W-1702
(New 8/14)

STATE OF CONNECTICUT
DEPARTMENT OF SOCIAL SERVICES

RISK ASSESSMENT OF BREACH OF UNSECURED PROTECTED HEALTH INFORMATION (PHI)

(To be completed by Privacy Officer or Business Associate)

Entity Reporting: _____ **Date:** _____

Date of Breach: _____ **Date of Discovery:** _____ **# of Individuals Affected:** _____

Brief Description of the Incident:

1. Was PHI involved	If the information 1) identifies the person; AND 2) relates at least one piece of information about the individual's physical or mental condition (such as diagnosis); or the provision of health care (such as medication or hospitalization); or payment for health care (such as the name of a past, present or future medical insurance carrier, like Medicare, Medicaid), it is PHI	☐ Yes, PHI was involved. Continue to **question #2** ☐ No, PHI was not involved. No breach reporting required under HIPAA
2. Was the PHI unsecured?	If the information is not encrypted under the technology requirements, it is unsecured. i.e. Was secure email or fax used?	☐ Yes, PHI was unsecure. Continue to **question #3** ☐ No, PHI was secure. No breach reporting required under HIPAA
3. Was there an acquisition, access, use, or disclosure of PHI in a manner not permitted by the Privacy Rule?	Note: 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. E.g. a client overhears a worker discussing another client's case, provided reasonable efforts were made to avoid being overheard.	☐ 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 by HIPAA.

EXCEPTIONS

4. Determine if one of the exceptions below apply. No reporting is required under HIPAA if an exception 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 (DSS) or business associate, (DSS Contractor) if it:

(i) Was made in good faith; and

(ii) Was within the course and scope of authority; and

(iii) 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 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 worker mistakenly hands a client papers belonging to another client, but quickly realizes his/her mistake and takes back the paperwork, the worker can reasonably conclude that the client could not have read or otherwise retained the information. These incidents would not constitute reportable breaches.)

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

☐ No, an exception does not apply. **Continue to the Risk Assessment**

RISK ASSESSMENT

---

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 it is demonstrated 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.)

(i) **The nature and extent of the protected health information involved, including the types of identifiers and the likelihood of re-identification;** consider whether the PHI could be used in a manner adverse to the client or to further the unauthorized recipient's own interests. Consider whether 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

(ii) **The unauthorized person who used the protected health information or to whom the disclosure was made;** 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.

(iii) **Whether the protected health information was actually acquired or viewed; and**

(iv) **The extent to which the risk to the protected health information has been mitigated** - for example, as by obtaining the recipient's satisfactory assurances that the PHI will not be further used or disclosed, has been completely returned, or has been/will be destroyed.

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 notification required under HIPAA.

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

6. Has a law enforcement official advised that notification to the individual would impede a criminal investigation? ☐ **Yes** ☐ **No**

IMPORTANT NOTE: This tool is helpful only with respect to a decision whether notification is required under federal law (HIPAA). A Business Associate may also have reporting obligations pursuant to a Business Associate agreement or other contract. The DSS Commissioner may require notification even if there is a low probability that the PHI has been compromised.

RECOMMENDATION: ☐ **Notify Client** ☐ **Do Not Notify Client**
Justification:

Person submitting this report
Name:

Title/Organization:

Email: **Telephone:**

Send this report to: PrivacyOfficer.dss@ct.gov

Persons who are deaf or hard of hearing and have a TTD/TTY device can contact DSS at 1-800-842-4524.
Persons who are blind or visually impaired, can contact DSS at 1-860-424-5040.