US Department of Health and Human Services

Privacy Impact Assessment

Date Signed:

08/26/2016

OPDIV:

SAMHSA

Name:

Transformation Accountability System

PIA Unique Identifier:

P-2965359-373110

The subject of this PIA is which of the following?

Major Application

Identify the Enterprise Performance Lifecycle Phase of the system.

Operations and Maintenance

Is this a FISMA-Reportable system?

Yes

Does the system include a Website or online application available to and for the use of the general public?

Yes

Identify the operator.

Agency

Is this a new or existing system?

New

Does the system have Security Authorization (SA)?

Yes

Indicate the following reason(s) for updating this PIA.

Describe the purpose of the system.

The Transforming Accountability (TRAC) system is a Web-based data entry and reporting system that provides a data repository for Center for Mental Health Services (CMHS) program performance measures. Performance measures are collected as part of CMHS effort to promote accountability within its grantee programs. The subject for these programs are grantees with discretionary grants covering programs such as the Children's Mental Health Initiative, Minority AIDS Initiatives, Primary and Behavior Health Care Integration, etc. Additionally, this system will enhance the ability of SAMHSA's public health mission to understand and meet the unique mental health and substance use needs of the nation's different population groups. This effort is mandated by the Government and Performance Results Act (GPRA) and the Office of Management and Budget (OMB).

Describe the type of information the system will collect, maintain (store), or share.

The Transforming Accountability (TRAC) system will collect and maintain consumer/client level outcome data covering the CMHS Center for mental Health Services NOMs National Outcome Measrues domain. The data from these mental health outcomes will consist of consumer functioning, stability on housing, education and employment, crime and criminal justice, perception of care, and social connectedness. This data use is de-identified consumer IDs. Aggregated Program and Grant level reports use cell suppression to obscure these de-identified consumers in reports when cross tabulated by demographic variables. Personal information (PI) like name, address, SSN, etc. are not entered into TRAC system by Grantees for mental health consumers. The demographic data collected by the system are gender, sexual identity, ethnicity, race, and month and year of birth.

Additionally, information is collected about the grant system users, annual goals and budget and infrastructure, prevention and mental health promotion activities. System user information (name, e-mail, work phone number, etc.) are provided only to verify users to allow system access for role specific activities.

Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily.

Data will be collected at the grant and consumer levels to examine consumer outcomes based on grants' and program performance with CMHS. The system does not collect SSN, full DOB, etc. Grantees will enter this data directly into the TRAC system, it will be stored in a manner that allows grant only access to consumer level records for entry and updating purposes, and reported out to CMHS Program GPOs and staff in aggregate formats. Consumer level data are only released to authorized CMHS evaluation contractors through the creation of thorough and rigorous Data Use Agreements approved as contract modifications to the Evaluators contracts and require the contractors to file and maintain non-discloser agreements.

Does the system collect, maintain, use or share PII?

Yes

Indicate the type of PII that the system will collect or maintain.

Name

E-Mail Address

Phone Numbers

Military Status

Employment Status

Month/Year of Birth

Indicate the categories of individuals about whom PII is collected, maintained or shared.

Vendor/Suppliers/Contractors

Patients

How many individuals' PII is in the system?

100,000-999,999

For what primary purpose is the PII used?

The PII is part of the demographic data to be collected that will be used in determining grant performance for CMHS Program |Grants.

Describe the secondary uses for which the PII will be used.

N/A, all data are used solely for performance monitoring of CMHS Programs and Grants.

Identify legal authorities governing information use and disclosure specific to the system and program.

This effort is mandated by the Government and Performance Results Act (GPRA) .

Are records on the system retrieved by one or more PII data elements?

Yes

Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being use to cover the system or identify if a SORN is being developed.

SORN is In Progress

Identify the sources of PII in the system.

Directly from an individual about whom the information pertains

In-Person

Government Sources

State/Local/Tribal

Non-Governmental Sources

Public

Private Sector

Identify the OMB information collection approval number and expiration date

Current OMB: # 0930-0285   Expiration Date 1/31/2016

New OMB clearance is expected 2/1/2016 and to be extended until 1/31/2018

Is the PII shared with other organizations?

No

Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason.

For all data collection, participants are provided detailed information about the purpose and content of the data collection by the Grantee. The Grantee then asks the respondent to consent. Participants are informed of their right to stop participating in the data collection at any time without any repercussions.

Is the submission of PII by individuals voluntary or mandatory?

Mandatory

Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason.

Clients may refuse to participate in any TRAC consumer level interview at any time. They may also refuse to answer any question(s) at any time.

Process to notify and obtain consent from individuals whose PII is in the system when major changes occur to the system.

