Federal Bureau of Prisons

Privacy Impact Assessment
for the
Bureau Electronic Records Initiative

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 Bureau's electronic medical records initiative includes the following systems for the management of health information for federal inmates:

- The Bureau Electronic Medical Records System (BEMR): collects and stores medical and dental history and examination records, and diagnosis and treatment notes.
- The Bureau Pharmacy System (BEMRx): collects and stores pharmaceutical records, including prescription and dosage information. Integrated with BEMR.
- The Bureau Laboratory Information System (LIS): collects and stores lab tests and result. System data will be integrated with BEMR/BEMRx; and,
- The digital teleradiology system (MedWeb): standalone system collects and stores radiology tests and read results.

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?

The Bureau's electronic medical records systems provide for the collection, storage, maintenance, analysis and dissemination of comprehensive electronic medical records for more than 200,000 offenders remanded for federal custody. The systems include the inmate's medical, social and psychological history and ongoing medical social, and psychological data and informational records.

Specific personally identifying information (PII) collected includes:

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

1.2 From whom is the information collected?

The information is collected from persons committed to the custody of the Attorney General and 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; 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?

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

The information is collected to ensure that the Health Services Division (HSD) of the Federal Bureau of Prisons 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.

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

18 U.S.C. 4003, 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).

2.3 Privacy Impact Analysis: 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 privacy risk related to the inadvertent disclosure of sensitive information to the persons not authorized to receive it. To mitigate this risk, staff are annually trained on how to properly handle sensitive information. Access to the relevant system is limited to those persons who have an appropriate security clearance which is regularly reviewed.

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 codes to access the system. Only those Bureau personnel who require access to perform their official duties may access the system equipment and the information in the system. Data transmission is also encrypted.

There is also a risk of unauthorized data modification and misuse. This risk is mitigated by enforcing access controls and encryption (as described above) and by providing auditing of user and system administration activities.

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 manage and provide medical 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. See the following System of Records Notices for a detailed list of uses:

- BOP-005, Inmate Central Records System, 67 Fed. Reg 31371 (2002); 72 Fed. Reg. 3410 (2007);
- BOP-007, Inmate Physical and Mental Health Record System, 67 Fed. Reg. 11712 (2002); 72 Fed. Reg. 3410 (2007).

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.)

The systems do 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 systems is used operationally each day and is “cleansed” (i.e. due to frequent use, monitoring and review, information is continuously monitored for accuracy and updated or corrected as needed). System accuracy is assured using program edit checks to prevent data entry errors. Data entry is also limited to users

that provide services to a specific location. Inmates are also free to request record information via a Freedom of Information (FOIA) request to review accuracy of information contained in the relevant system. Inmates may request their record be amended if they believe there is an error. Even if the information is not amended, the inmate's request will be filed as part of the record.

Chart reviews are conducted monthly at each institution by health information and clinical staff. Documentation is also audited upon peer review, program review, Joint Commission surveys and American Correctional Association audits.

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)?

Data in BEMR, BEMRx, 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 # N1-129-08-15).

Data in the Teleradiology system is stored as follows:

(1) X-ray digital images

Disposition. Temporary. Destroy 5 years after expiration of sentence.

(2) 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.

(3) 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 Privacy Impact Analysis: 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 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. Information is safeguarded in accordance with Bureau rules and policy governing automated information systems security and. 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 are routinely trained on the use and handling of information in the system.

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 these systems is shared with the United States Marshal Service and the Office of Federal Detention Trustee (OFDT) to ensure the continuation of medical care during inmate transport and temporary custody exchange. In the future, information may be shared with various other law enforcement components within the Department of Justice including the FBI, EOUSA, Criminal Division, U.S. Parole Commission and Office of Inspector General.

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

Data regarding required medications, diagnoses, and expected treatments are provided to the USMS to ensure a continuum of care during physical custody transfers. Services and treatment information is also provided to OFDT to estimate budgetary costs and calculate reimbursement expenses. The data may also be shared for law enforcement and court-related purposes such as investigations, possible criminal prosecutions, civil court actions, or regulatory or parole proceedings.

