

Federal Bureau of Prisons



Privacy Impact Assessment for the Residential Reentry Referral Management (R3M)

Issued by:

Michael Rogers
RIM Chief / SCOP

Approved by: Andrew J. McFarland
Senior Counsel
Office of Privacy and Civil Liberties
U.S. Department of Justice

Date approved: June 4, 2026

(March 2025 DOJ PIA Template)

Section 1: Executive Summary

Provide a high-level overview of the project or information technology (e.g., application, tool, automated process) in non-technical terms that describes the project or 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.)

The Federal Bureau of Prisons (FBOP) protects society by confining offenders in community-based facilities that are safe, humane, and appropriately secure. Pursuant to 18 USC § 3621(b), residential Reentry Centers (RRCs) are contracted by the FBOP to supervise and support inmates in the successful transition from FBOP custody into society prior to their release from federal custody by providing work and other self-improvement opportunities. RRCs are utilized for inmates continuing FBOP custody, released from FBOP custody as a condition of their release, or as a resource for individuals transitioning between FBOP custody and release. R3M only maintains information about the RRCs and inmates in RRCs for the purpose of continuing FBOP custody. Community Treatment Service (CTS) providers are contracted by the FBOP to provide mental health services while the inmate is in the RRCs.

The Residential Reentry Referral Management System (R3M) is currently approved in the eICF PIA; however, based on significant changes and upgrades to the system, FBOP is completing this updated PIA to only address R3M. R3M has been upgraded to FBOP's AWS Cloud platform that resides on our Enterprise Cloud Platform (ECP). R3M information is shared between the FBOP's inmate case management system, the inmates' central files, and electronic medical records system, to include information entered by the RRCs and CTS providers. For more information about FBOP's inmate case management system, the inmates' central files, and electronic medical records system, please review their individual privacy compliance documents.

R3M collects and maintains inmate data to include first and last name, date of birth, demographic information, photos, social security numbers, scars, marks and tattoos, criminal history information, government assigned and electronic identifiers, RRC location, home address, occupation, cell phone numbers, emergency contact phone numbers, and any possible medical and mental health documentation.

The system collects and transmits information regarding inmate events and reports to the electronic inmate central file and the electronic medical records systems. Inmate events and reports include:

- RRC referral packets – The institution's Case Management employees create RRC referral packets regarding an inmate's release from federal prison to an RRC. The packet is then submitted to the Residential Reentry Management Office (RRM) for review, and the RRM Office then reviews, either accepts or rejects the packet, and if accepted, sends the pack to the RRC via R3M. The RRC providers review the R3M information to identify space and available resources back to the RRM who then approves/denies the placement.

- Inmate's movement and programming – RRCs enter all inmate movement in and out of their facility and upload final case reports on the inmate's programming while in the RRC into R3M.
- Medical pre-certifications – a RRC will upload a pre-certification for inmate medical care into R3M and FBOP health specialists approve or reject pre-certification based on the information provided in R3M.
- Mental health referrals – CTS employees create referrals for mental health care, using reports and documents uploaded by CTS employees relevant to an inmate's mental health care.
- Escape reporting– In the situation where an inmate has escaped from an RRC, the escaped inmate's RRC will notify the RRM Office via telephone, fax, or email. RRM's use R3M to create escape flyers, escape reports, and apprehension reports. The escape flyers are sent to the Federal Bureau of Investigation and U.S. Marshals Service via email or fax to assist in apprehending the escaped inmate.
- First Step Act reporting – RRCs enter First Step Act quarterly reporting (downloaded to a file, not maintained on R3M).
- Prison Rape Elimination Act documentation – In accordance with the Prison Rape Elimination Act (PREA), RRM's create log entries (including as an inmate event) and upload documents regarding PREA events that are stored in R3M.
- RRC and CTS provider contract information – R3M tracks RRC and CTS provider contract information, including procurement and business information, as well as contractors' NCIC background check clearance dates, PREA incidents, and Office of Internal Affairs (OIA) incidents.

Section 2: Purpose and Use of the Information Technology

2.1 Explain in more detail than above the purpose of the project or information technology, the type of technology used (e.g., databases, video conferencing, artificial intelligence, machine learning, privacy enhancing technologies), 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.

