Federal Bureau of Prisons

Privacy Impact Assessment
for the

Federal Bureau of Prisons
Medical Claims Adjudication (MCA) System

Issued by:
Sonya D. Thompson
Assistant Director / CIO

Approved by: Peter Winn
Chief Privacy and Civil Liberties Officer (Acting)
U.S. Department of Justice

Date approved: February 1, 2023

(May 2019 DOJ PIA Template)

[This PIA should be completed in accordance with the DOJ Privacy Impact Assessments Official Guidance (and any supplemental guidance) at https://www.justice.gov/opcl/file/631431/download.] The following questions are intended to define the scope of the information in the information technology, specifically the nature of the information and the sources from which it is obtained. The responses should be written in plain language and should be as comprehensive as necessary to describe the information technology.]

Section 1: Executive Summary

Provide a high-level overview of the information technology (e.g., application, tool, automated process) in non-technical terms that describes the information technology, its purpose, how the information technology operates to achieve that purpose, the general types of information involved, how information may be used and shared, and why a Privacy Impact Assessment was conducted. (Note: this section is an overview; the questions below elicit more detail.)

In order to effectively provide executive oversight of outside medical cost and maximize the utilization of available resources, each Federal Bureau of Prisons Institution (BOP Institution) has a contract with a Comprehensive Medical Contractor (CMC) to provide healthcare services which cannot be provided by BOP personnel. The pricing terms in these contracts use Medicare billing regulations as a baseline although they do not necessarily reflect Medicare reimbursement rates.

The BOP contracts with a Medical Claims Adjudication service (MCA Service) to ensure that invoiced amounts from the CMCs of the BOP Institutions are accurate, the invoiced amounts are appropriately audited, , and are paid by the BOP Institutions. Specifically, the MCA Service helps the BOP Institutions determine the correct reimbursement amount payable for all healthcare services rendered by the CMCs under their contract with the Institution. The information prepared by the MCA Service contractor is used by each Institution to reconcile invoices received from their CMC, helping to prevent possible payment errors. The medical claims adjudication process also helps to identify and prevent potential fraudulent medical billing practices.

The key information technology used by the MCA Service and the BOP Institution is a Commercial Off-the-Shelf (COTS) medical claims processing system. The designated system is the engine behind the MCA system, used by health insurance plans to adjudicate medical claims. This system is also used to audit claims from BOP CMC contractors to ensure compliance with the Medicare-based billing regulations in conformance to contract pricing terms negotiated by the BOP.

The personal information collected and used by the system includes:

- Names
- Inmate federal register numbers
- Dates of birth
- Medical, lab, radiology and psychological claim information, i.e., treatment codes, provider name service dates and locations.

Access to the claims adjudication system is limited to those persons who are authorized to review such information for their official duties. User access is restricted to those staff who need to view and upload data, and user roles are defined to so limit access. Their work is regularly reviewed to ensure that their access to and use of the data is appropriate.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the information technology, why the information is being collected, maintained, or disseminated, and how the information will help achieve the Component's purpose, for example, for criminal or civil law enforcement purposes, intelligence activities, and administrative matters, to conduct analyses to identify previously unknown areas of concern or patterns.

The pricing for each service under a CMC's contract is based upon the reimbursement rates established by the Medicare program plus a negotiated increase or discount. Calculating the appropriate reimbursement rate for a healthcare service provided by a CMC is complex and requires in-depth clinical/reimbursement expertise, as well as an understanding of the myriad payment methodologies used by Medicare.

To align with Information Technology strategy for systems deployment and sustainment, the designated system will be hosted by the MCA Service contractor in a private cloud for the BOP's use. The cloud hosting environment is a specially engineered and operated cloud hosting service designed to host U.S. Government sensitive systems/data and regulated workloads—adhering to a higher level of security and compliance requirements than used in their normal commercial cloud regions.

The key data inputs are 1) the medical claims submitted by the CMC for reimbursement after provision of a service; 2) the inmate's location (BOP Institution name) on the date of service (each Institution has negotiated different rates with their CMC—thus, if an inmate transfers among Institutions, the contracted rates will change); and 3) the contracted rates for each CMC (and the underlying Medicare rates used in the calculation of the amounts payable to each CMC).

