SOCIETY OF NUCLEAR MEDICINE & MOLECULAR IMAGING

SNMMI RadioPharmaceutical Therapy Registries (RaPTR and RaPTR+PLUS)

Contents

Background

Radiopharmaceutical therapies (RPTs) are gaining prominence in the cancer armamentarium. This new wave was started with the approval of ^{177}Lu-dotatate for neuroendocrine tumor disease. RPTs are becoming more mainstream with the use of ^{177}Lu-PSMA-617 that improves survival in patients with common diseases such as metastatic prostate cancer. Of course, sodium iodide (^{131}I) therapy has been used for over 70 years in treating malignant and benign thyroid diseases, but we are still in a learning phase in relation to understanding the toxicity from radiopharmaceutical therapies. SNMMI has established the RaPTR and RaPTR+PLUS as quality improvement registries for the use of RPTs.

RaPTR stands for RadioPharmaceutical Therapy Registry. RaPTR is comprised of two components – a REDCap database and MIM Cloud. REDCap hosts data on patients including disease and treatment history along with outcome and adverse events relative to radiopharmaceutical therapies. MIM Cloud – used in the RaPTR+PLUS registry – hosts de-identified PET, SPECT, and planar scans. Currently, RaPTR modules include 177Lu-dotatate and 177Lu-PSMA-617 therapies.

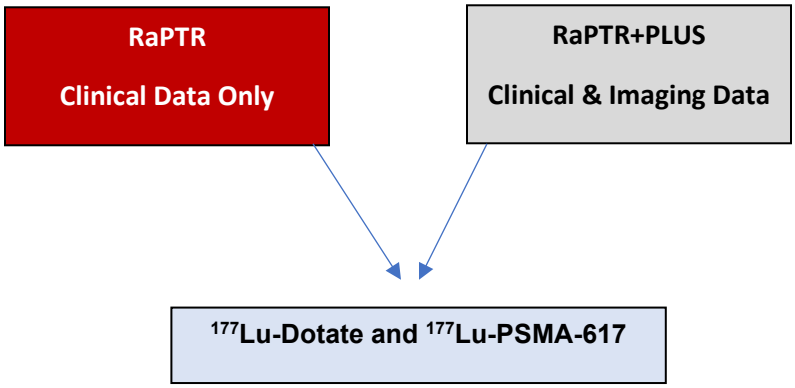
SNMMI Setting the Standards of Radiopharmaceutical Therapies

RaPTR and RaPTR+PLUS will provide the framework to support our field to ensure patient-centered imaging and therapy, patient-safety, improved outcomes, practice transformation and innovation, through ongoing data collection and quality improvement. Collection of this RPT data and associated images will help ensure high quality care for all patients. This will also enable identification of knowledge deficiencies and allow for the rapid development and deployment of tools and resources to address gaps in quality, patient care, and outcomes.

Registry Goals

- Establish a robust framework to collect data on patients receiving RPTs to enhance patient safety, optimize patient outcomes, and advance our field.
- Demonstrate the value of diagnostic nuclear medicine procedures and radiopharmaceutical therapies.
- Create a community of sites performing radiopharmaceutical therapies to develop and share best practices.
- Develop tools and resources, guidelines, national benchmarks, and standards to help sites improve patient outcomes.
- Utilize registry data to advocate for appropriate reimbursement for radiopharmaceutical therapies.
- Develop a robust database of patient and facility information to serve as a potential research source for future projects.
- Use imaging data to create a well annotated dataset that could be used for future AI development.
- Serve as a connection to the CMS's Quality Payment Program (QPP).

Registry Design



About the Pilot Phase (Phase 1)

The RaPTR Oversite Committee (RaPTR ROC) launched Phase 1 of RaPTR and RaPTR+PLUS. Up to 10 centers from various practice settings will participate. Sites can submit clinical data in the REDCap database and image data to MIM Cloud. (see Security details on pages 6-9) Image data can include pre-treatment PET scans and post-administration SPECT or planar images. RaPTR currently hosts data for ^{177}Lu-dotatate and ^{177}Lu-PSMA-617 therapies.