R3M automates the processing of inmates referred to an RRC from an institution. R3M allows RRC employees and CTS providers to automate the electronic transfer of inmate data to the respective FBOP systems, such as the electronic inmate central file and the electronic medical records systems. Previously, RRC and CTS employees had to manually email or physically mail the parent institution inmate data, and an institution employee would have to upload the inmate data into the appropriate file. With R3M, RRC and CTS employees can receive and access inmate information maintained in the inmate case management system and send inmate information to and from the electronic inmate central file and the electronic medical records systems. These data transfers within FBOP systems reduce privacy risks and increase productivity for RRC and CTS

employees.

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
Statute	18 U.S.C. §§ 3621, 4003, 4042 (federal inmates), 4082, 5003 (state inmates) and Section 11201 of Pub. L. 105-33; 111 Stat. 740 (DC Offenders); The Health Insurance Portability and Accountability Act (HIPPA), Public Law 104-191; and Prison Rape Elimination Act (PREA) of 2003 (P.L. 108-79).
Executive Order	
Federal regulation	45 CFR Part 160 and 164, 170-172; 28 CFR 513; and 28 CFR 550.56, 550.59 and 550.60.
Agreement, memorandum of understanding, or other documented arrangement	USMS- MOU 449-007 MOU between the USMS and the FBOP regarding the detention of federal prisoners; DOJ CIO Memo CIO-26_05- Department Approval for Federal Cross-Agency Microsoft 365 Federation; Naphcare- MOU/ISA between BOP R3M and Naphcare.
Other (summarize and provide copy of relevant portion)	

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.*

Department of Justice Privacy Impact Assessment
Federal Bureau of Prisons /Residential Reentry Referral Management (R3M)
Page 4

(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 Detainees; 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
<i>Example: Personal email address</i>	<i>X</i>	<i>B, C and D</i>	<i>Email addresses of members of the public (US and non-USPERs)</i>
Name	X	A, C, & D	First and last names of FBOP employees, authorized contractors, and inmates housed in RRC facilities.
Date of birth or age	X	C & D	Date of birth of RRC inmates.
Place of birth			
Sex	X	C & D	Sex of RRC inmates.
Race, ethnicity, or citizenship	X	C & D	Race of RRC inmates.
Religion			
Social Security Number (full, last 4 digits or otherwise truncated)	X	C & D	Social security numbers of RRC inmates.
Tax Identification Number (TIN)			
Driver's license			
Alien registration number	X	C & D	Alien registration numbers of RRC inmates.
Passport number			
Mother's maiden name			
Vehicle identifiers			
Personal mailing address	X	C & D	Home address of RRC inmates.
Personal e-mail address			
Personal phone number	X	C & D	Cell phone numbers of RRC inmates and their emergency contact numbers.
Medical records number			
Medical notes or other medical or health information	X	C & D	Medical and mental health data of RRC inmates.
Financial account information			
Applicant information			
Education records			
Military status or other information			
Employment status, history, or similar information	X	A	Contractor NCIC clearance dates, as well as Office of Internal Affairs and PREA incident reporting.
Employment performance ratings or other performance information, e.g., performance improvement plan			
Certificates			
Legal documents			

Department of Justice Privacy Impact Assessment
Federal Bureau of Prisons /Residential Reentry Referral Management (R3M)
Page 5

(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 Detainees; 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	X	C & D	Criminal records, projected release date, actual release date, and arrest data of RRC inmates.
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			
Proprietary or business information	X	A	RRC and CTS providers' business contact information to include addresses, phone numbers, and email addresses.
Location information, including continuous or intermittent location tracking capabilities			
<i>Biometric data:</i>			
- Photographs or photographic identifiers	X	C & D	RRC inmate identification/intake photos.
- Video containing biometric data			
- Fingerprints			
- Palm prints			
- Iris image			
- Dental profile			
- Voice recording/signatures			
- Scars, marks, tattoos	X	C & D	Description of RRC inmates scars, marks and tattoos.
- Vascular scan, e.g., palm or finger vein biometric data			

(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 Detainees; 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
- DNA profiles			
- Other (specify)			
<i>System admin/audit data:</i>			
- User ID	X	A	FBOP employee and contractor user IDs.
- User passwords/codes	X	A	FBOP contractor user PIN codes/numbers
- IP address		A	Currently,R3M stores log entries, including end-user IP addresses.
- Date/time of access	X	A	FBOP employee and contractor dates and time of access.
- Queries run		A	
- Contents of files			
Other (please list the type of info and describe as completely as possible):	X	C & D	FBI numbers, federal registration numbers, height and weight of RRC inmates.

