APPENDIX PR 12-B

HIPAA Breach Decision Tool and Risk Assessment Documentation Form

Hospitals and other health care providers may use this form when analyzing a potential health information privacy breach. This form will assist providers in documenting their consideration of the required factors and their decision whether breach notification is required under HIPAA. (This form does not need to be completed if the provider has already decided the breach needs to be reported to the patient and to DHHS.)

Hospitals should complete this form as best they can, understanding that the responses given to the questions below may change as more information becomes available. The terms used in this form shall be given the definitions assigned by HIPAA, not California law. Nothing in this form shall be construed as an admission in the event of litigation.

File #: _____

Name of person completing form: _____

Date incident occurred: _____ Date incident detected: _____

Brief summary of incident, including number of patients affected: _____

1. **Was protected health information (PHI) involved?** *(PHI is health information (including demographic information) that identifies, or there is a reasonable basis to believe it can be used to identify, the individual. Health information includes any information relating to the physical or mental health or condition of an individual, the health care provided to an individual, or payment for health care provided to an individual. PHI does not include employment records held by a hospital in its role as employer or PHI regarding a person who has been deceased for more than 50 years.)*

☐ Yes, PHI was involved. *Continue to Question 2.*

☐ No, PHI was not involved. No breach reporting required under HIPAA.

Describe the information involved: _____

2. **Was the PHI unsecured?** *("Unsecured PHI" means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of the U.S. Department of Health and Human Services in guidance, such as ecryption or destruction. The guidance can be found on the DHHS website at www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule/brguidance.html.)*

☐ Yes, the PHI was unsecured. *Continue to Question 3.*

☐ No, the PHI was secured. No breach reporting required under HIPAA.

Describe the PHI (for example, was it verbal, paper or electronic? Encrypted in compliance with NIST, password protected, other?): _____

3. **Was there an acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rule?** *(Providers should keep in mind that a violation of the "minimum necessary" standard is not permitted by the Privacy Rule. Providers should also keep in mind that a use or disclosure of PHI that is incident to an otherwise permissible use or disclosure and occurs despite reasonable safeguards and proper minimum necessary procedures is not a violation of the Privacy Rule. Providers may wish to consult legal counsel to determine if the acquisition, access, use or disclosure was permitted by the Privacy Rule.)*

☐ Yes, there was an acquisition, access, use or disclosure of PHI in a manner not permitted by the Privacy Rule. *Continue to Question 4.*

☐ No, there was no violation of the Privacy Rule. No breach reporting required under HIPAA.

Describe who acquired, accessed, used and/or disclosed the PHI, whether the person(s) was authorized or unauthorized, and how the PHI was acquired, accessed, used, or disclosed: _____

_____

_____

4. **Does an exception apply?** Check any box below that applies:

☐ **Exception A.** A breach does not include an unintentional acquisition, access, or use of PHI by a workforce member, or person acting under the authority of a covered entity or business associate, if it:

a. Was made in good faith; and

b. Was within the course and scope of authority; and

c. Does not result in further use or disclosure in a manner not permitted by the Privacy Rule. (Workforce" includes employees, volunteers, trainees, and other persons whose work is under the direct control of the entity, whether or not they are paid by the covered entity. A person is acting under the authority of a covered entity or business associate if he or she is acting on its behalf at the time of the inadvertent acquisition, access, use or disclosure.)

☐ **Exception B.** A breach does not include an inadvertent disclosure by a person who is authorized to access PHI at a covered entity or business associate to another person authorized to access PHI at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received is not further used or disclosed in a manner not permitted by the Privacy Rule.

☐ **Exception C.** A breach does not include disclosure of PHI where the provider or business associate has a good faith belief than the unauthorized person who received it would not reasonably have been able to retain the information. (For example, PHI sent in the mail and returned by the post office, unopened, could not reasonably have been read or otherwise retained by an unauthorized person. Or, if a nurse mistakenly hands a patient the discharge papers belonging to another patient, but quickly realizes her mistake and takes back the paperwork, the nurse can reasonably conclude that the patient could not have read or otherwise retained the information. These incidents would not constitute reportable breaches.)

☐ Yes, an exception applies. No breach reporting required under HIPAA.

☐ No, an exception does not apply. *Continue to Question 5.*

5. **Risk assessment.** An acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rule is presumed to be a breach and must be reported unless the covered entity demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the factors listed below. (Note: You MUST document your consideration of ALL of the factors listed below.)

Factor A. 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 whether the more sensitive financial information was involved, such as credit card numbers, social security numbers, or other information that increases the risk of identity theft or financial fraud. For clinical information, this may involve consideration of not only the nature of the services (mental health, STD, cosmetic surgery) but also the amount of detailed clinical information involved (diagnosis, medication, medical history, test results). Consider whether the PHI could be used in a manner adverse to the patient or to further the unauthorized recipient's own interests. Hospitals should also determine whether there is a likelihood that the PHI could be re-identified (if the PHI is de-identified) based on the context and the ability to link the information with other available information.)*

Describe the PHI involved, including identifiers and likelihood of re-identification (if the PHI is de-identified): _____

_____

_____

Consider whether PHI could be used in a manner adverse to the patient(s) or to further the unauthorized person's interests: _____

_____

_____

Factor B. Consider the unauthorized person who used or received the PHI. *(This factor must be considered if the PHI was impermissibly used within the facility as well as when the PHI is disclosed outside the facility. Consider whether this person has legal obligations to protect the information - for example, is the person a covered entity required to comply with HIPAA, or 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.)*

Describe who used or received the PHI, whether they have legal obligation to protect the PHI, and whether they can re-identify the PHI (if the PHI is de-identified): _____

_____

_____

Factor C. Consider whether the PHI was actually acquired or viewed. *(If electronic PHI is involved, this may require a forensic analysis of the computer to determine if the information was accessed, viewed, acquired, transferred, or otherwise compromised.)*

Describe whether the PHI was actually acquired or viewed (attach report from a computer forensic analyst, if one was obtained): _____

_____

_____

Factor D. 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. *(Hospitals should consider the extent and efficacy of the mitigation 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 in terms of the risk to PHI. For example, a hospital may be able to obtain and rely on the assurances of an employee, affiliated entity, business associate, or another covered entity that the person destroyed the information. However, such assurances from other third parties may not be sufficient.)*

Describe risk mitigation steps taken: _____

_____

_____

Factor E. Describe any other relevant factors (write "none" if appropriate): _____

_____

_____

Based on the factors noted above, is there a low probability that the PHI has been compromised?

☐ Yes (there is a low probability), thus **No** breach reporting required under HIPAA.

☐ No (there is not a low probability; there is a higher probability) thus breach reporting is required under HIPAA.

IMPORTANT NOTE: This tool is helpful only with respect to a decision whether reporting is required under federal law (HIPAA). State laws require notification of a breach as defined in state law regardless of the results of this risk assessment. *(See "IV. State Law: Breach of Computerized Data in Any California Business" and "V. State Law: Breach in a Licensed Health Care Facility" for information regarding notification under state law.)* A provider may also have reporting obligations pursuant to a business associate agreement or other contract.

Signature of person completing this form: _____

Title: _____ Date: _____