The majority of the medical claims submitted by a CMC will be in electronic format using their choice of any commercial claims clearinghouse service that are commonly used by providers to submit claims electronically to healthcare payers and insurers. Some claims will be submitted by the CMC in hard copy format depending upon the specifics of their contract with a BOP Institution.

The inmate location data will be generated from the BOP's Inmate Case Management System. The initial inmate file contains all inmates, and the daily electronic feed is securely shared with the MCA Service contractor. The daily feed provides the delta in new inmates, released inmates and deaths, which reconciles the adds, changes, and deletes from day-to-day in the source file to ensure the integrity of the data. The claims system displays the location of the inmate on the date of the medical procedure. The inmate location determines the correct pricing structure to apply to the medical services received. BOP comprehensive medical contracts (CMCs) are awarded to different vendors with different pricing structures by location.

BOP medical and accounting staff at each institution will have access to the designated system as required in order to audit and reconcile invoices received from their CMC contractor. This

invoice reconciliation process will include the viewing of authorizations, claims, explanation of benefit documents, and standard reports designed to facilitate the invoice reconciliation process. In addition, BOP Health Services Division staff will have access to this system to provide global oversight and to support data analysis related to preventing potential fraud, waste and abuse.

The operation of the designated system and the processing of BOP medical claims using will only be performed by MCA Service contractor staff.

The MCA Service contractor will share data with BOP for the preparation of:

- Good Faith Estimates (GFE) – Estimates for cost of care will be provided to BOP institutions daily for budget accrual of the institutions expected claim costs. Reports will be provided to the institution via secure web access (white-listed IP addresses) for those individuals with financial responsibility.
- Explanations of Benefits (EOB) – Justifications for the evaluation of medical claims for BOP review that will ensure that BOP reimburses the CMC appropriate for care provided. Documents will be provided via the same mechanism as the GFE.

2.2 Indicate the legal authorities, policies, or agreements that authorize collection of the information. (Check all that apply and include citations/references.)

Authority		Citation/Reference
X	Statute	18 USC § 3621, 4042, 4082 and 5003 (state inmates), Section 11201 of Pub. L. 105-33; 111 Stat. 740 (DC felons);
	Executive Order	
X	Federal Regulation	42 C.F.R. § 424.32 - Basic Requirements for All Claims
	Agreement, memorandum of understanding, or other documented arrangement	
X	Other (summarize and provide copy of relevant portion)	"Appropriation Language The FY 2021 budget estimates include proposed changes in the appropriation language listed and explained below. New language proposed for FY 2021 is italicized. Federal Prison System Salaries and Expenses For necessary expenses of the Federal Prison System for the administration, operation, and maintenance of Federal penal and correctional institutions, and for the provision of technical assistance and advice on

		corrections related issues to foreign governments, . . . Provided, That the Attorney General may transfer to the Department of Health and Human Services such amounts as may be necessary for direct expenditures by that Department for medical relief for inmates of Federal penal and correctional institutions: Provided further, That the Director of the Federal Prison System, where necessary, may enter into contracts with a fiscal agent or fiscal intermediary claims processor to determine the amounts payable to persons who, on behalf of the Federal Prison System, furnish health services to individuals committed to the custody of the Federal Prison System: . . .." The FY2021 Performance Budget Congressional Submission further details the Medical Claims Adjudication as a Health Care Cost Containment initiative: Medical Claims Adjudication. The BOP contracts with a medical claims adjudication vendor to review claims for duplicate billing, claims for services not requested or not appropriate for the stated diagnoses, and local market rates for physician and facility charges. Contracting for medical claims adjudication enables the BOP to identify patterns of fraud, waste, and abuse. The BOP will award a new claims adjudication contract in 2019 with increased oversight capabilities and fraud detection reporting. The rollout of the new services will expand into more institutions and improve outside medical cost monitoring.