4.3 How is the information transmitted or disclosed?

Information is printed and provided to such offices via email, fax or in hard copy. Information is handled in accordance with information security policy and directives relating to the handling of sensitive information. Information may also be made available electronically for viewing from the relevant system by authorized users within the respective agency. Data transmission within DOJ is encrypted. Certain agencies may receive batch downloads of data for integration with other automated systems.

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

There is a privacy risk related to the inadvertent disclosure of sensitive information to the persons not authorized to receive it. To mitigate this risk, access to the relevant system is limited to those persons who have an appropriate security clearance which is regularly reviewed. Users are trained as to the use of the system and information is safeguarded in accordance with BOP and DOJ rules and policy governing automated information systems security and access as well as medical privacy rules. These safeguards include the maintenance of records and technical equipment in restricted areas, and the required use of proper passwords and user identification codes to access the relevant system, the use of encryption for data transmissions, appropriately labeling hard copy materials to alert staff as to the sensitive nature of the data, storing hard copy printouts in secure, locked locations, and requiring authorization to remove hardcopy materials from the workplace. Sharing of data also increases the privacy risks of unauthorized access and modification and misuse. Additional mitigating controls include: data entry is only performed by select BOP medical personnel and individuals have the opportunity to consent to certain non-routine uses of the information.

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?

Information is shared with private corrections contractors who are authorized to manage federal inmates on behalf of the BOP and who are bound by the Privacy Act pursuant to the contract (FAR 24.104). Information may be shared via hard copy or eventually, direct access to the BEMR system. Information from a medical system is also shared with private medical care providers to provide treatment or emergency medical service to inmates transported outside the BOP facility. Information from a medical system may also be shared with federal, state, local, tribal, foreign and international law enforcement agencies and court officials. Information may also be shared with other non-DOJ entities in accordance with the aforementioned System of Records Notices.

5.2 What information is shared and for what purpose?

Information from the system is shared with private corrections contractors and private medical care providers to ensure a consistent continuum of care while federal inmates are within the physical custody of such entities. Information from the system may also

be shared for law enforcement and court-related purposes such as investigations, possible criminal prosecutions, civil court actions, or regulatory or parole proceedings, and, prior to release of an inmate, to the chief law enforcement officer of the state and local jurisdiction in which the released inmate will reside, as required by 18 U.S.C. 4042(b). Information is also shared for other purposes in accordance with published System of Records Notices.

5.3 How is the information transmitted or disclosed?

Information is printed and provided to such offices in hard copy. Hard copy information is handled in accordance with information security policy and directives relating to the handling of sensitive information. Information may also be made available electronically for viewing in the relevant system by authorized users within the respective entity. Data transmission is SSL-encrypted. Certain federal agencies may also receive batch downloads of data for integration with other automated systems in accordance with a Memorandum of Agreement or Statement of Work.

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

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

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

Users are notified of rules and procedures regarding access and use of the information via contract and information security briefings. Medical providers are separately subject to HIPAA privacy requirements, which require annual training for employees of covered entities.

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

Memoranda of Agreement and Statement of Works would include requirements for the recipient agency to review and monitor use of medical information. System transactions would also be logged and exception reports routinely reviewed.

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

There is a privacy risk related to the inadvertent disclosure of sensitive information to the persons not authorized to receive it. To mitigate this risk, access to the relevant system is limited to those persons who have an appropriate security clearance which is regularly reviewed. Users are trained as to the use of the relevant system and information is safeguarded in accordance with BOP and DOJ rules and policy governing automated information systems security and access. These safeguards include the maintenance of records and technical equipment in restricted areas, the required use of proper passwords and user identification codes to access the system, the use of encryption for data transmissions, appropriately labeling hard copy materials to alert staff as to the sensitive nature of the data, storing hard copy printouts in secure, locked locations, and requiring authorization to remove hardcopy materials from the workplace.

