

# NY Medicaid's HIE/MITA Enterprise Architecture: Using ARRA Funding to Improve Care for Medicaid Beneficiaries

CMS Second Annual Multi-State Health IT  
Collaborative for E-Health Conference  
February 8-9, 2010, Washington, DC

*Presented by  
James J. Figge, M.D., M.B.A.  
Office of Health Insurance Programs*



# **Vision: Patient-Centered State Medicaid HIT/HIE Plan for NY**

---

- NY Medicaid will leverage the Recovery Act “meaningful use” incentive funds and the 90/10 Medicaid administrative funds, together with NY State Health Budget initiatives, to create and implement a five-year patient-centered state Medicaid HIT/HIE plan for NY.



# Patient-Centered State Medicaid HIT/HIE Plan for NY

---

- Support HIT adoption and clinical practice workflow re-engineering.
- Incentivize “meaningful use” of EHR technology.
- Improve quality of care delivery by supporting the patient-centered medical home model.

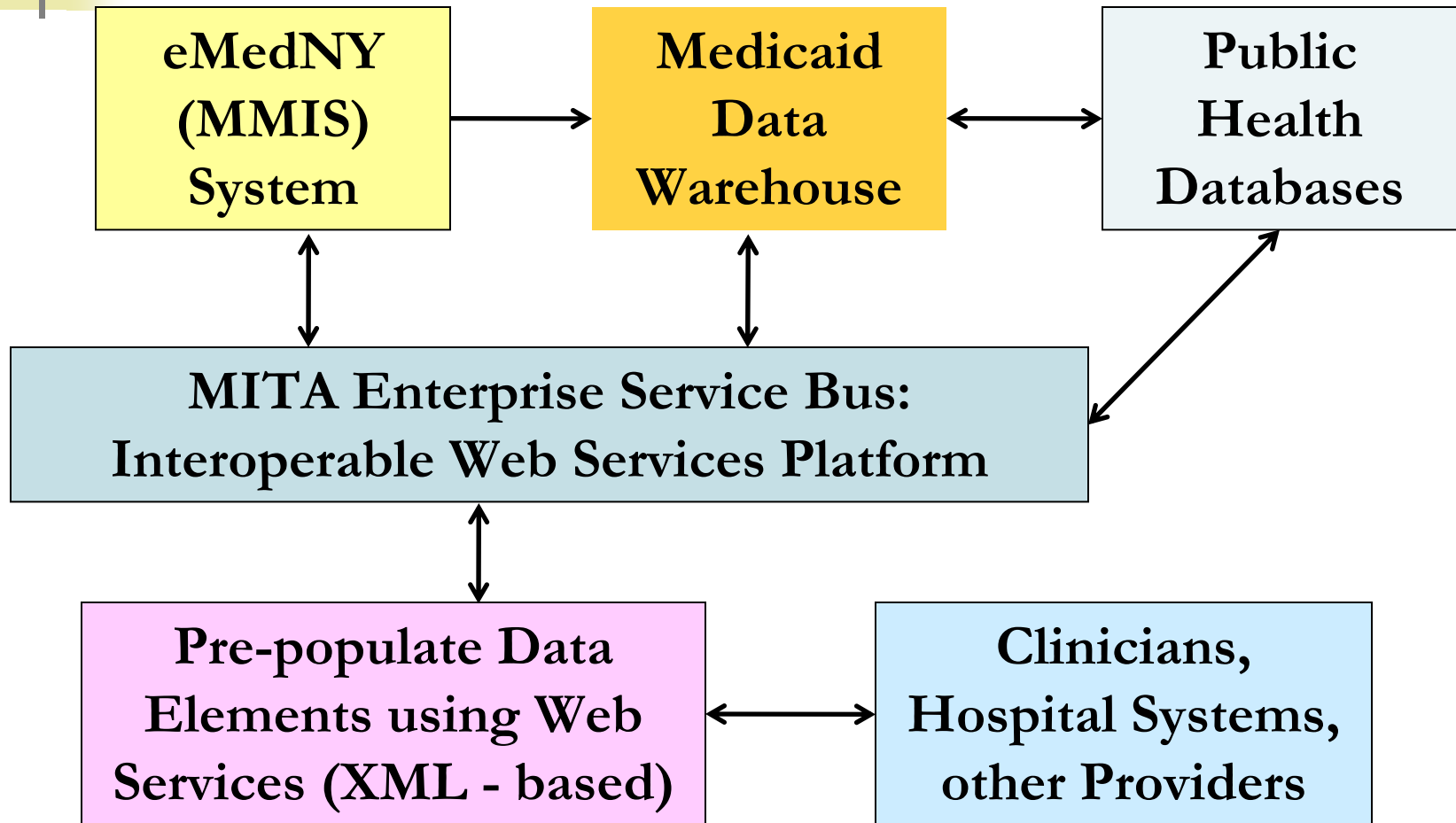


# Patient-Centered State Medicaid HIT/HIE Plan for NY (cont'd)

---

- Improve patient safety by incentivizing e-prescribing.
- Promote improvements in quality of care as documented by clinically-based electronically-reported quality metrics.
- Improve care coordination via use of clinical data distributed through interoperable HIE utilizing NY Medicaid's HIE/MITA enterprise architecture.

