

HIT Policy Committee Enrollment Workgroup
Testimony of Mr. Arvinder Singh, CNSI Health and Human Services
Wednesday, November 10, 2010
Marriott Wardman Park

In what state(s) do you currently operate enrollment systems for Medicaid and/or CHIP programs?

- **For what other programs do these systems also enroll individuals and families?**
- **Please briefly describe the high-level current architecture of the system(s).**
- **When was the system(s) procured and when did it become operational?**
- **What was the initial total cost of the system implementation, over how many years; what are the total annual maintenance costs?**

Good afternoon. My name is Arvinder Singh and I lead CNSI's Health and Human Services operating division. CNSI is a 16-year old IT firm that focuses on providing business solutions in the area of Medicaid, program integrity, and fraud and abuse prevention. I thank you for the opportunity to speak with you today regarding enrollment systems for Medicaid and CHIP programs.

As a health IT company with domain expertise in healthcare and Medicaid systems development and implementation, CNSI has many years of experience with provider, managed care, and mental health enrollment processing. CNSI is on a mission to deliver platform-based, open, and interoperable systems to enable state agencies in designing and operating programs that truly serve their constituency. Our success has been fueled and driven by challenging the status quo and driving innovation. We provide and support health IT systems at the state level to include:

- Medicaid claims adjudication and payment at the state enterprise level
- Managed care enrollment processing
- Program integrity data warehouses
- Surveillance utilization review reporting and management systems
- Eligibility and enrollment interfaces and processing

The states we have supported include Maine, Maryland, Michigan, and Washington. While we do not operate enrollment systems today, our focus has been in providing Medicaid systems that interoperate with enrollment systems. We bring a fresh and unique perspective to the challenges of dealing with enrollment systems from an IT and technology perspective. We understand the architectures of these systems and the challenges in addressing change. The architectures we have supported vary to address differences in state IT standards and

requirements; however, there are certain principles we have maintained in our implementations:

- Focus on non-proprietary technologies in the core of the architecture
- Integrate COTS wherever possible
- Standardize interfaces and integration with enterprise service bus (ESB) technologies
- Implement a community collaboration model to develop additional capabilities

Some of the challenges we have seen in addressing enrollment and eligibility include:

- File-based interfaces
- Complexity of the data structures
- Granularity of the data
- Data matching and standardization services

Do you provide for online enrollment?

- **If so, does the application contain error checks and/or business logic, or require applicants to complete all required questions before applications can be submitted?**
- **How is paper documentation handled?**
- **What percent of applicants apply online? What is the application completion percentage for these applications?**

CNSI does provide for online enrollment of providers, managed care programs, and mental health and substance abuse programs. In fact, we have developed centralized enrollment systems that are ready to be implemented in cloud-computing and software-as-a-service environments.

Our applications do contain error checks and/or business logic to ease the enrollment processes. These error checks and business logic processing are separated from the application code through data-driven configuration rules and also by the use of rules engine technologies. Rules engine based enrollment processing simplifies coding of complex rules and provides flexibility for changing these rules without subsequent modifications in code. It provides functional users and legacy system developers the flexibility to code the rules in simple logical statements. In addition to rules engine processing, CNSI's approach uses configurable decision matrices. . For example, in cases such as a newborn, which requires two enrollments – one for the first 21 or 60 days of birth based on the mother's enrollment, and another for a prospective period – the rules engine processing automatically creates more than one transaction to be processed in the system. Similar are also recommended for state-level enrollment and eligibility processes to lessen the burden of modifying and implementing new enrollment and eligibility policies.

The solutions provide a complete web-based solution for accessing information, from online data entry screens to validation processing to dashboard reporting. Our approach provides a framework for state agencies, providers, and other entities to share data and manage information holistically. We enable fiscal intermediaries, state agencies, and providers to share the same data set under differing rules and access privileges. For example, providers use self-service portal capability to enroll and maintain their data, while fiscal intermediary staff and state agencies have access to the system to approve applications and demographic updates. We focus on providing a paperless environment with rich innovative and integrated features, such as a document management and correspondence solution. Online screens guide the users through the enrollment process and support the data entry user with intuitive messages and context sensitive help. New applicants are able to submit online applications via business process wizards that simplify complex rules – much like TurboTax uses for submitting tax forms. Business process wizards provide a self-contained workflow view of the list of steps to navigate, view, and modify information.