Sharing of data also increases the privacy risks of unauthorized access and modification and misuse. Additional mitigating controls include: data entry is only performed by select medical personnel and individuals have the opportunity to consent to non-routine uses 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 imposed on outside medical providers regarding the protection of medical information; individuals have the opportunity to consent to non-routine uses of the information; and MOAs and SOWs exist concerning the security and privacy of data once it is shared.

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?

Some information in the systems is collected from the individual as part of the presentence investigation process. Notice regarding information collected by BOP

personnel is provided through applicable System of Records Notices. (See Section 3.1 above.). Inmates are also advised of health services procedures as part of the Admission and Orientation process.

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

No. 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.

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.. Individuals have the opportunity to consent to certain non-routine uses of the information pursuant to the Privacy Act, 5 USC Section 552a, e.g. disclosure to an academic institution or congressperson with whom the inmate wishes to disclose his or her personal information.

6.4 Privacy Impact Analysis: 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 Privacy Act System of Records Notices (SORNs) for BOP's inmate records. The information in these notices includes entities with which and situations when BOP may share investigative 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?

Inmates may file an administrative grievance in accordance with 28 CFR Section 542.10. This program allows an inmate to seek redress for any aspect of his/her confinement, including the accuracy of information collected about him/her. Inmates

may seek access to information about themselves by filing a Privacy Act Request.

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 Privacy Act are also available in each institution law library.

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

N/A. See 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 question 7.1 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?

BOP and DOJ staff with a need to access the relevant system to carry out their duties may be approved for access to the system. External agency users who are approved and have an appropriate security clearance may access the applicable system.

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.

Staff employed by private prison contractors housing BOP inmates have access to the BEMR/BEMRx systems. Statements of work include a clause binding the contractors to comply with the Privacy Act (FAR 24.104). Contractors who develop and support system applications also have access to the system. Relevant statements of work for development include a requirement that contractors adhere to and comply with DOJ IT security policies.

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

Yes, system roles are assigned and privileges to view data are based on such roles.

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

User access for an employee must be requested by a medical supervisor indicating that access is required for the performance of their duties. The request and subsequent access is documented in the BOP HelpDesk system.

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

Access to the relevant system is granted by the appropriate supervisory medical official. System account creation and removal is documented via the Help Desk system. Each user's access is reviewed and recertified, if appropriate.

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

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.

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 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 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.

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. Authority to Operate was granted by the CIO in August 2009. The final Certification and Accreditation was completed January 2010.

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

There is a privacy risk related to the inadvertent disclosure of sensitive information to the persons not authorized to receive it. To mitigate this risk, access to the systems is limited to those persons who have an appropriate security clearance which is regularly reviewed. Users are trained as to the use of the systems and information is safeguarded in accordance with BOP and DOJ rules and policy governing automated information systems security and access, e.g. update transactions are only available to certain approved users and timeout/inactivity restrictions are in place. These safeguards also include the maintenance of records and technical equipment in restricted areas, and the required use of proper passwords and user identification codes to access the systems. Data transmission is also encrypted.

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?

The BOP conducted an extensive market analysis and review to evaluate available technologies to fulfill its electronic medical records initiative, including government-owned systems, commercial-off-the-shelf products and custom development. The final

selection made use of an existing COTS product which is being extensively customized for BOP use and operations.

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

Risk management was addressed initially through a feasibility study performed by a project review team. Development was also structured to minimize risks; the design phase included extensive input and meetings with subject matter staff and end-users. Prior to full implementation, a pilot was performed first at one and then another institution. Ongoing management and project reviews occur on a monthly basis to monitor operational successes, impacts and deficiencies.

9.3 What design choices were made to enhance privacy?

The systems have always included design choices to ensure that privacy protections are ensured for the sensitive information (medical data) stored therein. 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.

Conclusion

The Bureau's electronic medical records initiative continues to evolve, utilizing currently available web technologies integrated with state-of-the-art database management and transaction processing augmented with automated medical devices and systems (pharmacy, laboratory, x-ray, etc.).