CONTRACTOR RISK ASSESSMENT FORM

Contracted Provider Name/ Program:	
Date Initiated:	Date Completed:
Completed By:	
Contact Phone #:	
Contact E-mail:	
Program Director:	

Brief Description of Incident:

Risk Assessment:

Part I. Pre- Risk Assessment

This pre-assessment is meant to assist the DHS Privacy and Security Office in documenting the factors for consideration in the determination of whether breach notification is required under HIPAA.

1. Was PHI involved?	☐ Yes, PHI was involved	☐ No, PHI was not involved. (No breach reporting required under HIPAA)
2. Was PHI unsecured?	☐ Yes, PHI was unsecured.	☐ No, PHI was secured. (No breach reporting required under HIPAA)
3. Was there an acquisition, access, use or disclosure of PHI in a manner not permitted under HIPAA?	☐ Yes, there was an acquisition, access, use or disclosure of PHI not permitted under HIPAA. (excluding incidental disclosures but including violations of the "minimum necessary" standard)	☐ No, there was no violation of the HIPAA regulations. (No breach reporting required under HIPAA)

CONFIDENTIAL

4. Does an exception apply?	☐ Yes, an exception applies. (Select applicable exception below. No breach reporting required under HI PAA)	☐ No, an exception does not apply. (Proceed with further risk assessment)
45 CFR 164.402 (1)(i)	☐ Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part	
45 CFR 164.402 (1)(ii)	☐ Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part	
45 CFR 164.402 (1)(iii)	☐ A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.	

Part II. 5 Factor Risk Assessment
An acquisition, access, use, or disclosure of PHI in a manner not permitted by the HIPAA regulations is presumed to be a breach and must be reported unless the County (DHS Privacy and Security Office) demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the factors below.

Factor 1.	
45 CFR 164.402 (2)(i): *The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;*	**Consider the nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification if the PHI is de-identified**. Consider the nature of services (i.e. Mental Health, Substance Use Disorder, and STD). Consider whether the PHI could be used in a manner adverse to the subject of the record or to further the unauthorized recipient's interests. Consider the likelihood of re-identification of the information based on the context and ability to link information with other available information.
Document considerations of Factor 1:	

Factor 2.	
45 CFR 164.402 (2)(ii): *The unauthorized person who used the protected health information or to whom the disclosure was made;*	**Consider the unauthorized person who used or received the PHI.** This must be considered if the PHI was impermissibly used within the County/Department as well as when the PHI is disclosed outside of the County/Department. Consider whether this person has legal obligations to protect the information, for example, is the person a covered entity required to comply with HIPAA, a government employee or other person required to comply with other privacy laws? If so, there may be a lower probability that the PHI has been compromised. Also consider if the unauthorized person has the ability to re-identify the information.
Document considerations of Factor 2:	

Factor 3.	
45 CFR 164.402 (2)(iii): *Whether the protected health information was actually acquired or viewed;*	**Consider whether the PHI was actually acquired or viewed.** If electronic PHI is involved, this may require backend system log or forensic analysis to determine if the information as accessed, viewed, acquired, transferred, or otherwise compromised.
Document considerations of Factor 3:	

Factor 4.	
45 CFR 164.402 (2)(iv): *The extent to which the risk to the protected health information has been mitigated.*	**Consider the extent to which the risk to the PHI has been mitigated—for example, as by obtaining the recipient's satisfactory assurances that the PHI will not be further used or disclosed (through a confidentiality agreement or similar means) has been completely returned, or has been/will be destroyed.** The extent and efficacy of the mitigation must be considered when determining the probability that the PHI has been compromised. OCR notes that this factor, when considered in combination with the factor regarding the unauthorized recipient, may lead to different results (the County/ Department can rely on assurances of employees and contractors, but assurances from third-parties may not be sufficient).
Document considerations of Factor 4:	

Factor 5.	
Ca Civ. Code 1798.29(f): For purposes of this section, "breach of the security of the system" means unauthorized acquisition of computerized data that compromises the security, confidentiality, or integrity of personal information maintained by the agency. Good faith acquisition of personal information by an employee or agent of the agency for the purposes of the agency is not a breach of the security of the system, provided that the personal information is not used or subject to further unauthorized disclosure.	**Consider whether the notification of a breach is required under State law (Information Practices Act of 1977).** State law requires notification of a breach regardless of the results of this risk assessment. **Consider the personal involved:** According to IPA, "personal information" means individual's first name or first initial and last name **in combination** with any one or more of the following data elements *(also called "notice-triggering elements)* , when either the name or the data elements are not encrypted (*check below if any of the elements apply*): ☐ (A) Social security number. ☐ (B) Driver's license number or California identification card number. ☐ (C) Account number, credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account. ☐ (D) Medical information. ☐ (E) Health insurance information. ☐ (F) Information or data collected through the use or operation of an automated license plate recognition system, as defined in Section 1798.90.5 of IPA. ☐ (G) A user name or email address, in combination with a password or security question and answer that would permit access to an online account

	The Department/County may have reporting obligations pursuant to a Business Associate Agreement or other contract.	
Business Associate, Data Use Agreement and/or Confidentiality Agreement Provisions	If we are granted access to PHI, PII or other personal information through contract/ agreement; consider the scope of work for which we have been granted access. Consider the uses and disclosures permitted or prohibited in such agreement. Consider the reporting obligations pursuant to the agreement. Consider the indemnification provision of such agreement (*if any*) and contact County Counsel for review.	
Document considerations of Factor 5:		
Based on the factors above, is there a low probability that the PHI has been compromised?	☐ Yes, there is a low probability (No breach reporting required under HIPAA)	☐ No, there is not a low probability. (Breach reporting required under HIPAA)

Contractor Disposition:

Upon review of the above factors we consider this incident to be a breach of:

Federal Law- HIPAA: Yes ☐ No ☐

State Law- CA IPA: Yes ☐ No ☐

Please indicate how the incident has been mitigated (*to the extent possible*):

For County Use Only:

It has been determined that the incident/ suspected or actual breach must be reported to the following:

☐ Privacy/Security Official Specified in Agreement	☐ Attorney General (PII of 500+)
☐ DHCS	☐ HHS Secretary (PHI of 500+)

It has been determined that a breach of State or Federal Law has occurred: Yes ☐ No ☐

It has been determined that the County must initiate Breach Response: Yes ☐ No ☐

Reviewed by: _____ Date: _____