J P Systems, Inc.

Client Case Studies

Direct Secure Messaging Support for Federal Healthcare Client

The Veterans' Health Administration (VHA) sought a contractor to support the VHIE office Health Information Exchange program in developing software processes, content, and business and systems architecture. They needed to conduct and coordinate terminology standards activities, which included analyzing knowledge management for creating and managing healthcare terminologies. They needed a contractor who could develop and maintain terminology standards within the VHIE Health Business & System Architecture, including FHIR, Security Labeling Service (SLS), and Direct Secure Messaging protocol.

J P Systems used prior expertise in clinical Knowledge Based Systems, terminology standards, interoperability, and HIEs to fulfill VHA's needs. Through supporting internal VA groups and external partners, we transformed and defined VHIE Health's terminology standards and business objectives into goals and milestones for VA's Integrated Project Team (IPT). We did this by analyzing the SCRUM framework's business architecture and focusing on four areas: C-CDA expansion, Electronic Health Exchange (eHX) architecture enhancement, direct integration with end user applications, and tool integration.

We helped develop the VHIE Business and System Architecture, (formerly VLER), by analyzing its current state: architecture business capability, service capability, capability maturity, targets, and gaps associated with the VHIE program strategy and investment planning. We also made recommendations for the future, suggesting optimal workflows associated with HIE Business & Systems Architecture and defining As-Is & To-Be End-to-End Data Flow Architecture. As we have multiple option years, we continue to work with VHIE to optimize their Business & System Architecture through planning future state architectures and middleware evaluations for interoperability planning purposes. We guided the VA during the process of their acceptance into the Direct Trust's ATAB bundle for their HISP.

VHIE Case Studies: Direct Secure Messaging

What is Direct Secure Messaging?

Direct Secure Messaging is a Health Information Service Provider (HISP) and organizational model that allows individuals, providers, and organizations to share information with best practices that have trust and privacy considerations. Direct has Legal Business Associate Agreements with HIPAA and follows data collection, use, retention, and disclosure policies. The Direct Trust explains:

> "Direct Secure Messaging, commonly referred to as Direct, is a secure communication transport mechanism for sensitive information over the open internet. While appearing like email, Direct Secure Messaging utilizes digital certificates and a Public Key Infrastructure (PKI) to encrypt the contents of a message, meaning only the intended recipient can decrypt the message. Today, Direct Secure Messaging utilizes the foundation of the Direct Standard™, and is a widely deployed and accessible means for communicating sensitive health information to other trusted parties. Considered a "push" interoperability mechanism because of the sender "pushing" a message to the receiver, Direct Secure Messaging is a cornerstone of facilitating interoperability between disparate health technologies and organizations." [https://directtrust.org/what-we-do/direct-secure-messaging]

For more information, see our blog on new use cases for Direct.