STATE OF CONNECTICUT
DEPARTMENT OF SOCIAL SERVICES
PROGRAM INFORMATION BULLETIN

Kathleen M. Brennan (AHP)
Deputy Commissioner, Kathleen M. Brennan

Immediately
Effective Date

INFORMATION BULLETIN NO: 14-02

PROGRAMS: ALL

SUBJECT: Procedures for reporting Breaches of Personally Identifiable Information (PII) or Protected Health Information (PHI)

Overview	This information bulletin describes the standardized procedures that all staff and Business Associates (BA) will follow to report breaches of PII or PHI.
What is a Breach	The unauthorized use, disclosure, acquisition, access, or compromise of personally identifiable and/or protected health information, whether physical or electronic for an unauthorized purpose.
What is Personally Identifiable Information (PII)	Information that can be used to distinguish or trace an individual's identity such as an individual's first name or first initial and last name in combination with any one, or more, of the following data: (1) Social Security number; (2) driver's license number or state identification card number. Other common examples are date of birth, passport number or financial records.
What is Protected Health Information (PHI)	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
When Should a Breach be reported?	You should report both suspected and confirmed breaches as soon as they are discovered in order to begin remediation and investigation of any compromised information.

What should a DSS employee do if he or she suspects a breach?	All DSS employees must report possible breaches directly to their managers.
What action must the DSS manager take when he or she has been informed of a suspected breach?	Within one business day of obtaining the breach information, the manager shall e-mail or fax the complete W-1701 Report of Breach of Unsecure PHI or PII form, to the DSS Privacy Officer or legal counsel
What action will the privacy officer take after being informed of a suspected breach by DSS employee?	Within one more business day, the Privacy Officer with the manager will determine whether the improper use or disclosure is a breach. Not all improper disclosures are breaches but all improper disclosures of PHI are considered breaches pending an evaluation of the circumstances. If the disclosure is a breach the Privacy Officer will complete a risk assessment to determine if notification is required. If there is a high probability that the information was compromised, DSS, through the Privacy Officer or legal counsel, must notify all individuals affected by the breach as soon as possible, but no later than 60 days after the discovery of the breach.
What should a DSS Business Associate do if a breach is suspected?	The BA shall notify DSS of all breaches without delay, by completing the W-1701, Report of Breach of Unsecured PHI or PII form and emailing it to PrivacyOfficer.dss@ct.gov The BA shall also provide a risk assessment to the Privacy Officer by completing W-1702, Risk Assessment of Breach of PHI form. This should be completed without unreasonable delay and in no case later than 30 days after the breach is discovered. See BA agreement and contact for additional information.
What action will the privacy officer take after being informed of a suspected breach by a Business Associate?	The Privacy Officer will review the W-1701, Breach Report of PHI or PII form and the W-1702, Risk Assessment of Unsecured PHI provided by the BA to determine if notification is required.

Breach Notification/Resolution	Based on the risk assessment the Privacy Officer shall make recommendations to the commissioner on whether notification is required. The Commissioner has the discretion to notify the client even if it is not required by HIPAA The Privacy Officer will send a response to the manager/BA representative notifying him/her of the disposition of the case by completing W-1703 Breach Resolution form.

Disposition:	Please retain this bulletin for future use
Distribution:	DSS Staff and Business Associates
Responsible Unit:	Office of Legal Counsel, Regulations, and Administrative Hearings
	860-424-5391
Date Issued:	November 2014

WH