



**careevolution**  
HEALTHCARE TECHNOLOGY

---

# **Technology Practices and Trends in RHIO Deployment**

**An Introduction to contemporary technology  
approaches to RHIO deployment and a review of our  
blueprint for NHIN compliance**

## Background

Patients, caregivers, case managers, and public health officials are painfully aware that clinical records are fragmented in chart rooms in the basements of facilities like hospitals, clinics, pharmacies, laboratories, nursing homes, and consumer homes. Despite advances in site-specific electronic medical records, attempts to link records amongst the fragmented silos are just getting started. Regional Health Information Organizations (RHIO) have emerged as an organizational strategy for enabling healthcare providers to share clinical data electronically. At the federal level, a blueprint for a National Health Information Network (NHIN) is being developed to interconnect RHIOs. The eventual goal is the seamless exchange of patient information meeting the five rights - right information about the right patient at the right time at the right place to the right person.

## Status Quo Trends

In the 2 years since RHIOs and the NHIN have taken center stage in the national health agenda, there seem to be almost daily announcements of new RHIO formations. As affirmed by HIMSS, CalRHIO, Connecting for Health, and the ehealthinitiative, most RHIOs are at an early formative stage, contending with issues related to policy, organization, governance, and most importantly sustenance (funding). The results of the efforts from the 2004/2005 ONCHIT and AHRQ RHIO grant winners highlight several trends highlighted below.

- **No Off-the-shelf solutions** - There are no out-of-box proven vendor solutions for a RHIO platform, as evidenced by the broad consortia that have come together for the prototype projects. Of course, the traditional HIT vendor community is recasting existing EMR solutions as platforms for RHIO deployment. While convenient and certainly commercially attractive, the distinct needs of secure data exchange from those of an EMR have left most such attempts unsuccessful amongst the targeted customers. In our view, true technical work beyond remarketing and re-branding existing products is just getting started.
- **Build-Your-Own** - Most RHIO implementations have cobbled together results delivery functionality in the community using a combination of existing HL7 gateways and some manner of a web based viewer of the consolidated results.
- **Technology Architecture Soup** - Compliance with architectural recommendations from ONCHIT is hit or miss at best. As expected, the pilots and prototypes are trying a variety of approaches to the data exchange, typically driven primarily by local practical concerns and preferences. In our review of the reports filed by the early efforts, there are four specific areas where the existing efforts have the greatest room for improvement.

- **Federated Architecture** : while there is broad consensus that a federated, non centralized architecture is ideal, compliance with this recommendation is mostly lacking.

This is understandable since most current initiatives are, in some manner, extensions of pre-existing clinical messaging or results reporting efforts that were planned and begun prior to the development of the federated, non centralized, privacy maintaining contemporary recommendations. Secondly, service oriented, peer to peer approaches necessitated by the federated model are quite new and the technology heritage of most vendor partners predates them.

- **Identity Management and Record Location**. Everyone agrees that an effective Community MPI is a critical pre-requisite to an effective RHIO. However, just as organizations have struggled with effective implementation and integration of an MPI solution within their facilities, there have been significant challenges in implementing an MPI across the community. The typical solution is some sort of a record linking implementation that depends in large part on manual disambiguation clinical end-user at the time of need. Of course, this **honor system** exposes potential false links to end users and is less than an ideal solution to satisfy the increasing privacy and security concerns of citizen groups.

We also observe that in the case of patient demographic information, all current efforts have opted for the convenience and ease of centralizing the patient pool. Coincidentally, there has been an increase in the targeted theft and hacking of healthcare institutions by those with unscrupulous intent. Given the current identity theft landscape and the specific targeting of health data aggregators, it is our view that having a centralized repository of patient demographic information open to all those who operate the RHIO is an unacceptable security and privacy risk.

- **Terminology Standardization**. While some, notably IHIE (Regenstrief), have done an admirable job of standardizing lab results, medications, and other clinical data in a consistent display and retrieval format, most are just beginning to apply NLM based lexicons to the consolidated stores of clinical information. This goal is further challenged as one aspires to an increasingly non-centralized, federated model. There is no clear successful implementation of a non-replicated, federated data model that also achieves the terminology standardization objectives.