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	X	Hard copy: mail/fax		Online
Phone	X	Email		
Other (specify):				

Government sources:				
Within the Component	X	Other DOJ Components		Other federal entities
State, local, tribal		Foreign (identify and provide the international agreement, memorandum of understanding, or other documented arrangement related to the transfer)		
Other (specify): Contracted CTS providers input medical and mental health data into R3M.				

Non-government sources:				
Members of the public		Public media, Internet		Private sector
Commercial data brokers				

Other (specify):

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	Access to the system is limited to only those FBOP employees and contractors who require access to perform their official duties and such access is further refined via the user of role/group access management to enforce “least privilege” policies.
DOJ Components	X			Sharing with DOJ law enforcement entities only as needed in accordance with established agreements via secure e-mail or physical mail.
Federal entities	X			Data sharing with Federal Courts only as needed and authorized in accordance with established agreements via secure e-mail or physical mail.
State, local, tribal gov't entities				
Public				
Counsel, parties, witnesses, and possibly courts or other judicial tribunals for litigation purposes	X			FBOP can share information maintained in R3M with counsels, parties, witnesses, or courts for litigation purposes in accordance with law and regulation or a court order.

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.
Private sector			X	Authorized and approved CTS providers have direct log-in access to input their mental health records into R3M in accordance with their procurement agreement with FBOP.
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 kind of notice, if any, will be provided to individuals informing them about the collection, use, sharing or other processing of their PII, e.g., a Privacy Act § 552a(e)(3) notice? Will a System of Records Notice (SORN) be published in the Federal Register providing generalized notice to the public? Will any other notices be provided? If no notice is provided to individuals or the general public, please explain.*

Inmates are provided a general notice regarding the collection of their information as part of the inmate’s admission into the RRC. FBOP also provides general notice through published System of Records Notices in the Federal Register:

Justice/BOP-005, BOP’s Inmate Central Records System, 48 FR 23711 (June 7, 1984), last modified 84 FR 19809 (May 16, 2019), available at:
<https://www.govinfo.gov/content/pkg/FR-2019-05-06/pdf/2019-09204.pdf>

Justice/BOP-007, BOP’s Inmate Physical and Mental Health Record System, 67 FR 11712 (Mar. 15, 2002), last modified 89 FR 49906 (June 12, 2024), available at:
<https://www.govinfo.gov/content/pkg/FR-2024-06-12/pdf/2024-12221.pdf>

Justice/DOJ-002, DOJ's Department of Justice Information Technology, Information System, and Network Activity and Access Records, 64 FR 73585 (Dec. 12, 1999), last modified 86 FR 37188 (July 14, 2021), available at:

https://www.justice.gov/d9/pages/attachments/2021/08/02/2021-14986_-_doj-002_sorn_update.pdf

For RRC inmates receiving medical and mental healthcare, pursuant to FBOP contracts, CTS provides inmates with a Release of Information that notifies them that their records will be shared with FBOP and allows the inmate to consent to the sharing of information with the U.S. Probation Office and/or FBOP

In some instances when an RRC inmate is receiving medical care, FBOP is not required to provide the inmate specific notice that the medical provider will share the inmate's patient information with FBOP, pursuant to 45 CFR § 164.512(k)(5), which provides that, "A covered entity may disclose to a correctional institution or law enforcement official having lawful custody of an inmate or other individual protected health information about such inmate or individual, if the correctional institution or such law enforcement official represents that such protected health information is necessary for:...(A) The provision of health care to such individuals...[.]"

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.*

Federal inmates do not have the right to decline to provide information while in federal custody, as well as the processing of their personal health information through this system, in accordance with 18 USC § 4042, and are not required to consent to the sharing of their information when in custody and receiving medical care, pursuant to 45 CFR § 164.512(k)(5).

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.*

All inmates are allowed to review their information. Inmates placed in an RRC can submit a BP-A0148 Request to a Staff member to the RRM's office or a FOIA request through bop.gov to obtain the information R3M holds on them. Inmate records are exempt from disclosure under the Privacy Act (see [28 CFR 16.97](#)), inmate requests for records under the Privacy Act will be processed in accordance with the FOIA. 28 C.F.R. §§ 513.50; see 28 [C.F.R. §§ 513.61-513.68](#).

