FIRST THINGS FIRST

Collaborator Data Policy

Purpose

The First Things First (FTF) Collaborator Data Policy[1] pertains to data collected by or shared with collaborators, which include grantees (i.e., grant partners), governmental entities and vendors (i.e., contractors) assisting with an FTF needs and assets report, conducting an FTF-funded program or service, conducting an informal survey, performing a formal study, or collecting data through other approaches on behalf of FTF ("collaborators").

The Collaborator Data Policy supplements FTF's Data Security Policy. Additionally, the collection, use, analysis, publication or sharing of tribally protected data is limited by FTF's Tribal Data Policy.

Background

The mission and vision of FTF is to lead and partner in the creation of a family-centered, equitable, high-quality early childhood system that supports the development, well-being, health and education of all Arizona's children, birth to age 5, so they are ready to succeed in school and in life. This work involves coordination and funding for early childhood development and health programs.

Under state law, FTF must identify and report on the assets available for these programs and the unmet need for these programs throughout each region of the state in order to determine which programs to fund.[2] FTF must also measure the success of its funded programs by their outcomes for children and families.[3] In order to meet these requirements, FTF collects, maintains and reports data on the needs and assets available for early childhood development and health programs and on the performance of FTF's funded programs in each region of Arizona.

Collaborator Data Security Policy

Collaborators must maintain confidential and limited distribution data in a secure manner. Data collected by a collaborator 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 collaborator protects that data in all its forms, during all phases of its life cycle, from

[1] The Collaborator Data Policy was formerly known as the Data Security, Submission and Suppression Guidelines and Requirements for Collaborators.
[2] A.R.S. §§ 8-1161(A)-(C) & 8-1192(A)(1)
[3] A.R.S. §§ 8-1151(B)(6), 8-1174 & 8-1192(A)(4)

inappropriate access, use, modification, or disclosure. 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 must comply with those laws.

In this Policy as well as in the Data Security Policy and Tribal Data Policy, the term "collect" broadly refers to getting data, such as by collecting, obtaining, receiving, gathering, creating, or acquiring the data, including primary, secondary, and tertiary data and the term "publish" refers to disseminating materials in a printed or electronic format for public distribution (e.g., needs and assets reports, impact reports, fact sheets, annual reports).

Data Definitions

Confidential Data. Confidential data is nonpublic 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.

Limited Distribution Data. Limited distribution data is aggregated data created from confidential data of just a few individuals, which creates a risk that the aggregated data will permit the identification of an individual whose data is included. (*See* Data Suppression for Publications, below.) Limited distribution data may be subject to HIPAA, FERPA, tribal law, or other data regulation.

Public Data or Publicly Available Data. Public data is data that is readily available to the general public, such as data located on websites, in publications, or in other widely used sources, as well as unpublished information that members of the public may obtain upon request without needing tribal permission. 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 another organization (e.g., census data). Public data also includes aggregated data, except where the aggregated data constitutes limited distribution data or tribally protected data.

Tribally Protected Data. Tribally protected data is nonpublic data collected from tribal lands of individuals living or working on tribal lands, including nonpublic aggregated data, where the tribe regulates the collection, use, analysis, publication, or sharing of the data. Tribally protected data is considered confidential data except to the extent the tribe has given permission for the data's collection, use, analysis, publication, or sharing, as described in the Tribal Data Policy. Tribally protected data includes nonpublic data FTF collects directly from tribal sources, such as individuals living on tribal lands, tribal programs and departments, tribal Head Starts and child care facilities, and tribally run health care facilities, as well as nonpublic data held outside tribal sources that FTF can only collect with permission from the tribe, such as nonpublic data held by Indian Health Services and the Inter Tribal Council of Arizona. Tribally protected data does not include publicly available data from any source.

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 and submission 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 or 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 may submit public data, limited distribution data or confidential 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 a 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 the data is secured and any confidential data is encrypted or de-identified.

FTF may also receive program data of a collaborator in other ways, such as from a national organization that oversees the program model the collaborator is using (e.g., Parents as Teachers home visitation model) or from another data collection system housing FTF collaborator data, such as the Arizona Early Childhood Workforce Registry.

Collaborators Assisting with a Needs and Assets Report or Performing Formal Studies 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 individual-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 individual-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 primary data from an individual, such as when conducting a program, providing a service, or conducting in-person surveys or 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 an agreement for FTF funding it has appropriately enquired and satisfied itself that it has the ability and authority to comply with the requirements of this section.

Data Suppression for Publications

Confidential or limited distribution data must not appear in publications. When a publication includes aggregated data, FTF or its collaborator will suppress any limited distributed data. The statistical cutoff procedures help ensure that aggregated data does not allow the identification of any individual. FTF's intent is to avoid the possibility of inadvertently reporting personally identifiable information associated with confidential and limited distribution data.

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 or IFSP.

For data related to health, 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 data include preterm births and births to mothers using tobacco during pregnancy.

Third-Party Sharing

Collaborators must not share collected data with individuals or entities other than FTF or the collaborator's subcontractor or subgrantee approved by FTF (see Collaborator Subcontractors and Subgrantees section) 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 (e.g., Parents as Teachers home visitation model). 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. No data may be shared in violation of law.

Notwithstanding the foregoing, no tribally protected data or related protected materials may be shared with any individual or entity, including organizations overseeing models and grantors other than FTF or the collaborator's subcontractor or subgrantee approved by FTF (see Collaborator Subcontractors and Subgrantees section), except in accordance with the FTF Tribal Data Policy.

Collaborator Subcontractors and Subgrantees

All collaborators must contractually require any subcontractor or subgrantee used by them to assist with the collection, maintenance, submission, analysis, or publication of data to comply with this Collaborator Data Policy. In addition, collaborators must obtain advance written approval from FTF before using a subcontractor or subgrantee for any of these purposes.

Alternate Purpose Restriction

Collaborators must not use collected data for a purpose other than those approved by FTF in writing.

In addition, collaborators must not use any tribally protected data or related protected materials for their own academic, research, or publishing purposes without prior, separate consent of the tribe. Collaborators may publicize, without obtaining consent, the fact that they are or have conducted programs or services for children and families living on tribal lands, such as when describing the activities of the organization generally or applying for grants to conduct programs or services in the future.

Tribal Approval

FTF recognizes the right of tribes in Arizona 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, publish, and share tribally protected data (i) with appropriate tribal approvals, which approval may require participation in cultural education and community orientation classes, and (ii) in accordance with FTF's Tribal Data Policy as applicable. FTF's Tribal Data Policy sets forth the principles and basic process by which FTF and its collaborators will seek agreements and other approvals with tribes for the collection, use, analysis, publication, or sharing of tribally protected data related to children 5 and younger and their families who are living on tribal lands and early childhood professionals working on tribal lands.

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 or that FTF will take responsibility for obtaining the approvals. Collaborators should coordinate their efforts to obtain tribal approvals with FTF. FTF Regional Area Directors and Tribal Relations 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, conducting an informal survey, or performing a formal study on behalf of FTF, FTF staff will take the lead in securing the appropriate tribal approvals. Collaborators need to assist FTF in this process as requested by FTF, which includes providing information and documentation requested by a tribe.

Compliance

The failure to comply with any requirement of this Collaborator Data Policy constitutes a material breach of an agreement with FTF to assist with an FTF needs and assets report, conduct an FTF-funded program or service, or perform other informal or formal data collection on behalf of FTF.

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