Court Services and Offender Supervision Agency (CSOSA)

AccuCare
Privacy Impact Assessment

CONTROLLED UNCLASSIFIED INFORMATION

2020

Office of Information Technology
Court Services and Offender Supervision Agency
800 North Capitol Street, NW Washington, DC 20004

Overview of AccuCare

The Court Services and Offender Supervision Agency (CSOSA) core mission is to effectively supervise adults under our jurisdiction, to enhance public safety, reduce recidivism, support the fair administration of justice, and promote accountability, inclusion and success through the implementation of evidence-based practices in close collaboration with our criminal justice partners and the community. To further this mission, The Office of Information & Technology (OIT) established the AccuCare system to assess addiction severity and create individualized intervention plans for offenders monitored by CSOSA and the Pretrial Services Agency (PSA). The AccuCare system is used by the CSOSA for the District of Columbia's personnel in the Behavioral Intervention Division/Assessment, Evaluation and Placement Unit (BID/AEPU).

The purpose of this new Privacy Impact Assessment (PIA) is to address privacy risks associated with the collection, storing, dissemination, and disposal of Personally Identifiable Information (PII) in the AccuCare system.

1. Description of the System

1.1. Describe the system, including the system name, system, acronym, and a brief description of the major functions.

The Accucare System is an Electronic Health Record and Billing Application. An electronic health record, or EHR, is a software system that handles electronic versions of a patient's healthcare history. This replaces the traditional paper chart system, containing all of the important records about a patient like their medications, progress notes, demographics, vitals, history and more. The EHR system not only keeps this information but also tracks it and compiles it, automating basic functions while allowing for more streamlined reporting.

The Accucare system performs the following functions:

- Centralized Client Intake
- Screenings and Supplements
- Assessments
- Admission, Transfer, Discharge, and Diagnosis
- Treatment Plans,
- Progress Notes
- Multi-Dimensional Assessment with Decision Support
- Recovery Support
- Follow-ups
- Data Query
- Access Control (Provider ID)
- Medication Management
- Prevention
- Electronic Billing

- Reporting
- Scheduling
- Electronic Signature and Chart Management
- Census

The AccuCare system is managed by CSOSA. Information stored in the system is housed in a secure location at CSOSA. The Database for the AccuCare system resides on the Microsoft SQL Server located in a CSOSA data center. The AccuCare application and database servers are only accessible on the CSOSA internal network.

There are three program offices/treatment groups that use AccuCare:

1. PSA Pretrial Treatment– Conducts assessments and formulates treatment recommendations; facilitates pre-treatment, substance abuse education, anger management, and sanctions group programs; and monitors individual progress once the pretrial defendant begins treatment with a provider.
2. The Assessment, Evaluation & Placement Unit (AEPU)/Behavioral Interventions Division (BID) - The Behavioral Interventions Division (BID) coordinates and delivers interventions targeting criminogenic, stabilization, and behavioral health needs. The BID also serves as the central hub for delivering evidence-based interventions for criminal justice involved clients at various field locations and in differing levels of care. In addition, the BID works to structure restorative justice activities for offenders that focus on repairing the harm done to victims and communities as a result of their past criminal behavior. The BID is comprised of the Intensive Cognitive Behavior Interventions (ICBI), Assessment, Evaluation & Placement, and Restorative Justice Units. The BID serves as the Agency hub for delivering strategic interventions that are proven to be effective in targeting the needs of criminal justice-involved offenders.

   AEPU ensures assessment and evaluation of offenders for individualized criminogenic and stabilization needs to place them in the most appropriate behavioral, substance abuse, mental health interventions and other support services that are responsive to the risk the offender poses to public safety.

3. CSOSA Re-entry and Sanction Center (RSC) – Provides high-risk offenders and defendants with a four-week intensive assessment and reintegration program. Conducts assessments and formulates treatment recommendations; facilitates pre-treatment, substance abuse education, anger management and sanctions group programs; and monitors individual progress while the offender is being treated at the RSC facility.

As pretrial defendants and offenders, herein referred to as “individuals”, move through treatment program offices, they also move through the AccuCare system. For example, depending on an individual’s assessed addiction severity, he/she may be sent to a variety of treatment programs following each assessment. Each treatment program office conducts an assessment on the individual. Once the assessment is completed, the agency personnel enters the individual’s information into the AccuCare system. The agency personnel can then generate a treatment plan using the AccuCare system. Each assessment and treatment plan is stored in AccuCare and stays in the system as the individual moves between treatment groups.