Our managed care enrollment provides multiple enrollment services in both automatic and manual settings, such as:

- Assignment
- Re-enrollment
- Connect to family
- Newborn retro-enrollment
- Transfer
- Update demographics
- Update rate cohorts
- Disenrollment
- Exempt recipient from managed care

Managed Care Program level configuration, used in the enrollment process, allows features such as:

- Lock-in and lock-out
- Waiting list
- Enrollment process behavior controls:
 - Mandatory or non-mandatory enrollment
 - Auto assignment allowed

Paper documentation is handled through our systems with the use scanning, OCR, and key for entry technologies. Data captured through the OCR and keyed data entry are stored in a standardized format to be processed by online systems, at which point they are processed as if

they were entered online. Our solutions build a single repository for all correspondence, images, attachments, and documents, ensuring a single “data of record” for all operational documents that meets audit and legal requirements for security and privacy.

Business Rules (Item #3)

- **Do you currently express business rules outside of transaction systems?**
 - **What standard do you use for consistently expressing rules?**
 - **If so, what benefits have you seen from doing so? What challenges did you encounter?**
 - **If not, what (if any) challenges has this presented? What strategies do your systems currently employ to ensure the capacity and flexibility to change and/or modify rules as needed?**

The eCAMS platform implementation for the Medicaid Management Information System (MMIS) was the first implementation of a rules engine in high volume, high throughput transaction systems. CNSI’s rules engine, RuleIT, provided not only abstraction from the transaction processing, but also provided the much needed flexibility to accommodate future policy changes. In absence of industry standards, CNSI’s RuleIT builds a business dictionary of data elements to provide consistency of element usage across the company’s different implementations. RuleIT provides critical features, such as version control and time sensitive rules, that are fundamental in supporting the typical legislative and policy mandates seen in this space. RuleIT supports industry standards, such as Java Specification Request (JSR) 94 that defines the run time API for rules engines.

One of the critical dependencies in implementing a rules engine is the design and implementation of an object layer that represents business entities in terms of attributes and elements that are used to determine decisions and update underlying data structures. The design of the object layer becomes fundamental to the overall performance of the rules-based implementation. In high volume, high throughput environments, the implementation of rules using the typical Rete algorithm may not be effective, and may require a run time sequential wiring of rules like a decision tree.

CNSI’s implementation of using a rules engine-based approach has provided flexibility in implementing changes, provided visibility and transparency to the different stakeholders of the system’s enforced policy, and reduced the time to deploy changes in the production environment.

- **How could eligibility determinations made from these business rules be presented to consumers in a more clear, concise and unambiguous manner**

The communication to the consumer of the eligibility determinations based on these business rules requires a context-based representation and a different user experience. The business rules abstraction provides a clear knowledge base of system-enforced rules and simplifies the basis of communication with the consumer. For example in the claims world, the Explanation of Benefits (EOB) is a tool to provide consumer level communication of the claims adjudication. CNSI's implementation uses a configurable framework to define a communication framework for reporting the claim payment business rules. Even though the user experience can be significantly improved, it is a framework that allows flexibility and decoupling of business rules representation and its translation for common user consumption. It is recommended that additional context and rich user experiences be deployed to create a more compelling communication experience.

- **What challenges/opportunities are presented by the idea of a business rules repository as expressed in Recommendation 3.2?**
 - **Is additional standardization of business rules necessary to make this a valuable resource?**
 - **What strategies would you suggest for contributing to and/or maintaining such a resource?**

A successful business rules repository will require documenting the semantics of business vocabularies, business facts, and business rules, as well as a potential XML schema, for the interchange of these vocabularies and business rules among different entities. So the opportunity and the challenge lie in establishing the vocabulary and a dictionary for representing these business rules. The vocabulary definitions and dictionary are a significant undertaking. For example, even with the presence of HIPAA transactions for more than a decade, there seems to be little consensus on the semantics of some of the elements and their usage.

CNSI's implementation of its business rule repository is classified in a hierarchy of knowledge base, rule groups, and rules. The rule groups are created using a logical grouping of related business rules that govern a specific outcome. The knowledge base can be used to establish the general context of the business rules.

The maintenance of such a repository requires regulatory support and backing, and a community-led organization is the right model for such an evolving space. A well documented governance process, such as that used by Oracle (previously Sun Microsystems) for identifying JSR specifications, could potentially be leveraged in ongoing maintenance and support of such a repository. It should be clarified that the community model does not imply a voluntary participation approach. The maintenance of such a repository will require a core set of full-time resources aided by voluntary participation. The community on a periodic basis can elect these full-time resources.