Inmates are provided the opportunity to review their documents upon request. Inmates can submit a request, *Request to Staff Member* form (Form BP-A0148), to their unit team

staff with 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 every time they are transferred to another facility.

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 the system operates under an Authorization to Use (ATU) or other authorization mechanism, provide related details wherever an ATO is referenced): R3M will be authorized to operate, pursuant to the Residential Reentry Referral Management (R3M) ATO, which is currently being developed. If an ATO has not been completed, but is underway, provide status or expected completion date: 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:
	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	This information or information system has been assigned a security category as defined in Federal Information Processing Standards (FIPS) Publication 199, Standards for Security Categorization of Federal Information and Information Systems, based on the information it contains and consistent with NIST SP 800-60 v.2 rev.1, Guide for Mapping Types of Information and Information Systems to Security Categories: Appendices. Specify and provide a high-level summary of the justification, which may be detailed in the system security and privacy plan: R3M maintains criminal incarceration/rehabilitation and health information. If a loss of availability, integrity, or confidentiality regarding this information were to occur, the worst-case scenarios could include inmates or previously incarcerated individuals experiencing a breach of confidentiality; inmates receiving unnecessary or insufficient health care; breach of inmate or previously incarcerated individuals' confidence in their health record and FBOP may suffer an adverse effect on public and inmate confidence. Under NIST SP800-60 Volume 2, Rev 1, information maintained in R3M falls under Federal Correctional Activities, Health, and Law Enforcement, with a default Moderate categorization, where special factors could result in higher or lower impact level. No special factors exist in this instance. Based on the specific

	circumstances of R3M and lack of mitigating, aggravating, or special factors, R3M's information type categorizations are appropriately listed at the Moderate impact level.
X	Monitoring, testing, or evaluation has been undertaken to safeguard the information and prevent its misuse. Specify: Access to certain information that have higher sensitivity risks (health, PREA, etc.) requires specific authorization and is limited to select personnel with established need to know and have completed necessary, position-specific background checks that allow the handling of the sensitive information. Review and input of inmate medical data is restricted by user roles to those employees or contractors that directly provide care to the inmate or have a need to know as defined by their position description. FBOP will conduct regular testing of security controls to ensure proper implementation, monitoring, and safeguarding of information.
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: R3M tracks user account modifications and system events that will be reviewed by system administrators on a quarterly basis. Additional auditing of transactional data will be captured and maintained to align with records and information management requirements. A subset of approved internal users (e.g., employees, contractors) have been identified as system administrators to support organization-defined configuration, security, and access control.
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.
X	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: Pursuant to the FBOP contract, RRC and CTS contractors are required to undergo system-specific training, which informs the contractors of how to use the system, how FBOP uses the system, and what information will be held within the system.

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 R3M system uses several strategies to mitigate privacy risks, including the encryption of data while at-rest and in-transit. Access to the system is limited to those FBOP employees and contractors who have an appropriate security clearance and official need-to-know- (as stated in their position description) to access R3M information. These access limitations are regularly reviewed, and automated where possible. For example, the system is set to automatically lock accounts when security clearance renewal dates expire for RRC and CTS users. R3M uses role-based management to ensure that users

can only access and update data in relation to their functional duties at their specific RCC locations. User roles are defined to limit capability and prevent unauthorized access to R3M information. Additionally, FBOP employees can only access R3M, using their unique user ID and password.

- 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.) If the project involves artificial intelligence and/or machine learning, indicate if the information is used for training AI models, and if so, how this will impact data retention and disposition.*

Records in R3M are considered intermediary records. R3M documents are originally ingested from the inmate's electronic central file and case management systems, and the documents created in the system are transmitted back to the inmate's central file, the case management system, and their electronic medical records system.

GRS 5.2, item 020- Intermediary Records: Records that meet the following conditions:(1) They exist for the sole purpose of creating a subsequent record, and (2) They are not required to meet legal or fiscal obligations, or to initiate, sustain, evaluate, or provide evidence of decision-making. Temporary. Destroy upon creation or update of the final record, or when no longer needed for business use, whichever is later.

