Privacy Impact Assessment
for the
Psychology Data System

Issued by:
Sonya D. Thompson
Deputy Assistant Director/CIO

Reviewed by:	Vance E. Hitch, Chief Information Officer, Department of Justice
Approved by:	Nancy C. Libin, Chief Privacy and Civil Liberties Officer, Department of Justice
Date approved:	August 30, 2011

Introduction

The Federal Bureau of Prisons (BOP) protects society by confining offenders in the controlled environments of prisons, and community-based facilities that are safe, humane, and appropriately secure, and which provide work and other self-improvement opportunities to assist offenders in becoming law-abiding citizens.

The Psychology Data System (PDS) is used by the Federal Bureau of Prisons' (BOP's) Psychology Services staff to manage all documentation relevant to inmate mental health including: psychological evaluations and assessments, drug and alcohol abuse treatment, therapy, counseling, and crisis intervention.

PDS also has a Treatment Group component, which is used to manage the clinical treatment groups within the institution (e.g. Drug Education, Sex Offender Treatment, etc.).

The PDS software was originally developed by a contractor but since its original deployment in March of 2005, the PDS has been maintained and managed by BOP staff.

Section 1.0 The System and the Information Collected and Stored within the System.

The following questions are intended to define the scope of the information in the system, specifically the nature of the information and the sources from which it is obtained.

1.1 What information is to be collected?

PDS references and displays the following identifiable information from the Sentry system (the BOP's primary inmate management system):

- Name
- Register Number
- Date of Birth
- Home residence
- Photo

PDS also collects/stores numerous data elements relevant to the inmate's mental health and treatment status.

1.2 From whom is the information collected?

Information is collected from persons committed to the custody of the Attorney General or the Bureau of Prisons, including those sentenced to terms of imprisonment and those in pre-trial custody. Information may also be collected from federal, state, local, foreign and international law enforcement agencies and personnel; federal and state prosecutors, courts and probation services; educational institutions; health care providers; state, local and private corrections

staff; and Bureau staff and institution contractors and volunteers..

Section 2.0 The Purpose of the System and the Information Collected and Stored within the System.

The following questions are intended to delineate clearly the purpose for which information is collected in the system.

2.1 Why is the information being collected?

PDS provides a single-point of storage for inmate mental health assessments, counseling and therapy records, drug treatment records, and psychology treatment program records. This allows for much better continuity of care in a multi-therapist or multi-care provider environment, when compared to a paper-based system.

2.2 What specific legal authorities, arrangements, and/or agreements authorize the collection of information?

18 U.S.C. 4042 and 4082 authorize the BOP to manage inmates committed to the custody of the Attorney General. The Bureau is also responsible for individuals who are directly committed to its custody pursuant to the 18 U.S.C. 3621 and 5003 (state inmates), and inmates from the District of Colombia pursuant to section 11201 of Chapter 1 of Subtitle C of Title XI of the National Capital Revitalization and Self-Government Improvement Act of 1997 (Pub. L. 105-33; 111 Stat. 740).

Per Bureau policy, APA's Ethical Principles of Psychologists and Code of Conduct govern the conduct of psychologists employed by the Bureau of Prisons. Federal Bureau of Prisons. (1993) Program Statement 5310.12, Psychology Services Manual. Psychologists have a professional and ethical responsibility to develop and maintain records (American Psychological Association (APA) Ethics Code, Standard 6.01). Specifically, this standard states:

"Documentation of Professional and Scientific Work and Maintenance of Records: Psychologists create, and to the extent the records are under their control, maintain, disseminate, store, retain, and dispose of records and data relating to their professional and scientific work in order to (1) facilitate provision of services later by them or by other professionals, (2) allow for replication of research design and analyses, (3) meet institutional requirements, (4) ensure accuracy of billing and payments, and (5) ensure compliance with law."
American Psychological Association. (2002b) Ethical Principles of Psychologists and Code of Conduct. *American Psychologist, 57,* 1060-1073.

The Bureau encourages its psychologists to obtain and maintain their professional licensure as a psychologist. The majority of states also require their licensed psychologists to maintain professional records that accurately reflect the licensees' contacts with clients and the results of the services they provide.