Section 3: Information in the Information Technology

3.1 Indicate below what types of information that may be personally identifiable in Column (1) will foreseeably be collected, handled, disseminated, stored and/or accessed by this information technology, regardless of the source of the information, whether the types of information are specifically requested to be collected, and whether particular fields are provided to organize or facilitate the information collection. Please check all that apply in Column (2), and indicate to whom the information relates in Column (3). Note: This list is provided for convenience; it is not exhaustive. Please add to "other" any other types of information.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Example: Personal email address	*X*	*B, C and D*	*Email addresses of members of the public (US and non-USPERs)*
Name	X	C and D	First Name Last Name of Federal Inmate and Health Care Provider.
Date of birth or age	X	C and D	Date of Birth of Federal Inmate
Place of birth			
Gender	X	C and D	Gender of Federal Inmate
Race, ethnicity or citizenship			
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)			
Tax Identification Number (TIN)	X	A, B, C and D	These are from medical provider organizations subcontracted to the CMC. TIN is a required field on all claims.
Driver's license			
Alien registration number			
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address			
Personal e-mail address			
Personal phone number			
Medical records number	X	C and D	From medical claims personnel.
Medical notes or other medical or health information	X	C and D	From medical claims and BOP medical staff.
Financial account information			
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information			
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Device identifiers, e.g., mobile devices			
Web uniform resource locator(s)			
Foreign activities			
Criminal records information, e.g., criminal history, arrests, criminal charges			
Juvenile criminal records information			
Civil law enforcement information, e.g., allegations of civil law violations			
Whistleblower, e.g., tip, complaint or referral			
Grand jury information			
Information concerning witnesses to criminal matters, e.g., witness statements, witness contact information			
Procurement/contracting records	X	A, B, C and D	Invoices from CMC contractors and their contracted payment rates.
Proprietary or business information			
Location information, including continuous or intermittent location tracking capabilities	X	C or D	Location information (Institution name) of Federal Inmate
Biometric data:			
- **Photographs or photographic identifiers**			
- **Video containing biometric data**			
- **Fingerprints**			
- **Palm prints**			
- **Iris image**			
- **Dental profile**			
- **Voice recording/signatures**			
- **Scars, marks, tattoos**			
- **Vascular scan, e.g., palm or finger vein biometric data**			
- **DNA profiles**			
- **Other (specify)**			
System admin/audit data:			
- **User ID**	X	A	BOP system admin/audit data, including User IDs and passwords.

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public - US Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
- **User passwords/codes**	X	A	BOP system admin/audit data, including User IDs and passwords.
- **IP address**	X	A	BOP system admin/audit data.
- **Date/time of access**	X	A	BOP system admin/audit data, including date and time of access.
- **Queries run**	X	A	BOP system admin/audit data.
- **Content of files accessed/reviewed**	X	A	BOP system admin/audit data.
- **Contents of files**	X	A	BOP system admin/audit data.
Other (please list the type of info and describe as completely as possible):	X	C and D	Inmate Register Number

3.2 Indicate below the Department's source(s) of the information. (Check all that apply.)

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

Government sources:					
Within the Component	X	Other DOJ Components		Online	
State, local, tribal		Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)			
Other (specify): Inmate data file provided by BOP.					

Non-government sources:					
Members of the public		Public media, Internet		Private sector	X

Commercial data brokers					
Other (specify): Medical claims will be submitted from private sector health provider organizations who are subcontracted with BOP Comprehensive Medical Contractors.					

Section 4: Information Sharing

4.1 Indicate with whom the component intends to share the information and how the information will be shared or accessed, such as on a case-by-case basis by manual secure electronic transmission, external user authorized accounts (i.e., direct log-in access), interconnected systems, or electronic bulk transfer.

Recipient	How information will be shared			
	Case-by-case	**Bulk transfer**	**Direct log-in access**	**Explain specifics of the sharing, as well as how these disclosures will support and are compatible with the purposes of the collection.**
Within the Component			X	The BOP MCA Service contractor staff and BOP staff at each Institution will have direct access to the system as well as have access to copies of PDF document work products from the contract.
DOJ Components				
Federal entities				
State, local, tribal gov't entities				
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes				
Private sector				
Foreign governments				
Foreign entities				
Other (specify):				

4.2 If the information will be released to the public for "Open Data" purposes, e.g., on data.gov (a clearinghouse for data from the Executive Branch of the Federal Government), and/or for research or statistical analysis purposes, explain whether—and, if so, how—the information will be de-identified, aggregated, or otherwise privacy protected.

N/A

Section 5: Notice, Consent, Access, and Amendment

5.1 What, if any, kind of notice will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Federal Register System of Records Notice (SORN), providing generalized notice to the public, a Privacy Act § 552a(e)(3) notice for individuals, or both? Will any other notices be provided? If no notice is provided, please explain.