- **Security and Privacy Best Practices.** Few RHIO implementations currently support some basic, albeit technically challenging, privacy and security best practices promulgated by the think-tanks in the industry.
  - Patient opt-out
  - Patient contribution to personal record
  - Patient on-line review of audit records

## **Our Mandate & Guiding Principles**

Nearly three years ago, CareEvolution set out to define and develop a RHIO Technology Platform that would embody the recommended best practices espoused by the thought leaders in the space. We have been active participants in the collaborative discussions amongst the various stakeholder forums nationally over the previous 36 months. Our focus has been to develop a RHIO Technology Platform from the ground-up to incorporate the consensus derived technology best practices of :

- Federation
- Peer to peer data exchange
- World class identity management
- Comprehensive yet practical terminology services
- Immutable audit and logging services
- Service oriented architecture
- Contemporary security standards
- Granular data, patient, and provider based opt out capabilities

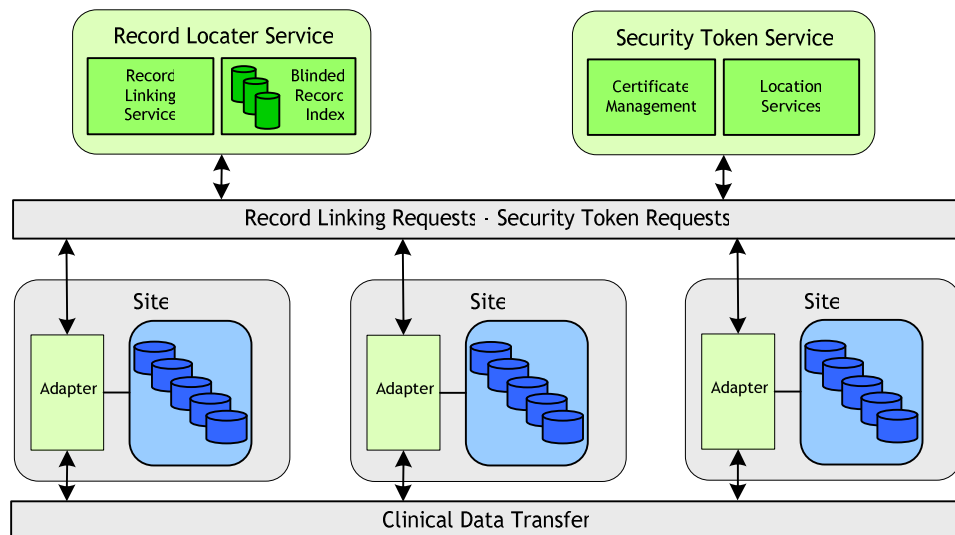
While the above represents a formidable list, we have also been focused on identifying specific platform capabilities that would facilitate adoption and success within the constraints experienced by real-world RHIO efforts. These real-world needs have served as guiding principles to the specific platform choices and capabilities we have invested in. Specifically the CareEvolution RHIO Technology Platform has been designed with the following overarching governing themes :

- **Keep RHIO Startup Costs Low** - given the funding challenges facing early RHIOs, it is critical that startup “costs” in terms of capital dollars, time, and opportunities are kept to a minimum
- **Leverage Customers’ Existing Applications Infrastructure** - whether it is existing HL7 message traffic, WAN/network standards, or security policies, it is critical to not have the RHIO **technology** force change. Policy, privacy, security, governance, compliance, and clinical value should drive the adopting organizations’ IT agenda, not the RHIO vendor requirements

- **Iterate & Increment** - given the nascent nature of the organizational constructs under which most RHIOs are operating, it is critical that the technology platform support a highly incremental approach to making progress towards a goal rather than a big-bang.
- **Allow A-la-Carte Adoption** - while we believe a holistic platform covering the gamut of technology components needed for effective RHIO deployment is necessary, we notice that different RHIO participants in a given RHIO have divergent needs. Not all participants need all or the same technology components to participate in the RHIO - the RHIO technology platform needs to be able to be adopted piecemeal on an as needed basis.
- **Assume Technology Leadership & Accountability** - RHIO organizations have their hands full with policy, governance, political, funding, and a myriad of other organizational issues. The ideal technology partner should offer holistic technology leadership and accountability. The RHIO should be able (after appropriate due diligence) to outsource the technology implementation details of the RHIO to its technology partner holding it accountable not for actions but rather results based on end-user observable milestones.

### The CareEvolution RHIO Technology Platform

The result of our work over the previous years is the CareEvolution RHIO Technology Platform -- a Federated, Service Oriented Architecture (FSOA) that achieves the guiding principles enumerated above.

