FIRST THINGS FIRST

Data Security, Submission and Suppression Guidelines and Requirements for Collaborators

Background

The purpose of the Arizona Early Childhood Development and Health Board (First Things First - FTF) is to aid in the creation of a system that offers opportunities and support for families and communities in the development of all children, so they can grow up healthy and ready to succeed. Our work is accountable and transparent to decision-makers and the citizens of Arizona. Collaboration and direct funding of grantees to undertake work on behalf of the children and families of Arizona is fundamental to the purpose and mission of FTF. Submission and reporting of data related to funded work is an important part of ensuring accountability and maximum positive impact for young children.

Scope

This Data Security, Submission and Suppression Guidelines and Requirements for Collaborators pertains to data collected by or shared with a grantee, governmental entity, or vendor ("collaborator") while assisting with an FTF needs and assets report, conducting an FTF-funded program or service, or performing research services on behalf of FTF.

Data Security Policy

Collaborators must ensure that the data is maintained in a secure manner. Collaborator data is likely to contain highly sensitive information on individuals, their education and their health. Therefore, all collaborators must have a data security policy in force that identifies how the organization ensures that data is protected in all its forms, during all phases of its life cycle, from inappropriate access, use, modification, disclosure, or destruction. FTF has the right to review and request changes to a collaborator's policy. All collaborators subject to HIPAA, FERPA, tribal law, or other data regulation are required to comply with those laws.

Data Classification

FTF classifies data by three levels:

- **Public data**
- **Limited distribution data**
- **Confidential data**

Public data is data that is readily available in the public sphere, such as websites, publications, or other widely used sources. Public data includes both data published by FTF (e.g., needs and assets reports and impact reports) and data that has been officially released by an organization and is able to be located and verified by any interested party utilizing the complete citation (e.g., census data). Public data also includes aggregated data, except where the aggregated data constitutes limited distribution data.

Limited distribution data is aggregated data that does not identify individuals, but which may be of sufficiently small cell size that its dissemination poses a reasonable risk to the anonymity of any individual. Limited distribution data may be subject to HIPAA, FERPA, tribal law, or other data regulation.

Confidential data is non-public data that identifies individuals or is governed by agreements or laws that limit its viewing, analysis, or dissemination. Confidential data may also include confidential business information. Confidential data may be subject to HIPAA, FERPA, tribal law, or other data regulation.

Data Submission to FTF

FTF wants to ensure that resources allocated have maximum impact for the benefit of children and families. To ensure this accountability, FTF has established data reporting requirements for collaborators. All collaborators will regularly submit reports as identified in their contract with FTF.

Collaborators Conducting an FTF-Funded Program or Service

Collaborators may submit **public data** and **limited distribution data** to FTF through the FTF Partner Grant Management System (PGMS). Subsequent to the award of a contract, FTF will provide the collaborator with general training on login and navigation within PGMS. With this login, the collaborator will be able to manage its contract information. FTF will also provide additional training on strategy-specific data submission requirements. Because PGMS is located in a secure extranet environment, collaborators using PGMS for data submission are not required to undertake additional security measures related to their data submission above those identified in the general and strategy-specific data submission orientations (password and login security, guidelines for upload of narrative and other reports).

Collaborators submitting **public data**, **limited distribution data** and/or **confidential data** may submit their data, with an agreement between the collaborator and FTF, through an established secure web service or FTP (File Transfer Protocol) site via the internet, rather than a PGMS web-based entry form. Collaborators that submit data through the secure web service must submit data within the established data structures and format, follow all login procedures, submit a formal data change request form if needed, and ensure that confidential data may not be intercepted or viewed at any time by parties other than the collaborator and FTF. Additionally, collaborators must ensure that throughout the reporting and submission process that the data is secured and that any confidential data is encrypted and/or de-identified.

Collaborators Assisting with a Needs and Assets Report or Performing Research Services on Behalf of FTF

Collaborators usually submit their data to FTF through an established secure web service or FTP (File Transfer Protocol) site. Collaborators must follow the more specific data submission requirements in their contracts with FTF. To the extent a contract does not provide more specific submission requirements, collaborators must seek and receive approval of their data submission method from FTF.