Inmates receiving medical treatment from outside physician ordinarily are provided with a standardized HIPAA notice of the fact that for purposes of payment of the physician's claims for the treatment provided to the patient, the treating physician will disclose the patient's personal health information to organizations responsible for payment of such claims as well as to organizations responsible for assisting payers to adjudicate those claims.

Generalized notice to the public is also provided in the form of the following SORN: BOP-007, Inmate Physical and Mental Health Record System, first published 67 FR 11712 (3-15-2002) and most recently updated 82 FR 24147 (5-25-2017).

5.2 What, if any, opportunities will there be for individuals to voluntarily participate in the collection, use or dissemination of information in the system, for example, to consent to collection or specific uses of their information? If no opportunities, please explain why.

Individuals will not have the opportunity to opt out of the choice of physician by BOP, as well as the processing of their personal health information through this system. The HIPAA Privacy Rule permits a covered entity to use and disclose protected health information (PHI), with certain limits and protections, for treatment, payment, and health care operations activities. Under 45 CFR 160.103, BOP's Comprehensive Medical Contractors and their provider subcontractors, the MCA Service contractor, and the Health Care Clearinghouse used by provider subcontractors, are all defined as covered entities under HIPAA and thus may use/disclose PHI in the payment process without the individual's authorization.

5.3 What, if any, procedures exist to allow individuals to gain access to information in the system pertaining to them, request amendment or correction of said information, and receive notification of these procedures (e.g., Freedom of Information Act or Privacy Act procedures)? If no procedures exist, please explain why.

Inmates may request copies of their medical records from the treating physician. They may also gain access to information pertaining to them in the system by filing a Freedom of Information Act (FOIA) and/or Privacy Act request. Inmates can submit a request by completing the Request to Staff Member form (Form BP-A0148) and submitting it to their unit team staff, providing any documentation they may have as to why the data needs to be corrected or amended. Inmates receive notification of these procedures (how to amend or correct information) during their initial incarceration at Admission and Orientation, which every inmate is required to attend and every time they are transferred to another facility. The public is advised of the opportunity and method to access their information via the relevant

SORN (see Section 7.2 below) and on the BOP website at www.BOP.gov. Certain Privacy Act exemptions are claimed for this system pursuant to 5 U.S.C. 552a(j). See 28 C.F.R. § 16.97.

Section 6: Maintenance of Privacy and Security Controls

6.1 The Department uses administrative, technical, and physical controls to protect information. Indicate the controls below. (Check all that apply).

X	**The information is secured in accordance with Federal Information Security Modernization Act (FISMA) requirements, including development of written security and privacy risk assessments pursuant to National Institute of Standards and Technology (NIST) guidelines, the development and implementation of privacy controls and an assessment of the efficacy of applicable privacy controls. Provide date of most recent Authorization to Operate (ATO):** **If an ATO has not been completed, but is underway, provide status or expected completion date:** March 1, 2022 **Unless such information is sensitive and release of the information could pose risks to the component, summarize any outstanding plans of actions and milestones (POAMs) for any privacy controls resulting from the ATO process or risk assessment and provide a link to the applicable POAM documentation:** No applicable POAMs.
	This system is not subject to the ATO processes and/or it is unclear whether NIST privacy controls have been implemented and assessed. Please explain:
X	**Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify:** The cloud environment includes mechanisms to monitor system security which include Identity and Access Management, Management Console, System Manager, CloudWatch, CloudTrail, Security Hub and Inspector. Additionally, the environment is under continuous monitoring of systems to safeguard information. Penetration testing by a FedRAMP certified third party assessment organization is performed as part of the security controls assessment required by the process to obtain an Authority to Operate.
X	**Auditing procedures are in place to ensure compliance with security and privacy standards. Explain how often system logs are reviewed or auditing procedures conducted:** System access logs are reviewed regularly by the MCA Service contractor staff. The contractor staff will perform a random audit of BOP and contractor user IDs regularly and routinely.
X	**Contractors that have access to the system are subject to information security, privacy and other provisions in their contract binding them under the Privacy Act, other applicable laws, and as required by DOJ policy**.