Therefore, to adhere to their state's laws/regulations associated with professional licensure, Bureau psychologists need to create the professional records maintained in PDS.

2.3 <u>Privacy Impact Analysis</u>: Given the amount and type of information collected, as well as the purpose, discuss what privacy risks were identified and how they were mitigated.

There is a minimal privacy risk related to the inadvertent disclosure of sensitive information to persons not authorized to receive it. To mitigate this minimal risk, staff are annually trained on how to properly handle sensitive information and annually trained on information security practices and procedures. Access to the system is restricted to BOP employees, interns, and contractors on a "need to know" basis. Information is safeguarded in accordance with Bureau rules and policy governing automated information systems security. Access is only available via the internal BOP network. Established IT security safeguards include the maintenance of records and technical equipment in restricted areas and the required use of strong passwords and unique user IDs to access the system. Only those users who require access to perform their official duties may access the system and record changes are tracked by user ID and a system date/time stamp.

Section 3.0 Uses of the System and the Information.

The following questions are intended to clearly delineate the intended uses of the information in the system.

3.1 Describe all uses of the information.

The information is used to:

- Provide the therapist or treatment specialist with historical context while assessing or treating the inmate.
- Assist in the administration of treatment groups
- Assist management in quantifying inmate population needs, trends and conditions.

See the following System of Records Notice for more detailed information:

BOP-007, "Inmate Physical and Mental Health Records System", 67 FR 11712 (03-15-02); 72 FR 3410 (1-25-07).

3.2 Does the system analyze data to assist users in identifying previously unknown areas of note, concern, or pattern? (Sometimes referred to as data mining.)

No, the system does not data mine.

3.3 How will the information collected from individuals or derived from the system, including the system itself be checked for accuracy?

Data from the system is used operationally each day and is reviewed due to frequent use, monitoring and analysis. System accuracy is assured using program edit checks to prevent data entry errors, e.g. certain fields must be completed, certain fields must be formatted using pre-defined entries, etc.. Data modification is also limited by facility location (i.e. users are limited as to what actions can be performed on data related to an inmate located at another facility).

3.4 What is the retention period for the data in the system? Has the applicable retention schedule been approved by the National Archives and Records Administration (NARA)?

NARA has approved the retention schedule. Authority: **N1-129-05-11**

a. Input. Notes, forms, test scores and other documentation entered into PDS are considered temporary. They are destroyed after verification or when no longer needed for reference purposes, whichever is later.

b. Output. Recurring and one-time reports are considered temporary. They are destroyed when no longer needed for reference purposes.

c. Data is considered "PERMANENT". A complete version of the data is transferred in accordance with the provisions of 36 CFR 1228.270, in five year increments, 85 years after the inmate leaves the system.

d. System documentation. Supporting material such as code books, record layouts, data dictionaries and source codes is considered permanent and a contemporary version is transferred with the data set, in accordance with the provisions noted in c, above.

3.5 <u>Privacy Impact Analysis</u>: Describe any types of controls that may be in place to ensure that information is handled in accordance with the above described uses.

Access to PDS is on a "least privilege" basis, controlled by the BOP's centralized directory authentication security model. All access requests are processed, routed, and logged in the BOP's Helpdesk ticketing system for proper approval and auditing. The BOP's Psychology Services Administrator has overarching authority on PDS access, which is delegated down to the regional psychology administrators and the chief psychologist at each facility.

Section 4.0 Internal Sharing and Disclosure of Information within the System.

The following questions are intended to define the scope of sharing both within

the Department of Justice and with other recipients.

4.1 With which internal components of the Department is the information shared?

Data from this system is not generally shared with any other DOJ component but, data from this system may be disclosed as permitted by law, and for reasons described in the routine uses set forth in the SORN, referenced above.

4.2 For each recipient component or office, what information is shared and for what purpose?

N/A

4.3 How is the information transmitted or disclosed?

N/A

4.4 Privacy Impact Analysis: Given the internal sharing, discuss what privacy risks were identified and how they were mitigated.

N/A

Section 5.0 External Sharing and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to DOJ which includes foreign, Federal, state and local government, and the private sector.

5.1 With which external (non-DOJ) recipient(s) is the information shared?

Data from this system is not shared with non-DOJ recipients.