1.2. Describe the purpose for which the personally identifiable information (PII) is collected, used, maintained, or shared.

Offender PII is collected and used to provide appropriate treatment. The information gathered in the system is used by CSOSA staff to complete a clinical assessment of the offender's substance abuse addiction severity using the imbedded assessment tool, Addiction Severity Index (ASI) Clinical Standard, in order to generate a preliminary diagnostic profile for use by the clinical team in the development of an agency compliant treatment plan.

1.3. Is this a new system or one that is currently in operation?

AccuCare is currently in operation.

1.4. Is this PIA new, or is it updating a previous version? If this is an update, please include the publication date of the original.

This is a new PIA.

1.5. Is the system operated by the agency, by a contractor, or both?

The AccuCare system is operated by CSOSA. Information stored in the system is housed in a secure location at CSOSA. The database for the AccuCare system resides on the Microsoft SQL Server located in a CSOSA data center. The AccuCare application and database servers are only accessible on the CSOSA internal network.

2. Legal Authorities and Other Requirements[1]

2.1. What specific legal authorities and/or agreements permit and regulate the collection, and use of the data by the system?[2]

Information maintained in the system is collected pursuant to a delegation by Congress, that CSOSA will exercise the powers and functions for the District of Columbia pursuant to the National Capital Revitalization and Self-Government Improvement Act of 1997, Pub. L. 105-33, D.C. Code § 24-133, and shall provide supervision for District offenders on probation, parole, and supervised release on behalf of the court or agency having jurisdiction over the offender being supervised.

2.2. System of Records Notice (SORN) Requirement: Is the information in this system retrieved by a name or a personal identifier? If so, this system will need to be covered by a Privacy Act SORN.[3]

[1] If you are unsure of your legal authority, please contact CSOSA's Senior Agency Official for Privacy.
[2] Legal authorities are statutes, executive orders, federal regulations, and/or Memorandum of Understandings. Include the citation/reference of the legal authority.
[3] System of Records Notice (SORN) is a formal notice to the public that identifies the purpose for which PII is collected, from

Yes, information in the system is retrieved by name or personal identifier. A SORN is required for the system.

2.3. Records Management Requirement: Does a records retention schedule, approved by National Archives and Records Administration (NARA), exist for the records contained in this system? If yes, please provide the NARA schedule number.[4]

AccuCare records are temporary and can be destroyed 1 year after assessment is completed Longer retention is authorized if required for business use. Disposition Authority is DAA-0562-2013-0004. The information is used for the purpose specified in this PIA.

2.4. Is the PII contained in this system disposed of appropriately, and in accordance with the timeliness in the records disposition schedule?

Yes, the records are disposed of. We work with the vendor to manually dispose the records in the database. CSOSA will identify all records that need to be disposed of.

2.5. Describe any potential threats to privacy as a result of the component's use of the information, and controls that the component has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.).

The risks identified are the risk of unauthorized access to or use of individual's personal information. In order to mitigate these risks, access to individual electronic case files is limited to those authorized personnel who manage and have direct business need over case file information. All authorized agency personnel, to include system administrators, have accepted the rules of behavior regarding the proper handling of CSOSA computer systems and information. All authorized personnel will receive computer security training specific to use of the AccuCare system. In addition, the AccuCare electronic system is Federal Information Security Modernization Act ("FISMA") compliant. Further, to ensure accountability of the information maintained in the system, audit logs will be kept and checked at regular intervals.

3. Characterization and Use of Information

Collection

3.1. Select the specific personal information data elements (e.g. name, email, address, phone number, date of birth, social security number, etc.) that the system collects, uses, disseminates, or maintains.

whom and what type of PII is collected, how the PII is shared externally (routine uses), and how to access and correct any PII maintained by CSOSA. Verify if there is an existing SORN for the system.

[4] If you are unsure of the records retention schedule, please contact CSOSA's Records Management Officer.

Identifying Numbers					
Social Security		File/Case ID	X	Financial Account	
Taxpayer ID		Driver's License		Financial Transaction	
Employee ID		Credit Card			
Other identifying numbers (please specify):					

General Personal Data					
Name	X	Date of Birth	X	Religion	X
Maiden Name		Place of Birth		Financial Information	
Alias		Home Address	X	Medical Information	X
Gender	X	Telephone Number	X	Military Service	
Age	X	Email address		Physical Characteristics	
Race/Ethnicity	X	Education			
Other general personal data (specify): Criminal charges.					

