Federal Bureau Of Prisons

Privacy Impact Assessment
for the
Bureau Electronic Medical Records Initiative

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

Reviewed by:	Luke J. McCormack, Chief Information Officer, Department of Justice
Approved by:	Joo Y. Chung, Acting Chief Privacy and Civil Liberties Officer, Department of Justice
Date approved:	September 25, 2013

Section 1: Description of the Information System

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 BOP's Bureau Electronic Medical Records System (BEMR) provides for the collection, storage, maintenance, analysis, and dissemination of comprehensive electronic medical records for more than 200,000 offenders remanded for federal custody. The system overall includes an inmate's medical, social, and psychological history and ongoing data and related informational records. The Bureau Pharmacy System (BEMRx), integrated with BEMR, collects and stores pharmaceutical records, including prescription and dosage information. Also, the Psychology Data System (PDS), formerly a separate system, is now being integrated into BEMR as well. PDS is used to manage all documentation relevant to inmate mental health, including psychological evaluations and assessments, drug and alcohol abuse treatment, therapy, counseling, and crisis intervention. It also has a Treatment Group component, which is used to manage the clinical treatment groups within an institution (e.g., Drug Education, Sex Offender Treatment, etc.).

Specific personally identifying information (PII) collected in BEMR includes:

- Name,
- Inmate federal register number,
- Date of birth,
- Social Security number,
- Medical, lab, radiology and psychological records.

Access to each system is limited to those persons who have an appropriate security clearance and are authorized to review such information for their official duties, which is regularly reviewed. User access is restricted to those staff who need to view and upload data, and user roles are defined to limit capability (e.g., only pharmacists are authorized to fill and dispense prescriptions). System access is web-based using a unique userID and password. All transmissions of data are encrypted using 128-bit SSL encryption.

The following systems data and software is planned to be integrated with BEMR at a future date:

1. **Bureau Laboratory Information System (LIS):** collects and stores lab tests and results.
2. **Digital Teleradiology System (MedWeb):** collects and stores radiology tests and read results.

The above systems include applicable medical peripheral devices such as barcode scanners, clinical decision-making software, and automated medication dispensing equipment, which may be interconnected to the systems.

At present, BEMR is interconnected with LIS and BOP's SENTRY inmate management system. The interconnection enables the retrieval of inmate demographic information and enables sharing of data to the Special Housing Unit (SHU) application for tracking SHU reviews by psychology staff. BEMR is also interconnected with the Bureau's Trust Fund Accounting System (TRUFACS) to share data regarding inmate medical co-pays and to allow inmates to request prescription refills electronically. Teleradiology is scheduled for a future date to be interconnected to BEMR.

Section 2: Information in the System

2.1 Indicate below what information is collected, maintained, or disseminated. (Check all that apply.)

Identifying numbers					
Social Security	X	Alien Registration		Financial account	
Taxpayer ID		Driver's license		Financial transaction	
Employee ID		Passport		Patient ID	
File/case ID		Credit card			
Other identifying numbers (specify):	X	Inmate federal register number			

General personal data					
Name	X	Date of birth	X	Religion	
Maiden name		Place of birth	X	Financial info	
Alias		Home address		Medical information	X
Gender	X	Telephone number		Military service	
Age	X	Email address		Physical characteristics	X
Race/ethnicity	X	Education	X	Mother's maiden name	
Other general personal data (specify):	X	Psychology evaluations and treatment plans, drug treatment assessments and treatment plans			

Work-related data					
Occupation	X	Telephone number		Salary	
Job title		Email address		Work history	
Work address		Business associates			
Other work-related data (specify):	X	Inmate's ability or limitations regarding fitness for work			
Distinguishing features/Biometrics					
Fingerprints		Photos	X	DNA profiles	
Palm prints		Scars, marks, tattoos	X	Retina/iris scans	
Voice recording/signatures		Vascular scan		Dental profile	X

Work-related data	
Other distinguishing features/biometrics (specify):	

System admin/audit data								
User ID	X	Date/time of access	X	ID files accessed				
IP address	X	Queries run	X	Contents of files				
Other system/audit data (specify):	X	User job title is displayed next to the user's name for psychology encounters.						

