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.

*All information entered into RISE, including PHI, is handled in a HIPAA-compliant manner and is fully encrypted both while in motion and at rest.*

- **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

- **PHI is separated upon entry into the system and stored in a separate, encrypted PHI Vault**
  - Housed in a separate virtual location from other patient data to provide extra security
  - Each practice is the sole owner of its patients’ PHI; it cannot be accessed or used by other practices or the ACR
  - PHI can easily link back to a patient’s record by the patient’s practice for reporting purposes

- **Data is stored using a secure cloud-based infrastructure**
  - 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