modify this Appendix. UC will update this Appendix from time to time as required by applicable laws and regulations, and Supplier agrees to sign a revised Appendix upon UC's reasonable request.

## **ARTICLE 9 – INSURANCE**

- A. **Insurance.** In addition to any general and/or professional liability insurance coverage required of Supplier under the Agreement, Supplier agrees to obtain and maintain, at its sole expense, liability insurance on an occurrence basis, covering any and all claims, liabilities, demands, damages, losses, costs and expenses arising from a breach of the security, privacy, or confidentiality obligations of Supplier, its officers, employees, agents and subcontractors, under this Appendix. Such insurance coverage shall be maintained for the term of the Agreement, and a copy of such policy or a certificate evidencing the policy shall be provided to UC at UC's request.

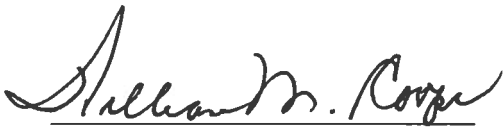
## **ARTICLE 10 – MISCELLANEOUS PROVISIONS**

- A. Assistance in Litigation or Administrative Proceedings. Supplier shall make itself, and any employees or agents assisting Supplier in the performance of its obligations under this Appendix, available to UC at no cost to UC to testify as witnesses, or otherwise, in the event of litigation or administrative proceedings against UC, its directors, officers, agents or employees based upon claimed violation of HIPAA, the HIPAA Regulations or other laws relating to security and privacy.
- B. Order of Precedence. To the extent that the terms of any other agreement(s) between UC and Supplier are inconsistent with the terms of this Appendix, the terms of this Appendix will control.
- C. Survival. The obligations of Supplier under Articles 3.C, 3.D, 3.E, 3.F, 3.G, 3.H, 3.I, 3.J, 3.L, 4.A, 5, 7.B, 7.C, 7.E, and 10.A of this Appendix shall survive the termination of any agreement between UC and Supplier.

The Appendix is signed below by the parties' duly authorized representatives.

**THE REGENTS OF THE  
UNIVERSITY OF CALIFORNIA**

**SUPPLIER**



(Signature)

William M. Cooper  
(Printed Name, Title) AVP & EPO

2/12/16  
(Date)

\_\_\_\_\_  
(Supplier Name)

\_\_\_\_\_  
(Signature)

\_\_\_\_\_  
(Printed Name, Title)

\_\_\_\_\_  
(Date)