As a pilot site, it is important to discuss your participation options with your internal leadership and key stakeholders. SNMMI has created guidance and factsheets to assist in the decision-making process.

Responsibilities of being a Pilot Site:

- Identify a champion or primary investigator (PI).
- Submit the RaPTR or RaPTR+PLUS participation agreement.
- Obtain IRB approval.
- Submit a list of individuals who will participate in the data entry process.
- SNMMI will set up a REDCap profile for personnel entering clinical data.
- MIM will provide access to the MIM Cloud server (if participating in RaPTR+PLUS).
    a. Sites applying for RaPTR+PLUS may need to work with their Chief Information Officer (CIO) or Information Security Officer (ISO) to get approval to use MIM Cloud. Participants do NOT need to have a separate agreement with MIM or currently use MIM. MIM Cloud can be accessed on the web (URL) or added as an extension to your existing MIM Platform. Please note, if you are using MIM at your center, the system must be upgraded to 7.3.4.
- Attend the introduction to RaPTR call (about 1 hour).
    a. Be prepared to have a patient case available to use during the REDCap data entry walk through.
    b. Ensure you have access to your REDCap dashboard prior to the call. It is recommended that you review the survey forms to familiarize yourself with the survey logic and the questions being asked.
    c. Be prepared to provide feedback and ask questions.
- The RaPTR COE may invite the PI or champion to join registry calls. It is not required to participate but highly encouraged.
- Complete at least 1-3 patient cases a week.

If you have any questions, please contact Rustain Morgan, MD SNMMI Chair of the Radiopharmaceutical Therapy Registry Oversite Committee (rustainmorgan@gmail.com) and Julia K. Trigger, MS SNMMI Associate Director, Evidence and Quality (jtrigger@snmmi.org).

SOCIETY OF NUCLEAR MEDICINE & MOLECULAR IMAGING

FAQs

1. **Will we need to submit any PHI data for either registry?**
- No. We created the survey to ensure that PHI data will not be entered into the REDCap database. We also included an algorithm in MIM Cloud to anonymize all PHI data that is uploaded to the participants MIM Cloud.

2. **Will my data be shared with external parties or other registry participants?**
- Since the registry was created to be a research tool, in the future, individuals can submit a data request form to gain access to the database. In this situation, the data will not contain your center or provider information. We will not share your data with other external parties or other registry participants without your consent. Note: This service is not available at this time.

3. **Is there a fee to participate in either registry?**
- Currently, we are not collecting participation fees. However, this may change once the registry has been fully launched.

4. **What is the time commitment for this project?**
- Depending on how well you're able to access your information. Each patient entry could take anywhere from 30 minutes to an hour. Additional time may be spent on reviewing data quality, data completeness, and providing feedback.

5. **Can I use the registry for quality improvement metrics?**
- Yes. You can use your own data in the registry to report on measures and create benchmarks.

6. **Is this registry a CMS Qualified Registry (QR) or Qualified Clinical Data Registry (QCDR)?**
- No. RaPTR and RaPTR+PLUS is not recognized by CMS as a QR or QCDR.

SOCIETY OF NUCLEAR MEDICINE & MOLECULAR IMAGING

MIM Data Storage Security Overview

MIMcloud Overview:

- MIMcloud is an imaging and communication system designed to work safely and securely in a cloud-hosted environment regardless of where people are physically located or what network they happen to be on.
- Follows or exceeds HIPAA and GDPR guidelines for transferring, storing, and accessing PHI outside of a traditional hospital environment.
- MIMcloud utilizes a robust anonymization template, and is configured to only allow data that has gone through a template to be uploaded.
- Built on a combination of Google App Engine™ and Amazon Web Services™.
- Used both clinically and for research, MIMcloud provides safe and convenient access to medical images without sacrificing performance.
- MIMcloud uses a group/sub-group architecture that allows users to control who has access to what data, and what they can do with it.
- Users can see patient data at their access level and below, but cannot see anything in parallel level groups or in the parent level without express permission.
    - Ex: A parent institution that controls three imaging centers. A parent group on MIMcloud would be created, with three subgroups for each center.
    - People at imaging center “A” would see their data, but not at center “B” or “C.” Those with permission to the parent group can see all data. This level of granular control has proven very effective at being an efficient system while allowing the necessary controls.