5.2 What information is shared and for what purpose?

N/A

5.3 How is the information transmitted or disclosed?

N/A

5.4 Are there any agreements concerning the security and privacy of the data once it is shared?

N/A

5.5 What type of training is required for users from agencies outside DOJ prior to receiving access to the information?

N/A

5.6 Are there any provisions in place for auditing the recipients' use of the information?

N/A

5.7 <u>Privacy Impact Analysis</u>: Given the external sharing, what privacy risks were identified and describe how they were mitigated.

N/A

Section 6.0 Notice

The following questions are directed at notice to the individual of the scope of information collected, the opportunity to consent to uses of said information, and the opportunity to decline to provide information.

6.1 Was any form of notice provided to the individual prior to collection of information? If yes, please provide a copy of the notice as an appendix. (A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice.) If notice was not provided, why not?

General notice is provided to inmates through the Systems of Records Notice that was published in 2002 (JUSTICE/BOP-007) regarding the BOP's retention of the type of information maintained in PDS and the permissible disclosures of this information as routine uses under 5 U.S.C. 552a(3). (See Section 3.1 above.)

Notice is provided to all inmates receiving psychology services in accordance with the guidance stated below:

Program Statement 5310.12, Psychology Services Manual, Chapter 2, pg 4-5

B. INMATE/THERAPIST RELATIONSHIP. Except for Rule 12.2, Federal Rules of Criminal Procedure, which deals with the relationship between a psychological examiner and defendant in cases defined by Title 18, U.S. Code, Sections 4241 and 4242, there are no federal statutes specifically defining any privileged relationship between an inmate and his or her therapist. In the past, federal courts have looked to common law and state statutes to define the degree of confidentiality inherent in the therapist/patient relationship. Some states have no law defining therapist/patient relationship. Other states do have laws defining this relationship, although they differ somewhat in terms of degree of privilege or who "owns" the privilege. Therefore, psychologists are encouraged to consult with their State Psychological Association, their Regional Psychologist, and their Regional Counsel to determine the exact degree of confidentiality allowed by law in the state in which they offer therapeutic services.

Psychologists should also be guided in their actions by APA's Ethical Principles of Psychologists and Code of Conduct. Based on this document, confidential information obtained from a therapeutic relationship should not be disclosed without the consent of the individual unless mandated by law. Typically laws will mandate that confidential information be released without the individual's consent

in order to protect the individual or others from harm or in cases where child abuse is suspected.

C. DISCUSSING THE LIMITS OF CONFIDENTIALITY Inmate users of psychological services within the Bureau of Prisons should be informed in advance of any limits to the confidentiality of their contact with psychology staff, (e.g., that the court will receive a report, that there is a duty to warn in certain instances, that information may be shared on occasion with other BOP staff, that psychology records are accessible under specific circumstances, that specific psychological information has been requested by a referring agency, supervisor, or staff member, etc.). Since psychology staff work for many "clients" within the Bureau of Prisons (i.e., the Courts, the Parole Commission, Wardens and other administrative staff, institution staff, and inmates), clearly defining who the client is to all involved parties represents the best "rule of thumb" when providing psychological services within the correctional environment. Information may also be shared with external parties in accordance with the routine uses defined in the aforementioned SORN.

2.3 DUTY TO WARN. General guidelines setting forth the conditions necessary for a therapist's duty to warn were established based upon the landmark decision in Tarasoff v. Regents of the University of California (1968). The duty, as defined by the court in the Tarasoff case, arises when a therapist determines that a client presents a serious danger of violence to another. When such a determination is made, the therapist is obligated to use reasonable care to protect the intended victim against such danger. Subsequent court decisions in other states have rendered slightly differing opinions on the psychologist's duty to warn.

Title 18, U.S. Code, Sections 4243 and 4246 specify that mental health professionals have a duty to recommend hospitalization, through the federal court system, when an individual, because of mental illness, presents a substantial risk of bodily harm to another person or serious damage to the property of another. The Bureau's Health Services Manual defines "substantial risk" as a belief by treatment staff that the inmate will, if released, commit a violent act within six months.

