W-1701
(New 8/14)

STATE OF CONNECTICUT-DEPARTMENT OF SOCIAL SERVICES

REPORT OF BREACH OF UNSECURED PROTECTED HEALTH INFORMATION (PHI) or PERSONALLY IDENTIFIABLE INFORMATION (PII)

(To be completed by DSS Manager or Business Associate)

Entity Reporting: **Date:**

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

Brief Description of the Incident:

Actions taken in response to the breach to mitigate harm or prevent recurrence:

Breach Involved *(click to select)*	**Type of Breach** *(click to select)*	**Cause of Breach** *(click to select)*

Type of Personally Identifiable Information involved in the incident (Select all that apply):

☐	**Social Security Numbers**	☐	**Date of Birth**	☐	**Personal Phone Number**
☐	**Names**	☐	**PHI (health information)**	☐	**Client Number**
☐	**Home addresses**	☐	**Financial information *(specify)***	☐	**Other *(Specify)***

If information was sent electronically was secure email or fax used? ☐ **Yes** ☐ **No**

Name of Person submitting this report:

Title/Organization:

Email: **Phone Number:**

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.

INSTRUCTIONS FOR COMPLETING FORM W- 1701
BREACH OF UNSECURED PROTECTED HEALTH INFORMATION
or
PERSONALLY IDENTIFIABLE INFORMATION REPORT

GENERAL INFORMATION

The employee will contact his or her manager to report disclosures that violate the Privacy Rule. These improper disclosures may include incidents such as but not limited to:

- Sending unsecure email containing client information
- Faxing client information to the wrong person
- Mailing client information to the wrong address
- Verbally providing client information to an unauthorized person
- Accessing client information for personal use
- Losing client information in a public place

The manager will obtain as much factual information as possible about the details of the improper disclosure to complete this form.

Date of Breach: enter the date the breach occurred

Date Breach Discovered: enter the date the breach was initially discovered by an employee

Entity Reporting: Enter "DSS" or the name of the Business Associate

DESCRIPTION OF THE INCIDENT:
Summarize the facts or circumstances of the theft, loss or compromise of PII or PHI including:

- to whom and when was the disclosure made
- what was the content of the disclosure
- if it was a paper or electronic disclosure ; if electronic was it sent securely, within the State system firewall

ACTIONS TAKEN IN RESPONSE TO THE BREACH:

- Summarize steps taken to mitigate actual or potential harm to the affected individuals and the organization. For example training, disciplinary action, policy modification, systems modification
- List findings form the investigation of the breach
- What steps were taken to have the improperly disclosed PHI/PII destroyed or returned to DSS

Breach Involved: Select form the drop-down list, Email, Info Dissemination, Paper Records or Equipment

Type of Breach: Select from the drop-down list, theft loss or compromise

Cause of Breach: Select from the drop-down list, Failure to follow policy, Failure to Safeguard Equipment or Information, Improper Security settings, or other

Type of Personally Identifiable Information involved: select all that apply. If financial information is selected provide additional details in the summary.

For assistance contact the Privacy Officer at 860-424-5391