Work-related Data					
Occupation	X	Telephone number		Salary	X
Job title	X	Email address		Work history	X
Work address	X	Business associates			
Other work-related data (please specify):					

Distinguishing Features/Biometrics					
Fingerprints		Photos		DNA profiles	
Palm prints		Scars, marks, tattoos		Retina/iris scans	
Video recording/signatures		Vascular scan		Dental profile	

System admin/audit data					
User ID		Date/time of access		ID files accessed	
IP address		Queries run		Contents of files	
Other system admin/audit data (please specify):					

3.2 Indicate the sources of the information in the system (e.g., individual, another agency, commercial sources, etc.) and how the information collected from stated sources (paper form, webpage, database, etc.).[5]

Directly from individual about whom the information pertains					
In person	x	Hard copy: mail/fax		Online	
Telephone		Email			
Other (please specify):					

[5] Examples include form filling, account verification, etc.

Government Sources					
Within the Component	x	Other CSOSA components	x	Other federal entities	x
State, local, tribal	x	Foreign	x		
Other (please specify):					

Non-government Sources					
Members of the public		Public media, internet		Private sector	
Commercial data brokers					
Other (please specify):					

3.3 Where will the PII be stored in the system?

The Database for the Accucare system in the CSOSA Data Center. The Accucare application and database servers are only accessible on the CSOSA internal network.

3.4 Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exists in light of the information collected or the sources from which the information is collected. Please describe the choices that the component made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.).

The Agency has established policies and procedures to prevent or mitigate threats to privacy in connection with the disclosure of information. All permanent and temporary CSOSA employees and contractors that use, manage, develop, maintain or support CSOSA information systems are required to adhere to the Agency's Information Technology Security Policy Statement 2036 and related Operational Instructions. The agency has also established a Social Security Number (SSN) Non- Collection guide to ensure that SSNs are not collected when using Accucare.

The other risks identified are the risk of unauthorized access to or use of individual participant's personal information. In order to mitigate these risks, access to individual electronic case files will be limited to those authorized personnel who manage and have direct control over case file information. All agency personnel, to include system administrators, have accepted the rules of behavior regarding the proper handling of CSOSA computer systems and information. All authorized personnel will receive computer security training specific to use of the AccuCare system. In addition, the AccuCare electronic system is FISMA compliant. Further, to ensure accountability of the information maintained in the system, audit logs will be reviewed regularly.

Purpose and Use of the System

3.5 Describe how and why the system uses the information to achieve the purpose stated in Question 1.2 above.

The agency's personnel collects PII and enters it into the AccuCare system to conduct assessments and provide a recommended treatment plan for the individual's monitored by CSOSA. The agency collects the information from the individual participant and enters it into the AccuCare system, to generate an accurate addiction severity index and create a level of care recommendation and treatment plan; information about the offender's addiction history, medical history, family and social history, criminal history, employment history, and income. This is necessary to meet the Agency's mission of protecting the public and preventing crime, and it allows the agency personnel to ensure that the correct level of treatment is provided to the individual.

3.6 Select why the information in the system is being collected, maintained, or disseminated.

Purpose			
For criminal law enforcement activities		For civil enforcement activities	
For Intelligence activities		For administrative matters	
To conduct analysis concerning subjects of investigative or other interest		To promote information sharing initiatives	
To conduct analysis to identify previously unknown areas of note, concern, or pattern		For administering human resources programs	
For litigation			
Other purpose (please specify): Enhancing the mission of providing medical behavioral interventions.			

Social Security Numbers[6]

3.7 Does they system collect Social Security Numbers? If so, explain the purpose of its collection, type of use, and any disclosures.[7]

Social security numbers are not collected or maintained in the system. The AccuCare system does have an option to collect SSNs, however staff are trained to not collect SSNs as they are not required.

3.7 Specify any alternatives considered in the collection of SSN and why the alternatives were not selected.

File/Case ID numbers are used to search for an individual in AccuCare.

[6] In order to collect Social Security Numbers, the System Owner must state the collection is: 1) authorized by the law, 2) necessary for an agency purpose, and 3) there is no reasonable alternative.
[7] In accordance with OMB Regulations, please note if the system collects SSN, the PIA will require a signature by the Assistant Secretary or equivalent.