Federal courts have also deferred to the substantive laws of the state in which the psychologist practices to help define duty to warn issues, especially in cases where mental illness is not clearly involved. Therefore, Bureau Psychologists are advised to contact relevant state agencies such as their State Psychological Association and to consult with their Regional Psychologist and Regional Counsel in order to determine how duty to warn issues are interpreted within their state.

The APA's Ethical Principles of Psychologists and Code of Conduct also permits the communication of information obtained in a therapy setting when there is clear and imminent danger to an individual or to society.

In beginning a therapeutic relationship with an inmate, it is mandatory that psychologists clearly establish that this duty to warn exists and place a limitation on the confidentiality of information shared in therapy which threatens another.

6.2 Do individuals have an opportunity and/or right to decline to provide information?

Yes, inmates may refuse to participate in an interview or psychological testing with a mental health clinician. Inmates declining to provide information are informed that their clinical records may be completed without their active participation, based on behavioral observations or review of psychosocial data contained in other records.

6.3 Do individuals have an opportunity to consent to particular uses of the information, and if so, what is the procedure by which an individual would provide such consent?

Individuals do not have the opportunity to consent to routine uses of the information, e.g. disclosure to law enforcement personnel, the judiciary, etc.. Under provisions of the Freedom of Information Act, inmates may authorize the non-routine release of their clinical records to outside parties by making a request in writing. Inmates may also request a copy of their own records. Exemptions from Freedom of Information provisions are made on a case-by-case basis, depending on the content of the clinical record. For example, clinical records containing the names of other inmates (second parties) may be exempted from FOIA because this information may affect the privacy of the second party.

6.4 <u>Privacy Impact Analysis</u>: Given the notice provided to individuals above, describe what privacy risks were identified and how you mitigated them.

The privacy risk identified would be the failure of persons to know their information may be collected and what it will be used for. BOP has published a Privacy Act System of Records Notice (SORN). The information in this notice includes entities with which and situations when BOP may share these records. This notice, therefore, mitigates the risk that the individual will not know why the information is being collected or how the information will be used.

Section 7.0 Individual Access and Redress

The following questions concern an individual's ability to ensure the accuracy of the information collected about him/her.

7.1 What are the procedures which allow individuals the opportunity to seek access to or redress of their own information?

Per BOP policy, inmates may request access to their information by submitting a request in writing. The applicable clinical services director may elect to allow inmates to visually review his or her record, or will provide a copy of the record upon request, contingent of a review to determine whether any exemptions apply.

Inaccuracies in the clinical record identified by the inmate may be reported to

clinical staff, and they may be corrected, at the discretion of the treating clinician. However, clinical records can only be modified within 30 days of data entry. In cases where an inmate seeks redress pertaining to records outside of this time frame, the clinical record cannot be changed by altering the original text. Clarifying or corrective information, with necessarily required documentation, is made as a separate entry in the clinical record.

7.2 How are individuals notified of the procedures for seeking access to or amendment of their information?

Inmates receive notification of the procedures for filing grievances as part of the admission into each facility (i.e. the Admission and Orientation program). The relevant BOP policies regarding the Administrative Remedy Program and FOIA are also available in each institution law library. Information about how to file requests for records is contained in the applicable System of Records Notices and departmental regulations. Procedures are also verbally described to inmates whenever they seek access to their clinical information.

7.3 If no opportunity to seek amendment is provided, are any other redress alternatives available to the individual?

See response to question 7.2 above.

7.4 Privacy Impact Analysis: Discuss any opportunities or procedures by which an individual can contest information contained in this system or actions taken as a result of agency reliance on information in the system.

See questions 7.1 and 7.2 above.

Section 8.0 Technical Access and Security

The following questions are intended to describe technical safeguards and security measures.

8.1 Which user group(s) will have access to the system?

PDS has four user groups:

- Read Only: Allows the user to view all data in the system, but not make changes. This role will be assigned to medical staff and/or executive staff with a need-to-know.
- Standard Access: Allows the user to make entries into the inmate record, as well as view existing data. This access is given to all members of the Psychology Services staff at each facility.
- Administrator Access: This role is usually assigned to the Chief Psychologist at every facility. In addition to viewing and editing inmate records, a user in this group will have the ability to control the document creation/review capability for users at his/her facility.
- System Administrator: This group controls system-wide look-up lists,

document data fixes, and messages of the day. Currently there are two users in this group at the agency headquarters.

