State and Local

Solution Profile

MMIS Modernization—Improving lives through Healthcare Modernization

MMIS Modernization

Medicaid was signed into law by President Lyndon Johnson in 1965. The first Medicaid Management Information Management System (MMIS) was introduced in 1970. The Centers for Medicare and Medicaid (CMS) are a division of Health and Human Services (HHS) and run the program as a state-federal partnership. States are responsible for processing claims, managing payments and handling eligibility. Medicaid is the third largest federal program making up 14% of the federal budget. Even though CMS funds up to 70% of the states operational costs, administering healthcare can make up a significant portion of a state's budget.

States need to upgrade their MMIS systems for a number of reasons: complying with the Affordable Care Act and other legislative changes; adding increased capacity; or modernizing systems that are already decades old.

CMS has created several programs to help states with their modernization efforts. The Medicaid Information Technology Architecture (MITA), is a comprehensive framework with three components: a business architecture, an information architecture and a technology architecture. The framework details how to transform legacy systems into a modern Service Oriented Architecture (SOA) using an enterprise service bus (ESB) with modular re-usable services and a business rules engine (BRE). To assist states with implementation, CMS can provide significant funding split for upgrades. To receive this funding, states must comply with guidelines in the "Enhanced Funding Requirements: Seven Conditions and Standards," often just referred to as the "Seven Conditions." To help ensure successful modernization, CMS has created the MITA 3.0 State Self-Assessment (SS-A).

In a recent survey of IT managers: Modernization in the Public Sector, (IDG Research Group, July 2015), 54% of respondents said protecting data was their number one concern and that Identity and Access Management was the top challenge in modernizing applications. When asked if they had a statewide identity access management solution for both internal employees and citizens/ constituents, 14% said they had one today and 32% expected to have one in the next two years. When asked about other challenges, 42% responded by saying that interfacing with disparate systems was their greatest challenge, and 38% said they planned on using an API management systems over the next year.

While states will rely on system integrators to manage and run their development projects, there are four areas of technology based on this survey that will help states achieve their goals.

