



ARTICLE

FEDERATED DATA CAPTURE: NAVIGATING GLOBAL RESIDENCY AND PRIVACY REQUIREMENTS

www.rgnmed.com | circles@rgnmed.com

The traditional healthcare data economy is built on an extraction model where third-party brokers monetize provider and patient data through "silent" de-identification clauses. This centralized approach creates significant legal and ethical friction, as it often necessitates moving sensitive information across borders or into proprietary silos, potentially violating increasingly stringent global data residency and privacy regulations. For healthcare executives, the risk of non-compliance with these residency requirements—where data must remain within a specific jurisdiction—represents a major barrier to participation in international research and evidence generation.

THE FAILURE OF CENTRALIZED EXTRACTION

Legacy health information technology frequently relies on siphoning data away from the point of care to a central repository for analysis. This creates several structural vulnerabilities:

- **Security Risks:** Large, centralized databases act as "honeypots" for cyberattacks, increasing the impact of any single data breach.
- **Trust Erosion:** De-identification without clear ownership or benefit to the source erodes the relationship between patients, physicians, and data users.
- **Legal Conflict:** Many jurisdictions now require that personal health information be stored and processed within the country of origin, making traditional "data scraping" and centralized brokerage models legally untenable.

THE CIRCLE DATASET INTERVENTION: FEDERATED HEALTHCARE DATA CAPTURE

A primary feature of **Circle Datasets** is the deployment of a **Federated Healthcare Data Capture model**. This architecture resolves the conflict between global research needs and local residency requirements by ensuring that sensitive clinical data remains at the primary point of care.

- **Decentralized Storage:** By keeping data localized, the platform satisfies global privacy and residency mandates, ensuring that "rights-laden" personal information is protected as a human right.
- **Secure Querying:** While the data remains decentralized, it can be queried and analyzed via secure, cloud-based infrastructure. This allows for the aggregation of insights and the creation of regulatory-ready datasets without the physical transfer of raw patient records.
- **Sovereign Identity Integration:** The use of Self-Sovereign Identity (SSI) and private keys ensures that patients manage their own identifiers, further minimizing the risk of unauthorized identification or data residency violations.

This federated approach allows health systems to transition from a "data brokerage" model to a "sovereign ownership" model. It fulfills the technical requirement for global evidence synthesis while respecting the legal and ethical boundaries of modern data privacy.

Download RegenMed white paper "[Bridging The 17 Years Evidence to Practice Gap](#)" to go deeper.

GET INVOLVED OR LEARN MORE – CONTACT US TODAY!

If you are interested in contributing to this important initiative or learning more about how you can be involved, please [contact us](#)*:

 [RegenMed | www.rgnmed.com](https://www.rgnmed.com)

 circles@rgnmed.com



SCAN ME

*If the links do not work for you, please download the PDF.