4 Notice

4.1 How does the system provide individuals notice about the collection of PII prior to the collection of information (i.e. written Privacy Act notice, link to a privacy policy, etc.)? If notice is not provided, explain why not.

The agency personnel notifies individual participants that, as part of the treatment program, the agency will collect personal information entered it into the AccuCare system prior to the collection of the personal information. The agency personnel interviews participants using the ASI survey. Before the interview begins, agency personnel explain that the information collected is used to generate an assessment plan to recommend the level of care and that the information is required to provide an accurate treatment plan.

4.2 Provide the text of the notice, including where it can be found, or the link to the webpage where notice is posted.

AccuCare is a commercial off-the-shelf system, the agency does not have the ability to modify the logon page to display a notice. The Privacy Act Statement is provided to offenders as a separate document.

Authority:

Information maintained in the system is collected pursuant to a delegation by Congress, that CSOSA will exercise the powers and functions for the District of Columbia pursuant to the National Capital Revitalization and Self-Government Improvement Act of 1997, Pub. L. 105-33, D.C. Code § 24-133, and shall provide supervision for District offenders on probation, parole, and supervised release on behalf of the court or agency having jurisdiction over the offender being supervised.

Purpose:

Offender PII is collected and used to provide appropriate treatment. The system allows CSOSA to provide treatment to offenders supervised by the Agency. The goal of the system is to assess the offender's addiction severity using the Addiction Severity Index (ASI) Clinical Standard in order to generate a Diagnostic and Statistical Manual of Mental Disorders (DSM-V) compliant treatment plan.

Routine Use:

Standard CSOSA Routine Uses:

- *For Law Enforcement Purposes*: To disclose pertinent information to the appropriate Federal, state, or local agency responsible for investigating, prosecuting, enforcing, or

implementing a statute, rule, regulation or order, where CSOSA becomes aware of an indication of a violation or potential violation of a civil or criminal law or regulation.

- *For Litigation*: To disclose information to the Department of Justice for the purpose of representing CSOSA, or its components or employees, pending or potential litigation to which the record is pertinent.

- *For Judicial/Administrative Proceedings*: To disclose information to another Federal agency, a court, grand jury, or a party in litigation before a court or administrative proceeding being conducted by a Federal agency, when the Federal Government is a party to the judicial or administrative proceeding.

- *For National Archives and Records Administration*: To disclose information to the National Archives and Records Administration for use in records management inspections conducted under the authority of 44 U.S.C. §§ 2904 and 2906.

- *For Congressional Inquiry*: To provide information to a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.

- *For Data Breach and Mitigation Response*:

  - To provide information to appropriate agencies, entities, and persons when (1) the CSOSA suspects or has confirmed that there has been a breach of the system of records; (2) the CSOSA has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the CSOSA (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the CSOSA's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

  - To provide information to another Federal agency or Federal entity, when CSOSA determines that information from this system of records is

reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach, or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

Disclosures:

Not all offenders/defendants who are supervised by the CSOSA or Pretrial Services Agency (PSA) are required to enter addiction treatment programs. An individual may opt out of treatment programs if their participation is not mandated by the court. If the offender/defendant elects or is ordered by the court to participate in a CSOSA or PSA substance abuse treatment program, it is mandatory that he/she provide the required information that is collected, entered into and maintained in the AccuCare system.

4.3 What opportunities are available for individuals to consent to uses, decline to provide information, or opt-out of this system/project?

Not all offenders/defendants who are supervised by the agency are required to enter addiction treatment programs. An individual may opt out if their participation is not mandated by the court. However, if the offender elects or is ordered by the court to participate in the agency's substance abuse treatment program, they must consent to provide information that is required in the system. Before the offender is interviewed by the agency personnel for addiction severity, the agency personnel verbally state the purpose of the interview, the information that will be collected and the reasons the information will be used. Offenders provide consent to provide PII and other information to participate in the treatment program or offenders may sign a right of refusal prior to the interview or at the conclusion of the interview upon receiving a treatment recommendation for which he/she is not in agreement.

5 Information Sharing

Internal

5.1 How do agency personnel gain access to the system and the PII (e.g., users, managers, system administrators, developers, contractors, etc.)?