All Collaborators

All collaborators must be prepared for FTF review of client-level data (e.g., child-level, professional-level, or early care and education provider-level) during on-site visits. Additionally, FTF data reporting requirements may include submission of client-level data. Collaborators agree to allow FTF to access such data. Should the data be subject to HIPAA, collaborators agree to enter into FTF's HIPAA Business Associate or Data Use Agreement as appropriate.

Beneficiary Permission for FTF Review

When a collaborator plans to obtain first-hand data from an individual, such as when conducting a program, providing a service, or conducting in-person research, the collaborator must inform the individual of FTF's reporting requirements. For instance, if the collaborator uses an enrollment form, the form should include the following statement: "I grant permission to [collaborator's name] to release my background, service, and impact related information to the Arizona Early Childhood Development and Health Board, also known as First Things First, which is funding this program or service." The collaborator warrants to FTF that prior to entering into the Agreement for FTF funding it has appropriately enquired and satisfied itself that it has the ability and authority comply with the requirements of this section.

Data Suppression Guidelines for Publications

Confidential and **limited distribution data** must not appear in publications. When a publication includes aggregate data, any limited distributed data must be suppressed. The statistical cutoff procedures help ensure that aggregated data does not put at risk the anonymity of any individual. FTF's intent is to avoid the possibility of inadvertently reporting personally identifiable information.

For data related to social service and early education programming, limited distribution data refers to counts of fewer than ten, excluding counts of zero (i.e., all counts of one through nine). Examples of social service and early education programming include the number of children served in TANF, AzMerit scores, and the number of children served with an IEP.

For data related to health or developmental delay, limited distribution data refers to counts of fewer than six, excluding counts of zero (i.e., all counts of one through five). Examples of health or developmental delay include the number of children without health insurance and the number of newborns admitted to an ICU.

Third-Party Sharing

Collaborators must not share collected data with individuals or parties other than FTF or the collaborator's contractor approved by FTF (see Collaborator Contractors section) or use the collected data for a non-FTF purpose without the prior written consent of FTF, except as follows. A collaborator that is an affiliate of an evidence-based model may share data with the organization that oversees the model as required by that organization. A collaborator providing a program or service under a grant from an entity other than FTF, such as the federal government, may share data with the other funding entity directly tied to that funding grant. Notwithstanding the foregoing, no data collected from tribal lands may be shared or used with any third-party without the appropriate tribal approvals and no data may be shared or used in violation of law.

Collaborator Contractors

All collaborators must contractually require any contractor used by them to assist with the collection, maintenance, submission, analysis or publication of data to comply with these Data Security, Submission and Suppression Guidelines and Requirements for Collaborators. In addition, collaborators must obtain advance written approval from FTF before using a contractor for any of these purposes.

Tribal Data

FTF recognizes Arizona tribes as sovereign nations that have the right to regulate research and data collection on their tribal lands. To this end, FTF is committed to obtaining all appropriate tribal approvals for data collection, analysis and reporting. Accordingly, collaborators must only collect, use and share data from tribal land with appropriate tribal approvals, which approval may require participation in cultural education and community orientation classes, and in accordance, as applicable, with FTF's Tribal Data Policy.

In the case of collaborators conducting an FTF-funded program or service, collaborators are responsible for obtaining the appropriate tribal approvals unless FTF notifies a collaborator in writing that FTF has already obtained the approvals. FTF Regional Directors and Tribal Affairs staff can provide support to collaborators in identifying and navigating each tribe's process and protocols.

In the case of collaborators assisting with a needs and assets report or performing research services on behalf of FTF, FTF staff will take the lead in securing appropriate tribal approvals for data collection. Collaborators need to assist FTF in this process as requested by FTF, which includes providing information and documentation requested by a tribe. Collaborators must not begin collecting data before necessary tribal approvals are obtained.

Compliance

The collaborator acknowledges that failure to comply with any requirement of these Data Security, Submission and Suppression Guidelines and Requirements for Collaborators constitutes a material breach of the Agreement.

FTF's own Data Security Policy & Procedures and Tribal Data Policy may be viewed on the FTF website at http://www.firstthingsfirst.org/grants/grantee-resources.