Other information (specify)	

2.2 Indicate sources of the information in the system. (Check all that apply.)

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

Government sources							
Within the Component		X	Other DOJ components		X	Other federal entities	X
State, local, tribal		X	Foreign		X		
Other (specify):							

Non-government sources					
Members of the public		Public media, internet		Private sector	X
Commercial data brokers					
Other (specify):	X	Outside hospital providers; Private Corrections Contractors who house BOP offenders			

2.3 Analysis: Now that you have identified the information collected and the sources of the information, please identify and evaluate any potential threats to privacy that exist 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 systems include design choices to ensure that privacy protections are ensured for the sensitive information (medical and mental health data) stored therein. For example, the system uses role-based management to ensure that users can only access and manipulate data in relation to their functional duties. Considerations were also made regarding the security and protection of such data to ensure that the systems comply with applicable privacy regulations and requirements for the protection of medical data. For example, the system is designed to ensure that inmate treatment is maintained in the same record regardless of whether an inmate's period of confinement is interrupted by release.

There is a privacy risk related to the inadvertent disclosure of sensitive information to persons not authorized to receive it. To mitigate this risk, staff is annually trained on how to properly handle sensitive information. Non-BOP users (e.g., private corrections staff, contract medical staff, etc.) are required to undergo information security awareness training prior to gaining access to a system or data. Access to any relevant system is limited to those persons who have an appropriate security clearance, which is regularly reviewed and who have an official need to access such information.

Information is safeguarded in accordance with Bureau rules and policy governing automated information systems security and access. These safeguards include the maintenance of records and technical equipment in restricted areas, and the required use of proper passwords and user identification to access the system. Data transmission in the system is also encrypted.

Section 3: Purpose and Use of the System

3.1 Indicate why the information in the system is being collected, maintained, or disseminated. (Check all that apply.)

Purpose			
X	For criminal law enforcement activities		For civil enforcement activities
	For intelligence activities	X	For administrative matters
X	To conduct analysis concerning subjects of investigative or other interest		To promote information sharing initiatives

X	To conduct analysis to identify previously unknown areas of note, concern, or pattern.		For administering human resources programs
	For litigation		
X	Other (specify): Reporting infectious diseases to CDC or state health departments		

3.2 Analysis: Provide an explanation of how the component specifically will use the information to accomplish the checked purpose(s). Describe why the information that is collected, maintained, or disseminated is necessary to accomplish the checked purpose(s) and to further the component's and/or the Department's mission.

The BOP provides essential medical, dental, and mental health services in a manner consistent with accepted community standards for a correctional environment. The Bureau uses licensed and credentialed health care providers in its ambulatory care units, which are supported by community consultants and specialists. For inmates with chronic or acute medical conditions, the Bureau operates several medical referral centers providing advanced care.

The information is used to manage and provide medical/psychological care and services for the BOP inmate population. It may also be used for administrative purposes (e.g., billing purposes for outside community providers), to report infectious diseases to state health departments and/or the CDC, to provide information to the judiciary or an adjudicative body when records are relevant, and to evaluate the quality of care provided to the inmates.

The information is thus collected to ensure that the BOP delivers medically necessary health care to inmates effectively in accordance with proven standards of care without compromising public safety concerns inherent to the Bureau's overall mission.

3.3 Indicate the legal authorities, policies, or agreements that authorize collection of the information in the system. (Check all that apply and include citation/reference.)

Authority		Citation/Reference
X	Statute	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 18 U.S.C. 3621 and 5003 (state inmates), and inmates from the District of Columbia 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).
	Executive Order	
	Federal Regulation	
	Memorandum of Understanding/agreement	
	Other (summarize and provide copy of relevant portion)	

3.4 Indicate how long the information will be retained to accomplish the intended purpose, and how it will be disposed of at the end of the retention period. (Reference the applicable retention schedule approved by the National Archives and Records Administration, if available.)

- Data in BEMR and the LIS is stored for 30 years after the expiration of the inmate's sentence.
    - The applicable authority has been approved by NARA (Authority # N1-129-09-15).
- Data in the Teleradiology system is stored as follows:
    - X-ray digital images. Disposition: Temporary. Destroy 5 years after expiration of sentence.
    - X-ray reports and X-ray metadata including but not limited to an inmate's name, register number, sentence information, examination, date, referring physician or facility, analysis reports, and system-generated fielded information. Disposition: Temporary. Destroy 30 years after expiration of sentence.
    - Un-scanned X-ray film. Disposition: Temporary. Destroy 5 years after creation.
    - The retention schedule has been approved by NARA (Authority # N1-129-09-13).

