Sample Data Breach in Personally Identifiable Information (PII)

Policies and Procedures

Washington State Coalition Against Domestic Violence

All services provided by this Program are confidential. The Program recognizes the very personal and private nature of the information that may be shared by those dealing with the trauma of domestic and sexual violence. The Program is committed to honoring the choices of survivors and to provide services in a manner that facilitates client empowerment. The Program will take all necessary steps under this policy and federal law to preserve the privacy rights of those who receive its services, unless expressly authorized by the client to do otherwise.

Records kept for the purpose of providing advocacy to survivors will contain minimal information specifically designed to provide continuity of services and supportive assistance. Information is only documented to the extent necessary to provide services.

Personally Identifiable Information (PII) is defined as *information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Some information that is considered to be PII is available in public sources such as telephone books, public websites, and university listings. This type of information is considered to be Public PII and includes, for example, first and last name, address, work telephone number, email address, home telephone number, and general educational credentials. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. Non-PII can become PII whenever additional information is made publicly available, in any medium and from any source, that, when combined with other available information, could be used to identify an individual.*

Data Breach: Unauthorized access to, unauthorized acquisition of, or accidental release of personal information that compromises the security, confidentiality, or integrity of the personally identifying information (PII) constitutes a data breach.

- Reasonable attempts shall be made to notify clients whose PII has been compromised or released without authorization.
- The Director or designee will notify the Department of Criminal Justice Services (DCJS) Information Security Officer and assigned grant monitor within 24 hours of identification of the actual or imminent PII breach.
- Concurrent to the actions outlined above, steps shall be taken to restore data, reinforce security and to return all systems to full operation as soon as possible.

Data Breach Procedure

Unauthorized access to, unauthorized acquisition of, or accidental release of personal information that compromises the security, confidentiality, or integrity of PII constitutes a data breach.

Identification of a Data Breach

The Director will be notified upon identification of an actual or suspected PII breach of data. Notification shall occur as soon as possible and not more than 24 hours following the discovery of a PII data breach. The program will conduct a notification to affected parties as described in the notification procedures.

Notification of a Data Breach

Reasonable attempts shall be made to notify clients whose PII has been compromised or released without authorization. A program staff person, in coordination with the director, will attempt to notify the survivor that their PII has been disclosed.

The program staff should discuss with the survivor what information or records were breached, explain the program policy and procedure, engage in safety planning as appropriate, and provide any additional information about the [insert organization name]'s plan to address the breach and contain further breach or exposure of the survivor's information.

The Director or designee will notify the Department of Criminal Justice Services (DCJS) Information Security Officer and assigned grant monitor, within 24 hours of identification of the actual or imminent PII data breach.

The actual PII will not be disclosed to DCJS in the notification but shall include the extent of the data breach (for example: 1 survivor's PII accidentally released or a database breach of entire agency client records).

Concurrent to the actions outlined above, steps shall be taken to restore data, reinforce security and to return all systems to full operation as soon as possible. All staff will be advised of this policy which will be updated as needed. The Director or designee will investigate the data breach cause and notify DCJS once a resolution has been completed. This may involve working with an IT person to install malware-blocking software, replacing equipment, or changing the locks to an office or file cabinet. In the event the breach involves paper copies of documents, immediate steps shall be taken to recover and secure all remaining documents.