## ATTACHMENT C

## NOTIFICATION OF BREACH

### A. Definitions

1. Breach shall have the meaning given to such term under HIPAA, the HITECH Act, the HIPAA regulations and the Final Omnibus Rule.

2. Electronic Health Record shall have the meaning given to such term in the HITECH Act, including, but not limited to, 42 U.S.C section 17921 and implementing regulations.

3. Electronic Protected Health Information (ePHI) means individually identifiable health information transmitted by electronic media or maintained in electronic media, as set forth in 45 CFR section 160.103.

4. Individually Identifiable Health Information means health information, including demographic information collected from an individual, that is created or received by a health care provider, health plan, employer or health care clearinghouse, and relates to the past, present or future physical or mental health or 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, that identifies the individual or where there is a reasonable basis to believe the information can be used to identify the individual, as set forth under 45 CFR section 160.103.

5. Privacy Rule shall mean the HIPAA Regulations that are found at 45 CFR Parts 160 and 164, Subparts A, D and E.

6. Personal Information shall have the meaning given to such term in Civil Code section 1798.29.

7. Protected Health Information means individually identifiable health information that is transmitted by electronic media, maintained in electronic media, or is transmitted or maintained in any other form or medium, as set forth in 45 CFR section 160.103.

8. Required by law, as set forth in 45 CFR section 164.103, means a mandate contained in law that compels an entity to make a use or disclosure of PHI that is enforceable in a court of law. This includes, but is not limited to, court orders and court-ordered warrants, subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information, and a civil or an authorized investigative demand. It also includes Medicare conditions of participation with respect to health care providers participating in the program, and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

9. Security Incident means the attempted or successful unauthorized access, use, disclosure, modification, loss or destruction of PHI or PI, or confidential data that is essential to the ongoing operation of the User's organization and intended for internal use; or interference with system operations in an information system.

10. Secretary means the Secretary of the U.S. Department of Health and Human Services (HHS) or the Secretary's designee.

11. Security Rule shall mean the HIPAA regulations that are found at 45 CFR Part 164, Subparts A and C.

12. Unsecured PHI shall have the meaning given to such term under the HITECH Act, 42 U.S.C. section 17932(h), any guidance issued pursuant to such Act, the HIPAA regulations and the Final Omnibus Act.

**B. Breaches and Security Incidents:**

1. ***Notice to DHCS.*** (1) To notify DHCS **immediately** upon the discovery of a suspected security incident that involves data provided to DHCS by the Social Security Administration. This notification will be **by telephone call plus email or fax** upon the discovery of the breach. (2) To notify DHCS **within 24 hours by email or fax** of the discovery of unsecured PHI or PI in electronic media or in any other media if the PHI or PI was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, any suspected security incident, intrusion or unauthorized access, use or disclosure of PHI or PI in violation of this Agreement and this Addendum, or potential loss of confidential data affecting this Agreement. A breach shall be treated as discovered by Business Associate as of the first day on which the breach is known, or by exercising reasonable diligence would have been known, to any person (other than the person committing the breach) who is an employee, officer or other agent of Business Associate.

   Notice shall be provided to the DHCS Program Contract Manager, the DHCS Privacy Officer and the DHCS Information Security Officer. If the incident occurs after business hours or on a weekend or holiday and involves data provided to DHCS by the Social Security Administration, notice shall be provided by calling the DHCS EITS Service Desk. Notice shall be made using the "DHCS Privacy Incident Report" form, including all information known at the time. Business Associate shall use the most current version of this form, which is posted on the DHCS Privacy Office website (www.dhcs.ca.gov, then select "Privacy" in the left column and then "Business Use" near the middle of the page) or use this link:

   http://www.dhcs.ca.gov/formsandpubs/laws/priv/Pages/DHCSBusinessAssociatesOnly.aspx

   Upon discovery of a breach or suspected security incident, intrusion or unauthorized access, use or disclosure of PHI or PI, Business Associate shall take:

   a. Prompt corrective action to mitigate any risks or damages involved with the breach and to protect the operating environment; and

b. Any action pertaining to such unauthorized disclosure required by applicable Federal and State laws and regulations.