3.5 Analysis: 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.)

Access to each system is limited to those persons who have an appropriate security clearance and are authorized to review such information for their official duties. User access privileges are regularly reviewed. Access is granted on a "least privilege" basis (i.e., users have access to only that information necessary to do their jobs), controlled by BOP's centralized directory authentication model. All access requests are processed, routed, and logged in BOP's helpdesk ticketing system for proper approval and auditing. Information in the system is safeguarded in accordance with Bureau rules and policy governing automated information systems security.

System transaction errors and exceptions are logged and reviewed on a routine basis. Data edit checks are included in program code to ensure appropriate and accurate entry of data. Staff is routinely trained on the use and handling of information in the system, including annual training on information security and handling of sensitive information. Contractors with access to a system (i.e., private corrections staff and outside medical hospital staff) are required to undergo information security awareness training prior to being granted access to a relevant system. Contracts (statements of work) also include provisions requiring contract staff to safeguard and protect information consistent with federal privacy requirements.

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information in the system and how the information will be shared, such as on a case-by-case basis, bulk transfer, or direct access.

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Within the component	X	X	X	
DOJ components	X			
Federal entities	X			
State, local, tribal gov't entities	X			
Public				
Private sector	X			X - Outside medical providers
Foreign governments	X			
Foreign entities				

Recipient	How information will be shared			
	Case-by-case	Bulk transfer	Direct access	Other (specify)
Other (specify):		X		X - Blue Cross/Blue Shield for medical bill adjudication

4.2 Analysis: Disclosure or sharing of information necessarily increases risks to privacy. Describe controls that the component has put into place in order to prevent or mitigate threats to privacy in connection with the disclosure of information. (For example: measures taken to reduce the risk of unauthorized disclosure, data breach, or receipt by an unauthorized recipient; terms in applicable MOUs, contracts, or agreements that address safeguards to be implemented by the recipient to ensure appropriate use of the information – training, access controls, and security measures; etc.)

Memoranda of Agreement or Statements of Work (contracts) restricts use of the data for only authorized purposes and prohibits further redistribution of the data. Outside medical providers are also subject to federal medical privacy rules such as the Health Information Portability and Accountability Act (HIPAA).

Users are notified of rules and procedures regarding access and use of the information via contract and information security briefings. Outside medical providers are separately subject to HIPAA privacy requirements, which require annual training for employees of covered entities. Sharing of data increases the privacy risks of unauthorized access and modification and misuse. In addition, mitigating controls are employed so that any data entry by non-BOP personnel is only performed by select medical personnel and inmates have the opportunity to consent to certain disclosures of the information.

External sharing of data also increases the privacy risks of unauthorized access and modification and misuse. Additional mitigating controls include: HIPAA requirements in certain circumstances; individuals have the opportunity to consent to certain disclosures of the information; and MOAs and SOWs prescribe the security and privacy requirements of data once it is shared.

Section 5: Notice, Consent, and Redress

5.1 Indicate whether individuals will be notified if their information is collected, maintained, or disseminated by the system. (Check all that apply.)

X	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 7.

X	Yes, notice is provided by other means.	Specify how: Admission and Orientation sessions conducted when the inmate first arrives at an institution.
	No, notice is not provided.	Specify why not:

5.2 Indicate whether and how individuals have the opportunity to decline to provide information.

	Yes, individuals have the opportunity to decline to provide information.	Specify how:
X	No, individuals do not have the opportunity to decline to provide information.	Specify why not: Information is required to be provided as part of the sentencing process, the initial intake and screening of the individual into custody, the re-admittance of the individual back into custody, or the release of the individual into the community. Note: inmates have the right to refuse treatment.

5.3 Indicate whether and how individuals have the opportunity to consent to particular uses of the information.

X	Yes, individuals have an opportunity to consent to particular uses of the information.	Specify how: Individuals have the opportunity to consent to any disclosures unrelated to the routine uses specified in the SORN in Section 7.1 below. If the request for information is non-routine and the inmate has not previously provided consent, the inmate will be contacted to notify him/her of the request and determine if they consent to the disclosure. The inmate can decline access to the information. Examples of non-routine use would be a reporter requesting access to an inmate's medical records; a member of the public who is seeking copies of inmate medical records via a FOIA request, or an inmate seeking access to the medical records of another fellow inmate.