Only agency personnel in PSA treatment, BID/AEPU, contractors and IT administrators will have access to the system. The agency personnel are standard users that can enter information into the system, but cannot make changes to the AccuCare database and application. The IT administrators are "super users" with escalated privileges that can make configuration changes to the system if approved by the Change Control Board within the agency.

5.2 Will information be shared internally with other CSOSA program offices and/or components, if so, which ones?

Yes, information will be shared internally. Information sharing is limited to raw testing scores taken from the Addiction Severity Index assessment tool. Only those staff from the Re-Entry and Sanctions Center, Behavioral Intervention Division and Pretrial Services will have access to the software to view data information. Raw data scores will be shared with OCSIS Community Supervision Officers. Internal agency confidentiality and privacy policies are in effect with respect to data access and data sharing.

5.3 What information will be shared and with whom?

Raw scores are incorporated into a final discharge summary which is released to the primary CSOSA supervision officer and only staff with access to AccuCare are able to view the ASI and/or raw score generated information. Internal agency confidentiality and privacy policies are in effect with respect to data access.

Summary screening and assessment results are provided in the RSC discharge summary. Under general circumstances, summary data is being shared with support of a fully-executed release of information form to external individuals and/or agencies.

5.4 How will the information be shared?[8]

In CSOSA's Reentry and Sanctions Center (RSC), final assessment reports will reference data collected in AccuCare. Summary data is shared with support of a fully-executed release form to individuals in hard copy mail or faxed documents, telephone, and secured online documentation.

5.5 What is the purpose of sharing the specified information with the specified internal organizations? Does this purpose align with the stated purpose in Question 1.2 above?

The purpose of data sharing is limited to provision of ongoing treatment recommendations based on the comprehensive assessment completed at the Re-Entry and Sanctions Center. A final discharge summary is released to the primary CSOSA supervision officer. Yes, the stated purpose aligns with 1.2.

5.6 Describe controls that the program offices and/or components have put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information.

The Agency has established policies and procedures to prevent or mitigate threats to privacy in connection with the disclosure of information. All permanent and temporary

[8] Examples, include but is not limited to, case-by-case, direct access, e-mail, etc.

CSOSA employees and contractors that use, manage, develop, maintain or support CSOSA information systems are required to adhere to the Agency's Information Technology Security Policy Statement 2036 and related Operational Instructions.

RSC employees are **prohibited** from disclosing any PII residents to the media or public. Staff adhere to the 42 CFR Part 2, Health Insurance Portability and Accountability Act (HIPAA) and Privacy Act regulations. All requests for information are forwarded to the FOIA/PA Officer in OGC and the Office of Legislative, Intergovernmental and Public Affairs (OLIPA) for action.

5.7 Is the access to the PII being monitored, tracked or recorded?

Yes, this information is stored in the AccuCare application log files.

External

5.8 Will the information contained in the system be shared with external entities (e.g. another federal agency, District of Columbia agency, etc.)?

Yes.

5.9 What information will be shared and with whom?

Data sharing is limited to raw testing scores taken from the Addiction Severity Index assessment tool. Information sharing is limited to permanent CSOSA contract vendors and contract employees. CSOSA staff adhere to the 42 CFR Part 2, HIPAA and Privacy Act regulations. All requests for information post record closure are forwarded to the FOIA/PA Officer in OGC and the Office of Legislative, Intergovernmental and Public Affairs (OLIPA) for action.

5.10 What is the purpose of sharing the specified information with the specified external entity? Does this purpose align with the stated purpose in Question 1.2 above?

Shared information is communicated for purposes of care continuity and ongoing treatment planning. Yes, the stated purpose aligns with 1.2.

5.11 How is the information accessed and used by the external entity?

Summary screening and assessment information is exclusively provided to external entities in the form of the RSC discharge summary or as part of the clinical assessment completed by BID/AEPU personnel. Under general circumstances, summary data is being shared with support of a fully-executed release of information form to external individuals and/or agencies.

5.12 What controls are in place to minimize risk and protect the data?

For the electronic interfaces, CSOSA has a number of technical controls in place to minimize risk including strong passwords, restricted firewall rules, and use of encryption. Data exchanged is limited to the minimum amount of data necessary to successfully add, update and maintain records.

RSC staff members manually share only data with external entities as part of the continuation of drug treatment care. Controls that are in place to minimize risk include sharing data via secured email, or via secured fax. Other controls include training for staff members on information security, privacy, and records management.