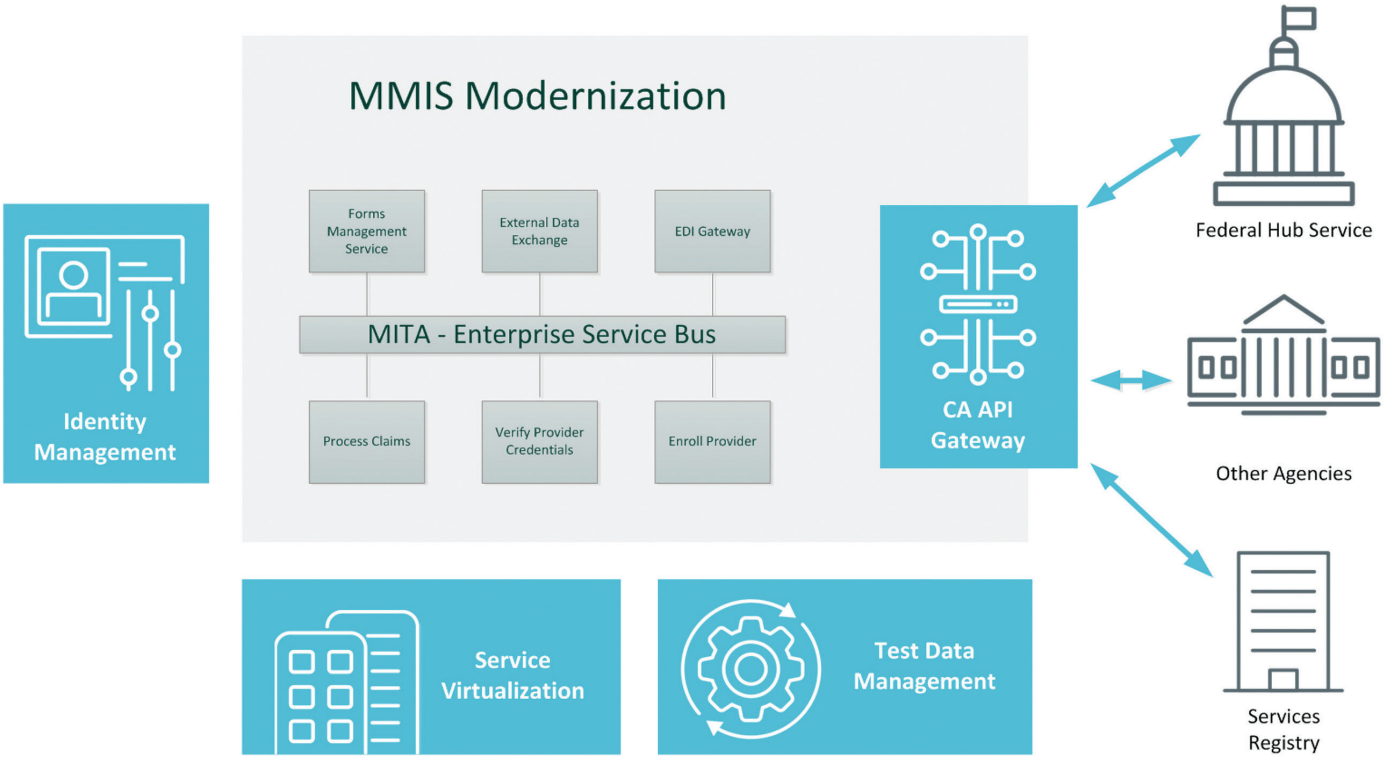
1) An Identity and Access Management system that can cost effectively scale to any statewide level. 2) API Gateways that work in tandem with SOA to facilitate secure communication with third party systems. 3) Service Virtualization that can reduce the unavailability of dependent systems during test, and significantly reduce the state's cost of maintaining test and development environments. 4) Test Data Management that can provision and secure test data so that states remain in compliance with HIPPA for the protection of Protected Health information (PHI) in test and development systems.

CA Solution

Identity Management

The CA Solution meets the needs of states as they expand to a statewide identity solution. The solution has been independently proven to scale up to one hundred million users (http://bit.ly/1N4ShYh). The CA identity solution is comprised of four components:

CA Identity Manager (CA IAM) streamlines the on-boarding and off-boarding of users, and automates the process of identity compliance. It features a user self-service portal which supports self-registration, forgotten passwords, and password resets. CA IAM has a packaged Pluggable Proofing Provider module that allow states to leverage public data for identity proofing. CA IAM is secure—it supports FIPS 140-2 support, Advanced Encryption Standard (AES) and proven crypto libraries (Crypto-J V3.5 and Crypto-C v2.0). It has built-in connectors, plus the Connector Xpress, a wizard-driven utility to generate custom connectors without coding.



CA Solution (cont.)

CA Technologies was a pioneer in removing the database as the underlying data storage in directory systems. Databases are unacceptably slow for this type of application. **CA Directory** dramatically improves speed, reliability, and scalability by leveraging the native operating system functions to commit data directly to disk, while maintaining all of the active data in a memory map. CA Directory's use of a memory mapped approach, combined with the ability to partition the data across multiple directory servers, is unique in the industry. CA Directory provides centralized monitoring across the enterprise, supports a REST based API for administration, and supports the SCIM Server 1.1 standard (System for Cross-domain Identity Management). SCIM is a standard for exchanging identity information between IT systems, which defines schema and protocols for identity management with data formatted in JSON or XML.

CA Single Sign-on provides a centralized platform for access management and authentication. CA SSO provides a secure and seamless user experience without the need for multiple logins to multiple applications. It helps MMIS developers focus on developing business logic so they can build new services faster. CA SSO supports SAML, OAuth, OpenID and WS-Security, REST and SOAP-based Web APIs. It is tightly integrated with CA IAM and CA Directory to provide a complete solution allowing users to securely connect to MMIS systems from any device any time anywhere.