8.2 Will contractors to the Department have access to the system? If so, please submit a copy of the contract describing their role with this PIA.

Contract phsychology personnel or psychology interns may have access to the system after an appropriate security background clearance has been obtained.

8.3 Does the system use "roles" to assign privileges to users of the system?

System roles are assigned to the user groups, as described in 8.1, above.

8.4 What procedures are in place to determine which users may access the system and are they documented?

PDS was specifically designed for the Psychology Services staff. Anyone outside of the Psychology Services program area that requires access, and has a need-to-know, must make a written request to the Chief Psychologist at his/her facility. If the request is approved by the facility Chief Psychologist, a helpdesk ticket is generated, and the user is added to the appropriate user group in the enterprise directory by the local computer services manager.

8.5 How are the actual assignments of roles and rules verified according to established security and auditing procedures?

PDS access at each facility is approved by the local Chief Psychologist. The Chief Psychologist cannot actually enroll users, however; enrollment is performed by the local computer services manager. If a request for access is received by the computer services manager which does not conform to standard operating procedure (e.g., the request is for a correctional officer), the computer services manager will investigate the validity of the request with the Chief Psychologist.

Similarly, since the Chief Psychologist can see who has local access to PDS, the Chief Psychologist can also audit accounts with the CSM as to why a specific user is accessing the system.

8.6 What auditing measures and technical safeguards are in place to prevent misuse of data?

Access to the system is strictly limited to those with a need-to-know and is controlled via userID and password . Data transmission is protected using SSL encryption.

8.7 Describe what privacy training is provided to users either generally or specifically relevant to the functionality of the program or system?

Users are trained as to the sensitive nature of the data within the system and continuously reminded of the need to strictly control the viewing and/or output of data from the system. BOP users are trained annually regarding the handling of

sensitive information and information security requirements. All employees who are involved in the management, operation, programming, maintenance, or use of a DOJ information system are made aware of the threats to and vulnerabilities of those systems and their responsibilities with regard to privacy and information security.

8.8 Is the data secured in accordance with FISMA requirements? If yes, when was Certification & Accreditation last completed?

Yes, the data is secured in accordance with FISMA requirements. The Certification and Accreditation for the parent system BOPNet was last updated on October 21, 2008.

8.9 <u>Privacy Impact Analysis</u>: Given access and security controls, what privacy risks were identified and describe how they were mitigated.

It was critical that only those with a need-to-know were given access to PDS. The application environment provides a strong security infrastructure to mitigate any risks of unauthorized access. Also, the separation of duties for the access process provides a procedural "check-and-balance" between two program areas.

Section 9.0 Technology

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, RFID, biometrics and other technology.

9.1 Were competing technologies evaluated to assess and compare their ability to effectively achieve system goals?

Many correctional systems use paper-based mechanisms to log and monitor their inmate populations; others use local or decentralized databases. The BOP decided to establish an operational, centralized database which could provide staff with accurate, real-time information. Because PDS resides on the BOP's intranet platform (BOPWare), the system design required that it be web-based, J2EE compliant, store data on the mainframe, and utilize the BOP's LDAP infrastructure for access control.

9.2 Describe how data integrity, privacy, and security were analyzed as part of the decisions made for your system.

BOP policy and APA ethics dictate that the BOP treat psychology records in accordance with industry practice and standards. Additionally, in leveraging the BOP's security infrastructure, the application takes advantage of SSL encryption, strong password authentication, data backups, clustered application servers, and an established standard user enrollment process.

Note, however, as described in 6.1 above, an inmate's right to privacy is not identical to what he/she can expect in a setting outside of the prison.

9.3 What design choices were made to enhance privacy?

The system follows general BOP system guidance: access is controlled via the BOP's LDAP infrastructure; user access is via the "least privilege" model; data views are restricted by whether the inmate is geographically present, and account authorization includes an ability to audit approvals by using the helpdesk system.

Conclusion

PDS was deployed in 2005 in an effort to improve the management of inmate mental health data. Due to strict security and limiting access to the information, the agency has improved protections regarding the privacy of records as compared to the previous paper-based system.