The process to notify and obtain consent is the sole responsibility of the grantee; the Contractor does not have access to individual clients' contact information or have any way to identify them. The data uses have and will remain the same throughout the contract; only aggregated data is used for reporting purposes. Suppression rules are programmed into systems-generated reports and applied to all ad hoc or off line written reports.

Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate.

Grantees will have direct access to the system to enter and edit PII data. Strict adherence to current security policies ensures integrity in the collection, storage and use of data with integrated measures to address and resolve non-compliance. Records are not directly retrieved by PII. Grants with issues or concerns with resolving PII issues can contact the TRAC Help Desk to resolve any issues and make requested updates. This process must be initiated by the Grantee.

Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy.

Periodic data reviews will be performed to ensure that only approved PII is collected. Consumer/ client IDs are de-identified and regular checks will be conducted against those identifiers and data collected to comply with contractual requirements for data integrity, availability, accuracy and relevancy.

Identify who will have access to the PII in the system and the reason why they require access.

Users:

Consumer level data entry is done by CMHS Grantees. Only Grantees receive role-based access to the data for their grant. The grant Project Director is responsible for approving user access for their grants.

Administrators:

In order to assist grantees with data entry and collection issues, administrators require the ability to access the records as part of their Help Desk duties.

Developers:

Developers have access to the production site for systems support (deployment of new site releases, data extraction and delivery of data, reporting, etc.) as approved/authorized by the contract and non-disclosure agreements.

Contractors:

Contractors have access to TRAC data and reports as specified in individual data use agreements (DUA) which stipulates that they must have signed nondisclosure agreements and receive approval before releasing anything out of the TRAC data or system.

Others:

1) Evaluators - Data extracts are provided to CMHS Program Evaluators with Data Use Agreements for data analyses and evaluation purposes. 2) Data Entry Specialists - Under the new TRAC Contract scanned paper forms will be directly entered into the TRAC system. Forms are required to only include the same information stored in the TRAC System.

Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII.

Access to data is based on the user roles as authorized by the grant project director for grant staff , the TRAC Contract Officer for SAMHSA staff, and the information systems manager for Westat staff. User rights at both application and server levels are assigned and applied, ranging from a public user (non-credentialed access to general information) to a systems administrator (full rights). Integrated system validation controls regulate access, and checks are in place to monitor and enforce activation, expiration, renewal and deactivation of user accounts.

Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job.

An individual user's job function determines the level of access provided and users are assigned only those rights necessary to fulfill responsibilities for their approved roles. System-level audit controls safeguard and audit use.

Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained.

Privacy and Security training is provided at on-boarding; Human Subjects Protection training is provided to all (Contractor) personnel using the system. The Human Subjects training outlines the privacy concerns for This training is required to updated annually for Westat employees via their Westat Human Subjects Protection Training and Information Security Awareness Training (ISAT) . Additional agency specific training as done as required by specific contracts.

Describe training system users receive (above and beyond general security and privacy awareness training).

Additional training for data collection, the use of data in analyses, and other task-specific training is provided as needed.

Do contracts include Federal Acquisition Regulation and other appropriate clauses ensuring adherence to privacy provisions and practices?

Yes

Describe the process and guidelines in place with regard to the retention and destruction of PII.

As directed in the Contract's Statement of Work, PII collected through the TRAC System will remain on secured TRAC server(s) until a request is made to move/remove/transition or destroy data at the end of the contract. The daily backup of servers follow Advanced Encryption Standard (AES) controls and corporate controls regulate restore/upgrade operations as needed. Upon completion of the contract, data will be transitioned to the government or other contractor as directed. * This Contract does not require National Archives and Records Administration (NARA) schedules.

Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls.

The TRAC system and all personnel (staff and contractors) and processes comply with the NIST 800-53 controls required to operate. These include: Contractor Agreements, System Security Plan (SSP), PII policies; security awareness and training, Redundancy measures, Backup systems, Encrypted media, Firewalls, encryption, intrusion detection, Role-based authorization and authentication with expiration and renewal limits; time-out controls for inactivity, Audit logs, Identification and data entry cards.

Identify the publicly-available URL:

The Website is currently in development. Once ATO is approved this link will go live.

Does the website have a posted privacy notice?

Yes

Is the privacy policy available in a machine-readable format?

Yes

Does the website use web measurement and customization technology?

Yes

Select the type of website measurement and customization technologies is in use and if it is used to collect PII.

Session Cookies that do not collect PII.

Does the website have any information or pages directed at children under the age of thirteen?

No

Does the website contain links to non- federal government websites external to HHS?

Yes

Is a disclaimer notice provided to users that follow external links to websites not owned or operated by HHS?

No