CA Advanced Authentication complements CA SSO by reducing the risk of identity fraud, data theft or misuse, and payment fraud. When citizens access healthcare systems they need to know their identity is secure. CA Advanced Authentication provides additional security with minimal impact on user experience and lowers the cost of implementation, distribution and support. CA Advanced Authentication provides multi-factor authentication and uses one-time passwords that can be delivered via SMS/voice/email as primary or step-up authentication methods. CA Advanced Authentication uses patented cryptographic camouflage to prevent man-in -the-middle and man-in-the-browser attacks and has 'unbreakable' passwords.

CA Solution (cont.)

CA API Management

In MMIS systems, the MITA framework calls for interoperability services to connect the core service infrastructure to external data sources such as other agencies, Federal Hub services, or other data sharing organizations. The CA API Gateway provides backend SOA connectivity across databases, applications, mainframes and middleware to easily connect external data sources to the MMIS SOA architecture.

In the MMIS Architecture, the SOA gateway is deployed in the DMZ or outside the firewall to provide secure communication with external data sources. It provides XML firewalling, and protocol translation from legacy sources to REST and JSON. It makes exchanging authentication and authorization data easy with security assertions with support for advanced SAML, OAuth, and XACML. A SOA Gateway is flexibly deployed as a virtual appliance, is managed by a central console, and provides clustering for scaling and high availability.

CA Test Data Management

The Health Insurance Portability and Accountability Act (HIPAA) requires that data be protected in both production and non-production environments. Organizations that fail to adequately protect HIPAA data have been subject to fines in excess of $4.3 million dollars. CA Test Data Management (CA TDM) de-sensitizes production data prior to provisioning it to lower environments. A TDM uses innovative data masking tools and synthetic test data generation to help states maintain compliance with HIPAA regulations.

Synthetic test data contains all of the characteristics of production data but without any Protected Health Information (PHI). CA TDM uses powerful data profiling techniques, to take an accurate picture of your data and use this model to quickly generate smaller, richer, and referentially intact sets of test data to facilitate development and allow states to remain HIPAA compliant. CA TDM increases testing efficiencies by creating a test data warehouse where developers can find and reserve data through a self-service interface.

CA Service Virtualization

Existing MMIS systems are complex. The MITA framework describes a Service Oriented Architecture (SOA), a business rules engine (BRE) and an enterprise services bus (ESB). But even with this tested framework, there are still development challenges. There is the need to integrate with partner agencies, test access from multiple devices, and there is the frequent unavailability of backend host systems. This complexity often makes the costs of integration labs prohibitive, leading to incomplete QA and user acceptance testing (UAT).

Service Virtualization captures, models and then simulates the behavior of constrained or unavailable systems. Removing constraints in the software development lifecycle (SDLC) earlier allows developers to build out real services to accelerate testing. A low-cost virtual, “life-like” environment that is on-demand and always available, allows developers to deliver high-quality software sooner with less down time and less project risk.

For developers, the benefits of virtualizing services is the reduction in the testing time, and an increase in test coverage. Service Virtualization allows developers to increase their test runs and regain more development time in the lab. This means higher quality development and more effective regression and system testing. For states agencies, the benefits of service virtualization is a significant reduction in the cost of creating and maintaining development and test environments, and the ability to create realistic integration labs at lower costs. When states virtualize services running on the mainframe, they can realize significant saving in MIPs fees.

CA Technologies (NASDAQ: CA) creates software that fuels transformation for agencies and enables them to seize the opportunities of the application economy. Software is at the heart of every business, in every industry. From planning to development to management and security, CA is working with state agencies to change the way we live, transact and communicate – across mobile, private and public cloud, distributed and mainframe environments.

To learn how government agencies are partnering with CA Technologies on modernization, visit ***ca.com/publicsector***