X	No, individuals do not have the opportunity to consent to particular uses of the information.	Specify why not: Inmates are required to provide certain information as part of the sentencing process, the initial intake and screening of the individual into custody, the re-admittance of the individual back into custody, or the release of the individual into the community. Individuals do not have the opportunity to consent to routine uses of the information in association with those purposes (e.g., disclosure to the U.S. Probation Office or local law enforcement, judges, or outside hospital personnel for purposes of medical treatment, etc.)

5.4 Analysis: Clear and conspicuous notice and the opportunity to consent to the collection and use of individuals' information provides transparency and allows individuals to understand how their information will be handled. Describe how notice for the system was crafted with these principles in mind, or if notice is not provided, explain why not. If individuals are not provided the opportunity to consent to collection or use of the information, explain why not.

Some information in the system is collected from the individual as part of the pre-sentence investigation process, the intake process when the inmate is admitted to custody, and the release process when the inmate is returning to the community. Notice regarding information collected by BOP personnel is provided through publication of the applicable System of Records Notices. Inmates are also advised of health services and psychology treatment procedures as part of the Admission and Orientation process which occurs at all BOP institutions.

Section 6: Information Security

6.1 Indicate all that apply.

X	The information is secured in accordance with FISMA requirements. Provide date of most recent Certification and Accreditation: January 2013 If Certification and Accreditation has not been completed, but is underway, provide status or expected completion date:
X	A security risk assessment has been conducted.

X	Appropriate security controls have been identified and implemented to protect against risks identified in security risk assessment. Specify: Authentication occurs via unique userIDs and passwords; change management is tracked and logged; and system maintenance activities are logged.
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: Documentation is audited upon peer review, program review, Joint Commission surveys, and ACA audits. Access to certain sensitive information requires specific authorization and is limited to select personnel. Review and input of inmate medical data is technically restricted to those that directly provide care to the individual inmate or have a need to know.
X	Auditing procedures are in place to ensure compliance with security standards. Specify, including any auditing of role-based access and measures to prevent misuse of information: User access is audited on an annual basis and information is audited as part of ACA and Joint Commission reviews.
X	Contractors that have access to the system are subject to provisions in their contract binding them under the Privacy Act.
X	Contractors that have access to the system are subject to information security provisions in their contracts required by DOJ policy.
X	The following training is required for authorized users to access or receive information in the system:

X	General information security training
X	Training specific to the system for authorized users within the Department.
X	Training specific to the system for authorized users outside of the component.
	Other (specify):

6.2 Describe how access and security controls were utilized to protect privacy and reduce the risk of unauthorized access and disclosure.

System roles are assigned and privileges to view data are based on such roles. User access for an employee must be requested by an applicable medical or psychology supervisor indicating that access is required for the performance of their duties. User access for a contractor is requested by the applicable program/project manager. The request and subsequent access is documented in the BOP HelpDesk system. Access to certain sensitive information requires specific authorization and is limited to select personnel. Review and input of inmate medical data is technically restricted to those that directly provide care to the individual inmate or have a need to know.

Users are trained as to the sensitive nature of the data within the systems and continuously reminded as to the need to strictly control the viewing and/or output of data from the systems. 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.

All contractors and volunteers who access Bureau information or systems are required to attend initial security awareness and training during orientation. Contractors and volunteers also receive 45-minute refresher security awareness training during annual training sessions. The Information Security Programs Office is responsible for providing the information on security requirements, procedures, and configuration management necessary to conduct the initial briefings for all users. External users are trained as to the use of the system and are required to sign and acknowledge Rules of Behavior before access is granted. Memoranda of Agreements with external agencies also require the appointment of an information security coordination to enforce the security and privacy aspects of the sharing program.

Section 7: Privacy Act

7.1 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. (Check the applicable block below and add the supplementary information requested.)

X	Yes, and this system is covered by an existing system of records notice. Provide the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system: • BOP-005, Inmate Central Records System, 67 Fed. Reg 31371 (May 9, 2002); 72 Fed. Reg. 3410 (Jan. 25, 2007); 77 Fed. Reg. 24982 (April 26, 2012); 78 Fed. Reg. 11575 (Feb. 19, 2013). • BOP-007, Inmate Physical and Mental Health Record System, 67 Fed. Reg. 11712 (March 15, 2002); 72 Fed. Reg. 3410 (Jan. 25, 2007).
	Yes, and a system of records notice is in development.
	No, a system of records is not being created.

7.2 Analysis: Describe how information in the system about United States citizens and/or lawfully admitted permanent resident aliens is or will be retrieved.

Information is retrieved from the system by federal register number or inmate name.