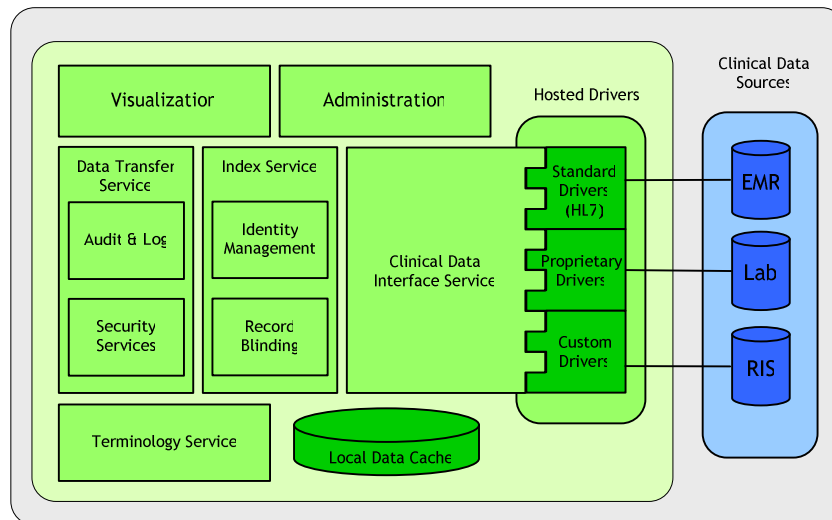


The key components of the architecture are briefly described below and greater detail regarding each is available at [www.careevolution.com](http://www.careevolution.com)

- **Adapter** -- Each participating institution runs the CareEvolution Adapter Service that provides the interface between the Record Locator Service, peer institutions, and the institution's local clinical data sources.
- **Record Locator Service (RLS)** -- The Record Locator Service (RLS) maintains an index of the locations of patient records for each person in the system. Clinical information is never sent to the RLS. Furthermore, the RLS only stores secured, **blinded** demographic information necessary for record linking. When a patient is registered with an institution, a query is submitted to the RLS. The RLS returns the location of any matching records. A location consists of a site identifier and a record identifier specific to the remote site.
- **Security Token Service (STS)** - The STS serves as an intermediary amongst participating members authenticating inter-member data exchange requests and insuring that no member is directly aware specifically of any other member. Adapters use the site identifier to query the STS to find the location and public key for the institution holding the desired record. Only then can peer institutions then use their local record identifier to locate the linked record.
- **Peer to Peer Data Exchange (PtPE)** - Finally, the located data interchange is managed purely between the adapters at the two institutions using encrypted web services.

### The CareEvolution Adapter

The CareEvolution adapter is composed of an Index Service, a Data Transfer Service, a Clinical Data Interface Service, a Terminology Service, and a Local Data Cache.



- **Record Index Service** - The Record Index Service provides the interface between the host systems and the Record Locator Service. It

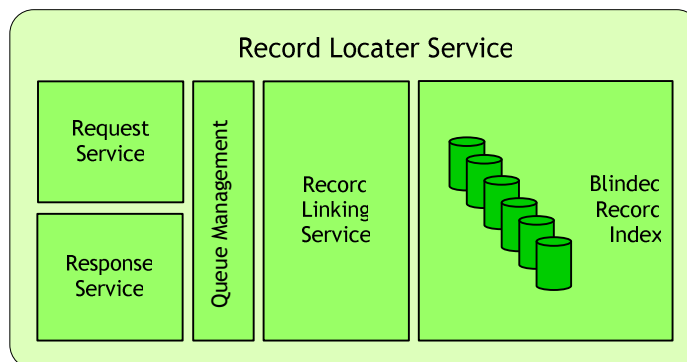
standardizes and blinds demographic information before sending requests to the Record Locator Service.

- **Data Transfer Service** - The Data Transfer Service manages adapter to adapter communication of clinical information. This is managed in pure peer to peer fashion.
- **Clinical Data Interface Service (CDIS)** - The CDIS hosts a set of pluggable drivers for communication with an institution's local clinical data sources such as EMR, lab, or pharmacy systems. The CDIS allows for easy customization to support the disparate clinical data sources of each institution. Each driver may run in one or more threads or processes dependent on the available hardware and required workload.
- **Terminology Service** - The Terminology Service is used by the Data Transfer Service and CDIS to provide translation between local and UMLS standard terms.
- **Local Data Cache** - The Local Data Cache provides a data store in which both record location index information and clinical information is cached. The Local Data Cache may be a single physical DBMS or can be federated across multiple physical databases.

### The CareEvolution Record Locator Service

The Record Locator Service (RLS) provides the functions necessary for patient linking and indexing. The Request Service, Response Service, and Queue Management Services manage the communications infrastructure between the RLS and client adapters.

- **Request Service** - The Request Service exposes the web service interface to receive asynchronous record add and update requests. The requests are queued for record linking.
- **Response and Queue Services** - The Response Service manages the communication of the results of record linking operations to the originating adapters for the linked records. Like all CareEvolution components the Request Service, the Response Service, and the Queue Management Service can be hosted with one instance of each on a single machine, multiple threads for each process on a single machine, or multiple processes on multiple machines. The required configuration is dependent on the traffic serviced by the RLS.



