



**Court Services and Offender Supervision Agency
for the District of Columbia**

OPERATIONAL INSTRUCTION

Operational Instruction CSS-2009-03

Policy Area: Supervision

Effective Date: 3/30/2009

Approved:

Thomas H. Williams, Associate Director
Community Supervision Services

Sensitive, Protected Offender Information in CSOSA's Case Management System

I. COVERAGE

This Operational Instruction applies to Community Supervision Assistants (CSAs), Community Supervision Officers (CSOs), Supervisory Community Supervision Officers (SCSOs), Branch Chiefs (BCs), Global Positioning System (GPS) Unit staff, Illegal Substance Collection Unit (ISCU) staff, Offender Processing Unit (OPU) staff, and other staff within Community Supervision Services (CSS) who have access to sensitive, protected offender information electronically through the Agency's case management information system.

II. BACKGROUND

In the performance of their work, CSS staff process, handle, or work with sensitive, unclassified information. Policy Statement 500.2, Safeguarding Sensitive, Unclassified Information provides general guidance on safeguarding sensitive, protected information. This Operational Instruction (OI) provides specific guidance to CSS staff in regard to documenting and disseminating sensitive, protected information that is maintained in the Agency's Supervision, Management and Automated Record Tracking (SMART) case management system.

III. GUIDANCE

A. Protected, Sensitive Information.

Protected, sensitive offender information collected and maintained in SMART includes information on:

- Medical conditions, including AIDS/HIV status;
- Chronic illnesses, such as tuberculosis and cancer;
- Mental health diagnoses, treatment, and prior treatment episodes;
- Substance abuse conditions, treatment, and prior treatment episodes;
- Sex offender treatment and registration;
- Domestic violence treatment;
- Drug testing and DNA testing;
- Social Security Number (SSN);
- Victim information; and
- Informant information.

B. SMART Areas and Screens with Protected, Sensitive Information.

SMART, the Agency's automated case management system, has several areas or screens within SMART where protected, sensitive offender data are collected and stored. These areas/screens and the type of protected, sensitive information include the:

- Basic information screen, which contains data on offender identifiers that are protected, including the Social Security Number (SSN), if the offender has a history of sex offenses and/or a requirement for sex offender registration, and if the offender was DNA tested;
- Notices of Action (NOAs), supervision periods, and special conditions, which may include offender requirements for entry in treatment programs and offender offense history;
- Drug testing data from PRISM, which maintains a history of an offender's drug test results;
- AUTO Screener assessments, which includes information on an offender's physical health, mental health, substance abuse history, sex offense history, domestic violence history, drug testing history, offense history, and special conditions;
- Victim information, including victim contact information;
- CSO referrals and treatment modules, which includes offender referrals for substance abuse, mental health, sex offender, and domestic violence treatment, as well as substance abuse testing;
- Investigative and supervision reports uploaded into SMART, which may include information on an offender's substance abuse history, compliance with previous or former supervision periods, victim information, etc.; and
- Offender profile screen, which shows the offender's SSN, DNA testing and sex offender registration requirements, and special conditions.

Staff authorized to review sensitive, protected information in SMART is limited to staff who are assigned to the offender's Team. Access to sensitive information outside of the Team is prohibited with the exception of Executive Management.

C. SMART Running Record Entries.

SMART running record entries are used by investigation and supervision staff to document chronological notes regarding an offender's assignment for an investigation or supervision period, investigation activities, supervision activities and compliance, collateral contacts, etc.

Running record entries must not contain sensitive, protected information. In particular, the SMART running record is not to contain information on an offender's medical or mental health condition, particularly the offender's AIDS/HIV status; victim information; or, information about the offender being an informant. Running record entries are not to be disseminated to anyone without that individual having made an approved request for such information through the Agency's Freedom of Information Act (FOIA) Officer, and if the request is made via a subpoena request, the records are not to be provided until the Office of General Counsel (OGC) authorizes

the release. Therefore, if you are served a subpoena, forward it to the OGC Helpdesk for consideration.

CSOs are only to review SMART running record entries for offenders under their supervision or if performing as the Duty Officer for another CSO. Also, under no circumstances are staff to review running record entries or other data in SMART for family members, friends, neighbors, etc. For example, if an offender is rearrested and becomes a high profile case, staff are not to access SMART to review the case supervision records unless the staff are the assigned CSO, SCSO, or Branch Chief, or Executive Management.

D. SMART Offender Profile Screen.

The SMART Offender Profile Screen may be shared with the Metropolitan Police Department and other law enforcement personnel without those individuals making special FOIA requests. However, when providing the Offender Profile Screen, CSS staff must ensure that they selected the Hide Sensitive Data button on the top right-hand side of the Offender Profile Screen before printing the Offender Profile Screen. Selecting this button removes the offender's protected SSN and special condition information from the Offender Profile Screen.

E. Disseminating Sensitive, Protected Information.

Agency staff are responsible for ensuring that protected, sensitive information is not disclosed to unauthorized individuals within or external to the Agency, regardless of how the information is maintained (electronically or in hard copy).

Under certain circumstances, sensitive, protected information can be disseminated to authorized individuals. Staff must ensure that the individual receiving the information is authorized. Authorized individuals are those for whom the offender has signed a consent form to release the information or those individuals who are authorized to receive information after having gone through the FOIA process. Staff who are uncertain about the appropriate degree of protection to afford the protected, sensitive information are to request guidance from the OGC, and as noted in section D of this OI, if the request is made via a subpoena, it should be forwarded to the OGC Helpdesk for consideration.

IV. AUTHORITIES, SUPERSEDESURES, REFERENCES, AND ATTACHMENTS

A. Authorities.

D.C. Official Code § 7-302 (Human Health Care and Safety, Reports of Cancer and Malignant Neoplastic Diseases, Confidentiality).

D.C. Official Code § 7-1605 Human Health Care and Safety, Aids Health Care, confidentiality of medical records and information).

D.C. Official Code § 7-1231.10 (Human Health Care and Safety, Mental Health Consumers' Rights Protection, information privacy).

45 CFR Part 164 (Security and Privacy).

42 CFR Part 2 (Confidentiality of Alcohol and Drug Abuse Patient Records).

5 U.S.C. § 552a, The Privacy Act of 1974.

B. Operational Instruction Supersedures.

None.

C. Procedural and Other References.

P.S. 500.2, Safeguarding Sensitive, Unclassified Information, dated 5/5/2000.