

INSTRUCTIONS TO FILL OUT BREACH REPORT FORM

Sections of the Breach Report Form are in bold font and instructions are in normal font. Please complete this form for all suspected breaches that occur. (A suspected breach is defined as an alleged infraction or violation of a standard that may result in unauthorized disclosure of confidential information.) Please refer to the HIV/STD Breach of Confidentiality Response Policy for more information on method and timing of submittal of this form.

Section 1: Initial Report:

Per the HIV/STD Program Breach of Confidentiality Response Policy, the DSHS staff member who received the initial notice of the suspected breach will document the incident by completing *Section 1: Initial Report* of this form.

Type of Breach

Put a check mark in the box that closest describes the type of breach that may have occurred.

Unauthorized Release of Information

Accidental or purposeful release of data— verbally, electronically, or by paper medium - to an entity or person that by law does not have a right or need to know.

Unauthorized Access to Information

Purposeful access of data - either in person or electronically – by an entity or person that by law does not have a right or need to know.

.....

Date and Time of Breach

Date: _____ **Time:** _____

Type in the date and time the suspected breach actually occurred. If uncertain of the exact date or time, use a best estimate.

.....

Location Where the Breach Occurred

Organization Name _____

Type in the Agency, Unit, Company, Group or Other Title that best describes the business affiliation of the location where the suspected breach occurred.

Address _____ **City** _____ **State** _____

Type in the physical address of where the suspected breach occurred, including: street, building or room numbers, suites, etc.

Type of Data that was compromised

Put a checkmark in the box that best describes the type of data that may have been breached:

Personally Identified Individual Record-Level Data: Defined in the *Release of HIV/AIDS and STD Data Policy* as: Individual patient records that contain personal identifiers. A personal identifier is a datum or collection of data which allows the possessor to determine the identity of a single individual with a specified degree of certainty. A personal identifier may permit the identification of an individual within a given database. Bits of data, when taken together, may be used to identify an individual. Personal identifiers may include name, address or place of residence, social security number, telephone number, fax number, and exact date of birth.

Pseudo-anonymized Data: Defined in the *Release of HIV/AIDS and STD Data Policy* as: Individual record-level data which has been stripped of personal identifiers (e.g., name, address, social security number) but may contain potentially identifying information (e.g., age, sex, race/ethnicity, locality information) that when combined with other information may identify an individual. If the combining of information could identify an individual, these data are considered confidential.

Aggregate Data: Defined in the *Release of HIV/AIDS and STD Data Policy* as: Data which are based on combining individual level information. Aggregate data may contain potentially identifying information, particularly if the aggregated data are very detailed or for a small subset of individuals.

Means of Unauthorized Access or Release of Information

Put a checkmark in the box (es) that best describe the method(s) by which the suspected breach occurred. See the *HIV/STD Confidential Information Security Policy* for more specific information regarding each of these methods.)

- Building security Field investigation Workstation Handling confidential mail
- Telephone Electronic data storage Electronic data transmission Faxing (facsimile) records
- Email Routine sharing of data Laptops Removable storage devices
- GPS systems Personal storage devices Wi-Fi/blue tooth Other: _____

Contact information for the persons involved with the suspected breach:

Person Submitting This Report

Name: _____ **Agency/Affiliation:** _____

Full name of the DSHS staff reporting the suspected breach (on behalf of the person who witnessed or discovered the suspected breach); and the Agency, Unit, Company, Group or Other Title that best describes their business affiliation.

Work Phone _____ **E-Mail Address** _____

Telephone number and E-mail address where this person can be reached during daytime hours.

Date Submitted _____ **Time Submitted** _____

Date and the Time of Day the Breach Report Form was filled out and submitted.

Signature _____ **Title** _____

Signature and job title of the person that is reporting the suspected breach.

Person Who Released the Unauthorized Information

Name: _____ **Agency/Affiliation:** _____

Full name of the person suspected of releasing unauthorized information and the Agency, Unit, Company, Group or Other Title that best describes their business affiliation.

Work Phone _____ **E-Mail Address** _____

Telephone number and E-mail address where this person can be reached during daytime hours.

Title _____

Job title of the person suspected of releasing unauthorized information.

Describe the Suspected Breach of Protocol that Occurred

Write a brief description of the suspected breach as it occurred. Include how the breach was discovered and any other relevant information.

Describe Contributing Causes to the Incident

Write the specific cause(s) that contributed to the suspected breach. (For example, policies and procedures were not followed, policies and procedures were not enforced, and/or training was not adequate.)

Section 2: Security Team Closing Report

Per the HIV/STD Program Breach of Confidentiality Response Policy, the Security Team will be responsible for completing *Section 2: Security Team Closing Report* of this form.

In answering the following questions see the *HIV/STD Breach of Confidentiality Response Policy* for definitions.

Did a breach in protocol occur? Yes or No

Did a breach in confidentiality occur? Yes or No

Was the breach due to negligence or was it purposeful in nature? Negligence or Purposeful

Has the confidential information been compromised? Yes No Unknown

If yes, what information has been compromised?

If no, please elaborate on your response.

Security Team Conclusions/Recommendations:

Conclusions:

Write the conclusions set forth by the Security Team.

Immediate Recommendations:

Write the immediate corrective actions to be taken.

Long-Term Recommendations:

Write the long-term corrective actions to be taken.

Is follow-up action needed: Yes or No

Select only one response.

Section 3: Follow-up Report

This section is to be completed by the Group Manager/External LRP.

Were any disciplinary actions or corrective actions taken to prevent the breach from occurring again?

Yes or No (Select only one response.)

If yes, please describe the disciplinary and/or corrective actions that have been taken monthly to prevent the breach from occurring again. (Provide a monthly update to the LRP until the LRP determines no further action is needed and the LRP closes out the report.)

Sign-off from Security Team Member(s)

This incident has been investigated, the proper officials have been notified, and the corrective actions have been implemented in the event a breach has been confirmed.

Security Team Member Signature: _____
(Group Manager/External LRP) (Signature)

Date: _____

Typed Name: _____

(Sign-off from Management)

I have reviewed and approved the resolution of this investigation and actions taken.

Internal LRP Signature: _____
(Signature)

Date: _____

Typed Name: _____

Internal LRP Signature: _____
(Signature)

Date: _____

Typed Name: _____