- **Blinded Record Linking Service** - The core work of the RLS, the actual record linking, is performed by the Blinded Record Linking Service. The Blinded Record Linking Service implements an incremental probabilistic matching algorithm to link each record added to the Blinded Record Index with the existing records in the index. Multiple instances of the Blinded Record Index Service can be used.

The Blinded Record Index data store is implemented as a federation of databases with each node of the index storing a subset of the records. This allows record linking to be done in parallel across disjoint subsets of the records in the index. As the size of the record index grows additional nodes can be added to the federation allowing the index to expand.

## Securing Identity Management - The Privacy Mandate

### RLS - The Traditional Weak Link in the RHIO Security Chain

As we have discussed earlier, we believe that the centralized store of accessible demographic information employed by most RHIO implementations creates an unacceptable security risk for any RHIO. Data aggregation accentuates three critical risk factors that increase the potential that sensitive information will be improperly disclosed:

- First, data aggregation increases the value of the centralized store creating a lucrative target for potential attackers.
- Second, it increases the number of entities that legitimately should have access to the central store; this in turn increases the number of avenues that can be compromised by attackers.
- Third, a centralized store of sensitive data can become a valuable resource that may be susceptible to political pressure for legalized access by interests claiming a need to know. A concerted effort by the government to obtain data from the large Internet search engines is a compelling example of this third risk factor.

### Blinded Record Linkage - The Solution

Methods must be deployed that can strongly secure this centralized data store. The CareEvolution RHIO Technology Platform provides a solution for this challenge. The CareEvolution RTP achieves a secure, performant solution to record linkage in the distributed system by using a **blinded directory** for centralized demographic data used in record location. A set of techniques are implemented to cryptographically (one-way) hash any demographic data that will be aggregated centrally. This ensures that patient demographic data stored in the centralized index is unrecoverable. There are two direct results of hashing the centralized index :

- **World Class Security** - From any plaintext string (i.e. “Smith”), a one-way hashing algorithm can quickly produce a long sequence of numbers (a “hash”), which represents the string “Smith”. However, to take this hash and reverse the algorithm to arrive at “Smith” would require years of computation, hence the term “one-way” hash.
- **Record Linking Challenge** - Since hashes of similar strings, such as “Smith” and “Smit” yield drastically different number sequences, the very process of hashing renders the traditional preferred probabilistic record linking techniques inoperable. As a result, all contemporary providers of MPI or Identity management solutions have avoided the formidable technical challenges posed by a crypto-hashed central directory. While this may have been acceptable when such solutions were intended to be implemented behind the security firewalls within an institution, **we believe that extending a non-hashed centralized repository of demographic information across a region, let alone the country, poses an unprecedented and unwarranted privacy risk.**

There is a solution, though it is not technically straightforward. Sophisticated string processing techniques are available that allow for both the security of one-way hashing and effective probabilistic matching. Approximate matching in this scheme is accomplished using a technique called bigramming. Bigramming breaks up the source string into many derived strings. Each derived string is given a similarity score that indicates how similar it is to the source. Two strings that have been bigrammed can then be compared by determining if they share a derived string. If so, the two derived similarity scores can be used to compute an overall “dice score.” Using a bigramming technique to generate derived strings, and then hashing derived strings allows for approximate, blinded identifier matching. This is the technique employed by the CareEvolution Crypto-Record Locator Service (Crypto-RLS)

### **Crypto-RLS - The CareEvolution Implementation**

In summary, using the CareEvolution Crypto-RLS provides an unprecedented privacy guarantee than any two-way encryption scheme because the underlying data cannot be decoded - even by the operators of the RHIO itself. Fortunately, once the underlying store of patient demographic information is no longer at risk, a centralized model for record location can actually **increase** security of the system. While the data itself cannot be compromised, record location requests from around the network can be monitored and audited for suspicious patterns of requests or other inappropriate activity.

## Summary

The health information exchange environment is evolving. It is critical to select an RHIO technology platform that can efficiently service your current and future needs. **CareEvolution** is a leading provider of secure interoperability solutions. Our RHIO Technology Platform is a robust Service Oriented Architecture (SOA) to enable RHIOs' heterogeneous underlying EMRs to "share" clinical information in a secure, reliable, and incremental manner. Distinct component such as Identity Management, Record Location, Clinical Data Integration, Audit & Log, Data Persistence, Visualization, Terminology, and Data Mining may be adopted piecemeal or as a comprehensive technology platform.

For More information please visit us at [www.careevolution.com](http://www.careevolution.com)