Who Controls the Data on MIMcloud:

- MIM Software, Inc. has a zero-knowledge approach to our data.
- MIM provides the platform, support, and architecture to successfully deploy a secure, encrypted, remote access and storage system that supports HIPAA compliance.
- All data is encrypted **prior** to leaving any local workstation
    - MIM does not have access to any encrypted data.
    - Each study is individually encrypted.
    - Each study is stored encrypted.
- Data transfers encrypted.
- No VPN is required – due to multiple layers of encryption used prior to any data leaving locally
- Data transfers back into local memory when it’s accessed, and is decrypted at that point.
- All access is granted by administrators of RaPTR.

Access to Data:

- MIM cannot reset passwords.
- MIM employees cannot add themselves to groups unilaterally.
- All MIM can do is help delete unwanted data, users, or groups.
- MIM cannot access any customer groups or data.

Level of encryption:

- Each DICOM study has its own unique 128-bit AES encryption key, and the entire system is additionally encrypted using 256.
- When data is uploaded to MIM, MIM generates a random encryption key.
- That key is used to encrypt the data. Security is then further enhanced by encrypting the key.
- The key is only accessible via an encryption chain—starting with an authorized user with appropriate credentials subject to password strength requirements.

Password Security:

- User enters password to access MIMcloud.
- Password gets turned into a key, which unlocks the user's key.
- User key unlocks the group's key.
- The group key unlocks the study key.
- The study key unlocks the study for display or transfer.
- MIM does not have access to any users passwords.
- Customers have configurable strength policies per individual group.
    - Length, special characters, time to reset, etc.
- Passwords are **not** stored in our database as plain text.
- MIM's entire database has an additional layer of encryption on top to protect from outside threats.

Summary:

MIMcloud is a unique solution that allows multiple institutions to safely, securely, and conveniently collaborate for projects such as RAPTR. By enforcing de-identification standards prior to data being uploaded outside the originating institution, PHI exposure risks are minimized as greatly as possible. The design on the system allows per study access controls that marry security and privacy with actual utility of the images for purposes of the RAPTR Registry.

SOCIETY OF NUCLEAR MEDICINE & MOLECULAR IMAGING

REDCap Data Storage Security Overview

REDCap (Research, Electronic, Data Capture) is an NIH-funded, free, secure web application for building and managing online surveys and databases used by over 3,000 institutions and is cited in more than 6,000 journal articles. While REDCap can be used to collect virtually any type of data (including in 21 CFR Part 11, FISMA, and HIPAA-compliant environments), it is specifically geared to support online or offline data capture for research studies and operations. The REDCap Consortium, a vast support network of collaborators, is composed of thousands of active institutional partners in over one hundred countries who utilize and support REDCap in various ways.

REDCap is hosted on Amazon Web Services (AWS).

Identity and Access Management on AWS

- Initial Access (SSO/LDAP/MFA)
- Segregation of Duties / Escalate to admin access/ higher permission when needed
- Manage access and permissions
- Least privilege access
- Termination on access (inactivity – process to audit access)
- Projects access / segmentation on environment (admin on project vs admin on redcap)
- Create RACI

Information Security as a service on AWS

- Encryption requirements
- Key management
- Data Classification
- Data de-identification
- Import Data security scan
- Test Database – sources
- WAF on AWS
- AV on AWS
- Image on EC2
- S3 Access
- DB to use
- VPN Access
- Event Logging
- BC/DR – Backup location(s)

Compliance / Regulations available on AWS

- HIPAA
- FedRamp
- FISMA

Why AWS?

Amazon Web Services features a complete and ready-to-use REDCap environment which is automatically deployed in an isolated, three-tiered Virtual Private Cloud (VPC). The environment enables automatic scaling up and down based on traffic load and the data is encrypted by default at rest and in flight (in accordance with HIPAA). Managed services on the platform are used that provide automated patching and maintenance of OS, middleware, and database software, and the backups are performed automatically to enable operational and disaster recovery. The design results in a reasonable monthly cost (TBD) for production.

A high-level diagram showing how the different functions of REDCap map to AWS Services is shown here: