Technical Information and Security

One of the ACR’s highest priorities in developing RISE is to ensure that all information uploaded to the registry, including protected health information (PHI), is secure through every step of the process. With this in mind, we work with FIGmd—an industry leader in clinical data registry technology—to develop a registry infrastructure that combines the highest standards of privacy with ease of use for optimal results.

✓ The RISE registry dashboard:
  - Summarizes quality measure performances against the registry average and the CMS benchmark so practices can see how they perform on quality measures compared to their national peers
  - Provides easy to interpret benchmark reports used for validating the data for quality care provided
  - Helps to identify opportunities for improvement and standardization of care in alignment with the society/registry requirements
  - Implements strict information security controls

✓ All information entered in RISE, including PHI:
  - Is handled in a HIPAA-compliant manner
  - Is stored on a secured FedRAMP compliant cloud platform
  - Is fully encrypted both when stored and while the data moves between the storage and FIGmd’s registry dashboard, and vice versa

✓ Participating practices have control over the whole process:
  - RISE is designed for streamlined integration into your current data management system
  - Each practice installs its own connector that links to the RISE system
  - Each practice has the ability to stop or intervene in the data transmission process at any point in time

✓ PHI
  - Is logically segregated for each practice’s data. For each practice, data is hosted on the separate instances on the secured FedRAMP compliant cloud platform
  - Each practice is the sole owner of its patients’ PHI; it cannot be accessed or used by other practices or the ACR except as agreed to in the Business Associate Agreement
  - PHI can easily link back to a patient’s record by the patient’s practice for reporting purposes

✓ Data is stored on a secured FedRAMP compliant cloud platform:
  - With a proven, secure infrastructure; requires Virtual Private Network (VPN) for access
  - Virtually unlimited capacity allowing for immediate, rapid scaling on an as-needed basis
  - Minimizes costs and limits need for additional investments (servers, etc.)

System installation requires minimal effort and upkeep: updates and maintenance needs are initiated and completed by the system automatically on a regular basis.