5.13 Is the external information sharing pursuant to a Computer Matching Agreement (CMA), Memorandum of Understanding (MOU), or other type of approved sharing agreement with another agency?

No.

6 Consent and Redress

6.1 How will individuals be notified if there are any changes regarding how their information is being collected, maintained, or disseminated by the system?

If there are any changes made to the system that affect individuals' PII, a communication from CSOSA agency personnel will be provided to the affected individuals detailing the changes and further guidance.

6.2 What are the procedures that will allow individuals to access their own information?

An individual participant will have to submit a Freedom of Information Act (FOIA) request to obtain information about themselves that the agency maintains in the system.

Under the provisions of the Privacy Act and FOIA, individuals may request searches of appropriate applications to determine if any records have been added that may pertain to them. This is accomplished by sending a written request directly to:

Court Services & Offender Supervision Agency
Office of the General Counsel
800 North Capitol Street, N.W., Suite 7217
Washington, DC 20002
ATTN: FOIA/Privacy Act Request

By facsimile at:
(202) 442-1963

ATTN: FOIA OFFICER

When seeking records about yourself from any CSOSA system of records, the request must conform with the Privacy Act regulations set forth in 49 CFR Part 10. The request must be signed, and the requestor's signature must either be notarized or submitted under 28 U.S.C. 1746, a law that permits statements to be made under penalty of perjury as a substitute for notarization. While no specific form is required, you may obtain forms for this purpose from the Chief Freedom of Information Act Officer, https://www.csosa.gov/foia/

In addition, the requestor should provide the following:

- An explanation of why the requestor believes the agency would have information on him/her;
- Identify which component(s) of the agency the requestor believes may have the relevant information;
- Specify when the requestor believes the records would have been created;
- Provide any other information that will help the FOIA staff determine which CSOSA component agency may have responsive records; and if the requestor is seeking records pertaining to another living individual, the requestor must include a statement from that individual certifying his/her agreement for the requestor to access his/her records.

Without this bulleted information the component(s) may not be able to conduct an effective search, and the request may be denied due to lack of specificity or lack of compliance with applicable regulations.

6.3 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Individuals may submit a written challenge to the accuracy of the information found in his or her record. The individual shall be required to provide the case manager with sufficient information in support of the challenge (names of persons to contact, government agency, etc.) When an individual provides such information, the Unit Manager or Case Manager shall review the alleged error(s) and take reasonable steps to ensure that the information is corrected. Prior to endorsing the summary results via offender signature; the offender has an opportunity to review the information collected for accuracy. Challenges to Pre-sentence Investigation (PSI) information shall be forwarded to CSOSA's PSI Processing Unit for resolution. Prior to endorsing the summary results via offender signature; the offender has an opportunity to review the information collected for accuracy.

6.4 How does the project notify individuals about the procedures for correcting their information?

All clients receive a program overview that includes confidentiality and privacy guidelines. Notification to individuals for how to update or correct their information maintained in AccuCare is provided through this PIA posted on CSOSA's website as well as information provided during orientation.

6.5 How will individuals have the opportunity to consent or dissent to particular uses of the information?

BID/AEPU Treatment office
Opportunities to consent are evidenced by written disclosures requiring the offender's signature. The offender is informed of the effective date and expiration date of the written disclosure. The Offender is also informed that he/she has the right to revoke the consent at any time in writing.

RSC Treatment office
Individuals must provide consent for collection and use of PII. Verbal and written disclosures of information on offenders must be documented. At the RSC, staff record the disclosures in the resident's record when a verbal request for resident information is made and/or information about a resident is disclosed verbally. Documentation of written disclosures is maintained in the same manner or may be made by requesting the information and a copy of the response in the file from which the record is disclosed. A copy of the resident's signed release form must be maintained as described above in all cases where Agency non-public protected information is disclosed.

PSA Treatment office
Opportunity to consent/dissent is provided through notice and comment on the System of Records Notices (SORNs) and/or via the procedures for correction of records set forth in the Joint FOIA/Privacy Act Policy Statement.

6.6 How will the agency provide notice to individuals that their PII may be shared with other agencies or entities (both internal and external)?