Privacy and Security (Item #5)

- **How, if at all, does the consumer interact with your system?**

CNSI has applied different implementation models to support consumer interaction. Depending on state requirements, consumers either directly interface with our solution or have access through public facing portals. In the MMIS space, the consumers are both providers and beneficiaries. We have architected the eCAMS solution to be compliant with the HIPAA security guidelines around administrative and technical safeguards. The authorization and authentication framework is built around all access points of the system. Consumer access to the system is secured through SSL for encrypting the transmission and login pages for authentication pages. Access to different features of the system is restricted based on Role Based Access Control (RBAC) policies. Our solutions support public key infrastructure (PKI) based cryptography, which provides privacy, authentication, integrity and non-repudiation functionality to the system. Digital signatures are validated to authenticate the information source and provide integrity and non-repudiation functionality. We are upgrading our solution for integration with identity and access management solutions for full logical access and auditing. We recommend that to be fundamental to all future health IT systems.

Our eCAMS solution also provides provider and beneficiary portals that are designed to provide self-service functionality. The beneficiary portal (used by consumers) provides extensive access to manage their managed care enrollment, search for network providers, and identify plans. The provider portal helps the provider to manage their Medicaid claims, PAs, and beneficiary eligibility enquiries. These portals can be accessed from WAP mobile devices and can be extended to support interaction through SMS.

Our consumer end user experience includes the following:

1. Real-time Web User Interactions:

A complete suite of web-based interactions for all the business processes, such as online verification of eligibility (270/271), claim status check, and enrollment verification (834) transactions.

2. Batch Interactions

Batch interactions involve process batch operations for interfaces with agencies, receipt and processing of all mandated HIPAA batch transactions, and generation of required HIPAA outbound transactions. The solution supports different technologies for interfacing with external agencies, such as web services and MQ series.

3. Real time Smartphone Interactions

Smartphone access on Apple's iPhone provides access to basic functions. Current customer interactions on smartphone include Benefit Inquiry, Claims Inquiry, and Payment Information. Other smartphone platforms on which eCAMS is extensible include Android and Blackberry.

- **How difficult would it be to modify your system to offer consumer access to and control over eligibility and enrollment information?**

eCAMS is architected to open up consumer access to eligibility and enrollment information. It already supports concept of "self access" or "other access" where others are either family members or designated case workers. All information is presented within the data content and security regulation and guidelines of HIPAA.

- **What functions/standards do your systems currently contain, if any, to track and monitor third party access?**
- **Do your systems currently have the ability to grant separate authentication and/or login for third parties; track third party access and activity in immutable audit logs; and/or provide tools for the applicant to designate and/or revoke or time-limit third party access?**

eCAMS offers a detailed and configurable security framework to meet the varying needs of Medicaid Operations. eCAMS' design accommodates security needs for Medicaid fiscal agencies, Medicaid state staff, Medicaid external agencies, or third parties. The framework defines the profiles permissible under each organization. The profiles are defined using roles that grant access to every component within eCAMS. The security for each component is defined as Ready Only, Read-Write, or No Access. This framework has been operational in three Medicaid states' operations and offers access in a time defined manner for every consumer to eCAMS. The RBAC based levels of authorization prevents any read and write access to audit logs. This provides a tamper-proof audit logging system.

- **What safeguard systems do your systems currently include?**

CNSI builds series of security safeguards at the different layers of the system to protect and guard the data integrity and confidentiality. The security dimensions include administrative procedures, physical safeguards, technical security like data encryption, role based access, network layer security

- **Do you currently encrypt data in motion? If not, why not? What are the challenges in doing so?**

Yes, data in motion is encrypted by encrypting the channel of communication.

- **Do your systems currently have the capacity to generate and publish audit logs? If not, why not? What are the challenges in incorporating this function?**

eCAMS has extensive audit logging capabilities that have been explained in the previous question. The logging features are a performance overhead and CNSI implementation approach to log the user actions balances the performance and auditing needs.

- **Do you have access control functions? If not, what are the challenges to incorporating this?**

eCAMS utilized RBAC (Role based access control) policies to implement authorization access to authorized users who log into the system. The access control functions need more than the typical simple role definitions of function/page and element level security. The area of client data requires security policy rules that are enforced at the time of access. These security policies can be complex business rules and contextual in nature.

- **Do your systems incorporate automatic log off functionality? If not, what are the challenges to incorporating this?**

eCAMS implements an automatic log-off functionality using the concept of session time out. This property is configurable for the system. However it is not a foolproof model in a web browser based application since the interaction is done in a request /response model. So if the user quite the browser instead of closing the application, the system will keep the session open till the session timeout is completed at the server side. This automatic logging off creates a window of security risk .

- **Do your systems currently include any standards for ID assurance? If so, at what level? What are the challenges associated with this?**

eCAMS also supports public key infrastructure (PKI) based cryptography which provides privacy, authentication, integrity and non-repudiation functionalities to the system. Digital signatures can be validated to authenticate the information source and provide integrity and non-repudiation functionality.