2. ***Investigation and Investigation Report.*** To immediately investigate such security incident, breach, or unauthorized access, use or disclosure of PHI or PI. Within 72 hours of the discovery, User shall submit an updated "DHCS Privacy Incident Report" containing the information marked with an asterisk and all other applicable information listed on the form, to the extent known at that time, to the DHCS Program Contract Manager, the DHCS Privacy Officer, and the DHCS Information Security Officer.

3. ***Complete Report.*** To provide a complete report of the investigation to the DHCS Program Contract Manager, the DHCS Privacy Officer, and the DHCS Information Security Officer within ten (10) working days of the discovery of the breach or unauthorized use or disclosure. If all of the required information was not included in either the initial report, or the Investigation Report, then a separate Complete Report must be submitted. The report shall be submitted on the "DHCS Privacy Incident Report" form and shall include a full, detailed corrective action plan, including information on measures that were taken to halt and/or contain the improper use or disclosure. If DHCS requests information in addition to that listed on the "DHCS Privacy Incident Report" form, User shall make reasonable efforts to provide DHCS with such information. If necessary, a Supplemental Report may be used to submit revised or additional information after the completed report is submitted, by submitting the revised or additional information on an updated "DHCS Privacy Incident Report" form.

4. ***Notification of Individuals.*** If the cause of a breach of PHI or PI is attributable to User or its subcontractors, agents or vendors, User shall notify individuals of the breach or unauthorized use or disclosure when notification is required under state or federal law and shall pay any costs of such notifications, as well as any costs associated with the breach. The notifications shall comply with the requirements set forth in 42 U.S.C. section 17932 and its implementing regulations, including, but not limited to, the requirement that the notifications be made without unreasonable delay and in no event later than 60 calendar days. The DHCS Program Contract Manager, the DHCS Privacy Officer, and the DHCS Information Security Officer shall approve the time, manner and content of any such notifications and their review and approval must be obtained before the notifications are made.

5. ***Responsibility for Reporting of Breaches.*** If the cause of a breach of PHI or PI is attributable to User or its agents, subcontractors or vendors, and User is a Covered Entity as defined under HIPAA and the HIPAA regulations, User is responsible for all required reporting of the breach as specified in 42 U.S.C. section 17932 and its implementing regulations, including notification to media outlets and to the Secretary. If a breach of unsecured PHI involves more than 500 residents of the State of California or jurisdiction, User shall notify the Secretary of the breach immediately upon discovery of the breach. If User has reason to believe that duplicate reporting of the same breach or incident may occur because its subcontractors, agents or vendors may report the breach or incident to DHCS in addition to User, User shall notify DHCS, and DHCS and User may take appropriate action to prevent duplicate reporting. The breach reporting requirements of this paragraph are in addition to the reporting requirements set forth in subsection 1, above.

6. ***Contact Information.*** To direct communications to the above referenced staff, the User shall initiate contact as indicated herein. The parties reserve the right to make changes to the contact information below by giving written notice to the User. Said changes shall not require an amendment to this Addendum or the Agreement to which it is incorporated.

| **DHCS Program Point of Contact** | **DHCS Privacy Officer** | **DHCS Information Security Officer** |
|---|---|---|
| See the Data Use Agreement for Program Point of Contact information | Privacy Officer<br>c/o: Office of HIPAA Compliance<br>Department of Health Care Services<br>P.O. Box 997413, MS 4722<br>Sacramento, CA 95899-7413<br><br>Email: privacyofficer@dhcs.ca.gov<br>Fax: (916) 440-7680<br><br>Telephone: (916) 445-4646 | Information Security Officer<br>DHCS Information Security Office<br>P.O. Box 997413, MS 6400<br>Sacramento, CA 95899-7413<br><br>Email: iso@dhcs.ca.gov<br>Fax: (916) 440-5537<br><br>Telephone:<br>ITSD Service Desk<br>(916) 440-7000 or<br>(800) 579-0874 |