Notice is provided through this published PIA. Staff review the residents' right to privacy, confidentiality of their medical records, program rules and responsibilities. All records created by staff for each new resident are protected by the Privacy Act of 1974. The resident's record contains both public and private information. Release of this information is subject to CSOSA policies. Release of PII contained in the resident's case file, other than information of public record, is prohibited. A resident consents to release of information from his file by signing a consent to release information that is comprehensive enough to cover the release of information for any purpose prior to the information release. A counselor shall secure completion of the Consent for Release of Information form, resident Acknowledgement of Resident Handbook Resident Rights and Responsibilities and Resident Grievance Procedures. If unintended contact with outside entities is made without resident acknowledgement, all efforts will be made to notify the resident immediately. Serious complaints, such as unauthorized release of resident information, are to be immediately reported to the Program. Documentation of the incident will be forwarded to

CSOSA's FOIA/PA Officer in OGC for follow-up and resolution.

7 Information Security and Safeguards[9]

7.1 Does the component office work with their Chief Information Officer (CIO) to build privacy and security into the system and build privacy extension to the extent feasible?

Yes. The Accucare System is a proprietary commercial off the shelf (COTS) packaged sold and supported by Orion Healthcare, Inc. The system is designed to meet the HIPAA standards since it is intended for use by Medical providers and has been completed a security authorization assessment to demonstrate that it meets NIST SP 800-53 Rev-4 standards.

7.2 Do contractors have access to the system?

Yes. At the RSC, contractors have access to AccuCare. Contract medical personnel complete assessments in the system. Other contractors add clinical documentation of group and individual therapy notes to the system as part of the provision of clinical interventions and maintenance of the resident health record.

7.3 What procedures are in place to determine which users may access the information and how does the project determine who has access?

Before gaining access to the system users complete internal access forms to request access to the system. The form is reviewed by management and the AccuCare administrators to determine which level of access the user needs to perform their job function.

7.4 What administrative, technical, and physical safeguards are in place to protect the information?

Physical Controls

The agency's Data Center that houses the AccuCare servers, requires an identification badge for entrance into the server room. A limited number of users are on the Data Center Access Control List (ACL). The authorized users with access are limited to personnel in Infrastructure, Facilities, and the Security units. The Data Center ACL is updated monthly to add and/or remove users' access. The ACL is signed and approved by the Chief Information Security Officer, Infrastructure Manager, and Director of Security each month.

The building where the Data Center is located also required identification badges for entry. There are security guards posted at the entrance to the building. Security cameras are also positioned outside of the building, on each floor of the building, and within the Data

[9] If you are unsure which safeguards will apply, please consult with CSOSA's Information Security Officer.

Center.

Technical Controls

The AccuCare application is only available through the CSOSA network. Users must login to their CSOSA workstation using their active directory (AD) account and then login to the AccuCare application using their separate AccuCare login credentials. Passwords are required to be a minimum of eight characters in length, and must contain one upper case letter, one lower case letter, one number and one special character.

Administrative Controls

AccuCare underwent a security assessment and authorization in March 2013 and is required by FISMA to be assessed at least once every three years. The AccuCare servers are also backed up every night to ensure no data is lost.

7.5 Is an Authority to Operate (ATO) required? Has one been granted?

An ATO is required and was granted on May 29, 2019.

7.6 Is the system able to provide an accounting of disclosures?

Yes, routine record audits are completed to ensure compliance with all federal guidelines for documentation standards and record keeping.

7.7 What controls are in place to prevent the misuse (e.g., browsing) of data by authorized users who have access to the data?

Access control have been implemented into the system to manage access, views, and browsing. Standard users can only see patients in their own treatment group. Supervisors can see all patients and transfer the cases between treatment groups (i.e. PSA,BID/AEPU, RSC). Additionally, at the RSC direct observation, clinical supervision, data analytics and routine record audits are used to prevent the misuse of data.

7.8 Is there a way to identify unauthorized users? If so, what controls are in place to prevent a data breach?

The servers are behind the security perimeter firewalls and are not accessible outside of the CSOSA and PSA production networks. Only authorized users can access the databases and system. Additionally, at the RSC, direct observation, clinical supervision, data analytics and routine record audits are used to prevent misuse and identify unauthorized users.

7.9 Does the agency provide annual security and privacy training for agency employees and contractors?

Yes. Privacy training is provided during the annual security awareness training. Staff are

also trained on the AccuCare system and are advised of how to properly handle and safeguard PII entered and maintained in the system.