	Each component is required to implement foundational privacy-related training for all component personnel, including employees, interns, and contractors, when personnel on-board and to implement refresher privacy training annually. Indicate whether there is additional training specific to this system, and if so, please describe: N/A

6.2 Explain key privacy and security administrative, technical, or physical controls that are designed to minimize privacy risks. For example, how are access controls being utilized to reduce the risk of unauthorized access and disclosure, what types of controls will protect PII in transmission, and how will regular auditing of role-based access be used to detect possible unauthorized access?

The MCA system is being implemented and operated in accordance with Security and Privacy Controls for Federal Information Systems and Organizations (NIST SP 800-53, Revision 5). These controls include the regular review of system access logs by the MCA Service contractor staff. Additionally, the contractor staff will perform a random audit of BOP and contractor user IDs regularly and routinely.

Claims and other data are securely transmitted between BOP, the CMCs, and the MCA Service contractor. Additionally, GFE and EOB reports will be provided to the relevant BOP institution by the MCA Service contractor via secure means for those individuals with financial responsibility.

6.3 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.)

Records will be maintained by the MCA Service contractor for 3 years after the final payment on the contract per Federal Acquisition Regulation (FAR) Subpart 4.7. The MCA system maintains 7 years of claims data. The BOP medical records are maintained for 30-years retention in the Bureau Electronic Medical Record (BEMR).

Section 7: Privacy Act

7.1 Indicate whether information related to U.S. citizens or aliens lawfully admitted for permanent residence will be retrieved by a personal identifier (i.e., indicate whether information maintained by this information technology will qualify as "records" maintained in a "system of records," as defined in the Privacy Act of 1974, as amended).

_____ No. __X___ Yes.

7.2 Please cite and provide a link (if possible) to existing SORNs that cover the records, and/or explain if a new SORN is being published:

BOP-007, Inmate Physical and Mental Health Record System, first published 67 FR 11712 (3-15-2002) and most recently updated 82 FR 24147 (5-25-2017)

https://www.govinfo.gov/content/pkg/FR-2002-03-15/pdf/02-6205.pdf

Section 8: Privacy Risks and Mitigation

When considering the proposed use of the information, its purpose, and the benefit to the Department of the collection and use of this information, what privacy risks are associated with the collection, use, access, dissemination, and maintenance of the information and how are those risks being mitigated?

Note: When answering this question, please specifically address privacy risks and mitigation measures in light of, among other things, the following:

- ***Specific information being collected and data minimization strategies, including decisions made to collect fewer data types and/or minimizing the length of time the information will be retained (in accordance with applicable record retention schedules),***
- ***Sources of the information,***
- ***Specific uses or sharing,***
- ***Privacy notices to individuals, and***
- ***Decisions concerning security and privacy administrative, technical and physical controls over the information.***

Privacy Risk: Unauthorized access or misuse by authorized users or compromise of data.

Mitigation: In order to mitigate this risk, MCA will be monitored for system security including Identity and Access Management, and audit trail activities. Additionally, continuous monitoring of systems is implemented to safeguard information. Furthermore, system access logs are reviewed regularly and routinely by the MCA Service contractor staff, who will also perform random audits of BOP and contractor user IDs regularly and routinely.

In order to prevent the compromise of information during transit, claims and other data are securely transmitted between BOP, the CMCs, and the MCA Service contractor. Additionally, GFE and EOB reports will be provided to the relevant BOP institution by the MCA Service contractor via secure means for those individuals with financial responsibility.

Medical claims adjudication will be done with the minimum necessary data requirements to ensure the appropriate recommendations are made with respect to the reimbursement of medical treatment. This is designed to mitigate the risk of over-collection of data and potential misuse and compromise of such data.

Privacy Risk: Inaccurate or incomplete data

Mitigation: MCA is designed to review claims from CMCs for any inaccuracies in the billing process. If claims are determined to be inaccurate by the MCA Service contractors, institution staff will communicate with the CMC and a resolution will be handled at the local level.

Information on inmates will be shared with the MCA Service directly from the BOP inmate management system to ensure accuracy. The inmate location data will be generated on a daily

basis to ensure timeliness of the information. The proper inmate location determines the correct pricing structure to apply to the medical services received. If the inmate location used on the claim was not accurate for the date of service, the pricing applied could be in error.

Additionally, inmates whose information is contained in the system may request amendments or corrections to their data by submitting a Privacy Act request to BOP through the procedures outlined in Section 5.3 above.