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:*

JUSTICE/BOP-005, BOP's Inmate Central Records System, 48 FR 23711 (June 7, 1984),last modified at 84 FR 19808 (May 6, 2019), and published at:
<https://www.govinfo.gov/content/pkg/FR-2019-05-06/pdf/2019-09204.pdf>;

Justice/BOP-007, BOP's Inmate Physical and Mental Health Record System, 67 FR 11712 (Mar. 15, 2002), last modified 89 FR 49906 (June 12, 2024), available at:
<https://www.govinfo.gov/content/pkg/FR-2024-06-12/pdf/2024-12221.pdf>;

JUSTICE/DOJ-002, DOJ Computer Systems Activity & Access Records, 86 FR 37188 (July 14, 2021), available at: <https://www.justice.gov/opcl/page/file/1419896/download>.

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? For projects involving the use of artificial intelligence and/or machine learning, identify the privacy risks uniquely associated with the use of AI/ML, and how those risks are being mitigated, for example the risk of output inaccuracies and mitigations in the form of testing, continuous monitoring, training, secondary review, etc.

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,*
- *Type of technology employed (e.g. AI/ML),*
- *Specific uses or sharing,*
- *Privacy notices to individuals, and*
- *Decisions concerning security and privacy administrative, technical, and physical controls over the information.*

Potential privacy risks associated with R3M include the risk of unauthorized access or dissemination to information, accuracy of information and improper use or disposal of information. FBOP mitigates risks related to unauthorized access or dissemination of R3M data, using technical and administrative safeguards that limit access to only those FBOP employees and contractors who have a need-to-know based on their position description and undergone training on how to handle DOJ and FBOP information, including how and when to properly disclose information to external entities.

R3M users receive annual training on how to properly handle sensitive information and manage the data maintained in the R3M modules. FBOP requires those accessing R3M and other FBOP information to undergo cybersecurity, privacy, and record training, as well as acknowledge and sign DOJ's General User's Rules of Behavior (ROB). Between the trainings and ROB, employees and contractors are notified that their use and access of FBOP data is limited to mission need and information disposal must adhere to federal records requirements and schedules. Additionally, those RRC and CTS providers, employees, and contractors with technical degrees, such as PhD or MD, also undertake their professional requirements, which may limit the use and dissemination of information based on local and federal requirements.

FBOP also limits access to the system to those people who have an appropriate security clearance which is regularly reviewed, need to know determined by job function, and completion of training on how to handle data within R3M and DOJ required annual privacy and cybersecurity training. The data is also segregated, limiting an employee's ability to update data they are not authorized to view or modify. Furthermore, R3M is set to automatically lock accounts when security clearance renewal dates are expired for RRC and CTS users. When an FBOP employee departs from the FBOP or transitions to a new position, the FBOP takes appropriate measures to deactivate the user's access to R3M. These mitigation efforts help ensure only those with the need-to-know and active credentials have access to R3M information

FBOP also takes measures to decrease risk of unauthorized disclosure of information when sharing information. FBOP encrypts data being transmitted from R3M, so the rest is encrypted at rest and in transit. Additionally, when information is shared with external entities, the risk of unauthorized access is mitigated by RRCs and CTS who are trained and required to safeguard R3M information, in accordance with the terms of their contracts with FBOP. FBOP employees mitigate the risk of unauthorized access when sharing information with external law enforcement agencies, federal courts and outside attorneys in accordance with established agreements and appropriate court orders.

Lastly, FBOP mitigates the risk of inadequate or inaccurate information by ensuring RRC and CTS providers, employees, and contractors have received the appropriate education credentials and training employees and contractors who have access to R3M on what information should be collected. RRC and CTS providers handle information related to professional services, such as health and mental health information. RRC and CTS providers, including their employees and contractors, undergo specialty training and education, such as medical school or therapy certifications, which teaches them what information is pertinent to provide. These same users are informed of how FBOP will use R3M and the information needed to ensure that inmates are provided with required healthcare services. The risk of FBOP collecting inaccurate information is further mitigated with interactions between RRC and CTS providers, employees, and contractors and the inmate receiving care. To conduct intakes or to ensure care is accurate RRC and CTS providers, employees, and contractors use their technical training to inquire about healthcare history, which includes correcting previous health information associated with the inmate patient.