7.10 Who is responsible for assuring safeguards for PII in the system?

The treatment offices who use the system are responsible for assuring safeguards for PII in the system.

7.11 How will owners of the PII be harmed if privacy data is unlawfully disclosed?

PII, which if lost, compromised or disclosed without authorization, could potentially result in substantial harm, embarrassment, inconvenience, or unfairness to the owner.

7.12 If contractors have access to the system, has the agency provided the contractor, who works on the system, a confidentiality agreement or a Non-Disclosure Agreement (NDA)?

Yes. This is part of the security clearance and orientation process for contractors.

7.13 What other IT security measures has the agency implemented to protect PII in the system?

The Agency has established policy and procedure to prevent or mitigate threats to privacy in connection with the disclosure of information. All permanent and temporary CSOSA employees and contractors that use, manage, develop, maintain or support CSOSA information systems are required to adhere to the Agency's Information Technology Security Policy Statement 2036 and related Operational Instructions.

The AccuCare Web System offers SSL Encryption (Secure Socket Layer) for the secure transmission of documents over the Internet. SSL uses a private key to encrypt data before its transfer. SSL is used to encrypt transmission of confidential user information, such as personal health information. AccuCare utilizes encryption/security software to safeguard the confidentiality of personal information from unauthorized access or disclosure and accidental loss, alteration or destruction. The agency has also established a Social Security Number (SSN) Non-Collection guide to ensure that unnecessary collection of SSNs are restricted when using AccuCare.

8 Auditing and Accountability

8.1 How does the system owner ensure that the information is used in accordance with the stated practices in this PIA?

As required by FISMA, the AccuCare system will undergo a security assessment at least once every three years or when a major change is made to the system. The assessment process will ensure that the information in AccuCare is used for the purposes stated in this

PIA. If the collecting or sharing of PII changes, the PIA will be updated accordingly.

Because the server and software is managed internal to the agency, the privacy risks are significantly limited to untoward or unintended acts of privacy violation by agency staff. Internal audits are designed and conducted to ensure compliance with regulatory standards. Potential breach of privacy can also be identified during this process. The staff treat all disclosures in accordance with professional confidentiality standards and applicable Federal and District of Columbia law.

8.2 What are the privacy risks associated with this system and how are those risks mitigated?

The risk of unauthorized access exists with any information technology system or document. CSOSA conducts thorough background checks on every employee and contractor, conducts annual Security & Privacy authorization assessments, and implements the necessary safeguards to keep our system secure and the information protected. No unknown privacy risks have been identified for the AccuCare system.

9 Data Quality and Integrity

9.1 How will the information that the agency collects be verified for accuracy and completeness when it is entered into the system?

The agency personnel collect the personal data directly from the individual and it is entered into the system by the agency personnel. Agency personnel verifies each answer with the offender for accuracy before the information is entered into the system.

9.2 Are there any privacy risks for individuals whose information is collected or used by the project that relate to data quality and integrity? If so, how will CSOSA mitigate these risks?

There are no privacy risks for information collected related to data quality and integrity. Risks are minimized because the information is collected directly from the individual and verified with the offender for accuracy before it is entered into the system.

10 Privacy Policy and Statement

10.1 Has the agency provided a privacy statement or policy for this system and is it provided to all individuals whose PII is collected, maintained or stored?

Yes. The Privacy Act Statement is provided to all individuals whose PII is collected, maintained or stored.

10.2 Is the privacy policy publicly viewable? If so where?

CSOSAs privacy policy is publicly viewable on the CSOSA website homepage.
https://www.csosa.gov/privacy-policy/

Authorizing Signatures

This Privacy Impact Assessment has been conducted by the Office of Information Technology and has been reviewed by Sheila Stokes, the Senior Agency Privacy Official, for accuracy.

James D. Berry, Jr.
System Owner Name (Please Print)

JAMES BERRY JR. Digitally signed by JAMES BERRY JR. Date: 2021.08.04 11:30:46 -04'00'
System Owner Signature _____ Date

Senior Agency Official for Privacy (Print)

SHEILA STOKES Digitally signed by SHEILA STOKES Date: 2021.08.05 13:05:18 -04'00'
Senior Agency Official for Privacy Signature _____ Date

General Counsel (Print)

SHEILA STOKES Digitally signed by SHEILA STOKES Date: 2021.08.05 13:03:45 -04'00'
General Counsel Signature _____ Date