# NY Medicaid HIE/MITA Enterprise Architecture: Develop a Continuity of Care Document (CCD) for each Patient

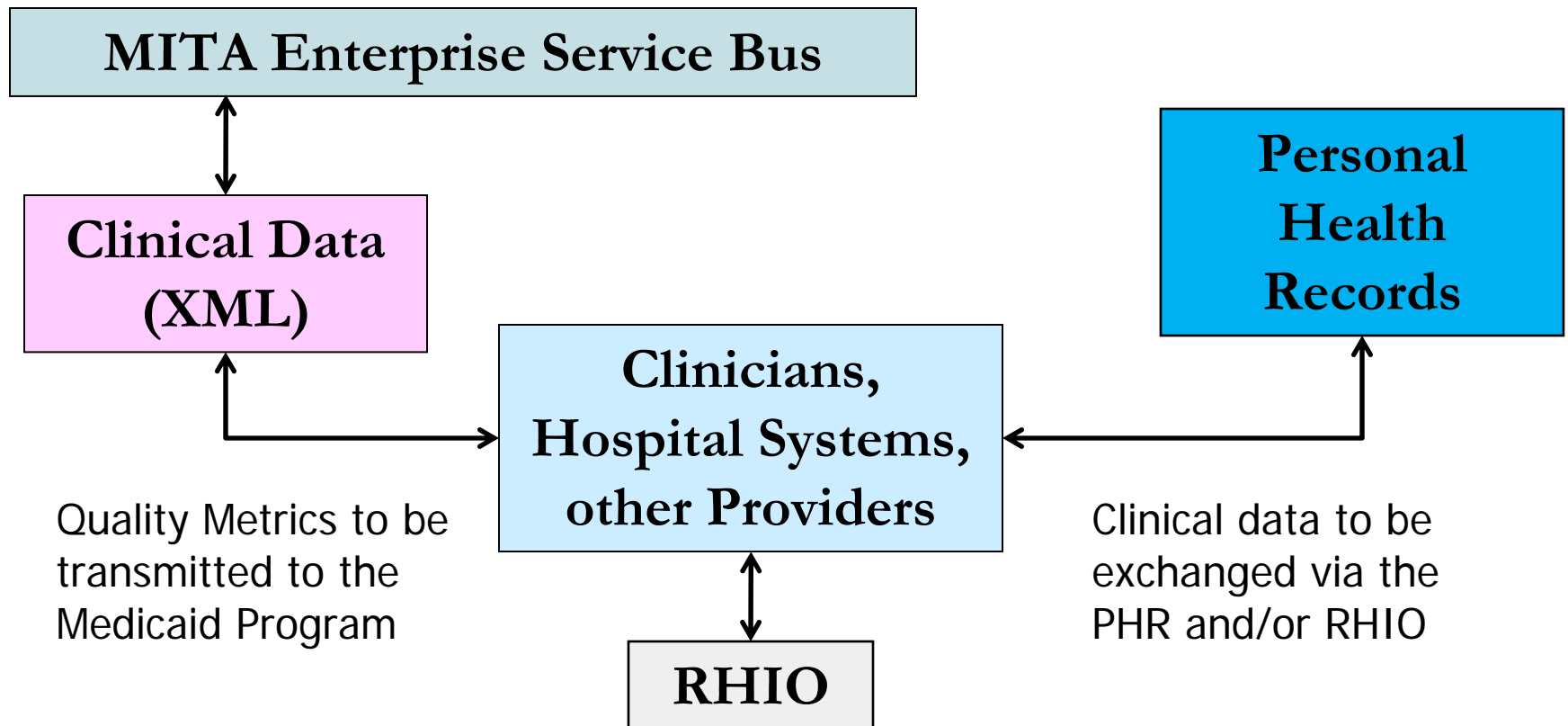


# Proposed Data Elements for the CCD



- Eligibility and Claims-based Data:
  - Eligibility;
  - Diagnoses;
  - Visit History;
  - Medication History.
  
- Clinical Data from External Sources:
  - Laboratory Results;
  - Radiographic Images and Reports.
  
- Public Health Data:
  - Immunizations, Lead, Newborn Screening.

# Data Delivery to Practitioners via the Statewide HIN of NY: Parallel Interoperable Pathways



Centralized Services: Security and Identity Management, Consent Policies

# Medication History



- Features
  - 180 days of Medicaid paid pharmacy claims (fee-for-service and managed care).
  - Medicare Part D claims (will be critical for dual eligible beneficiaries).

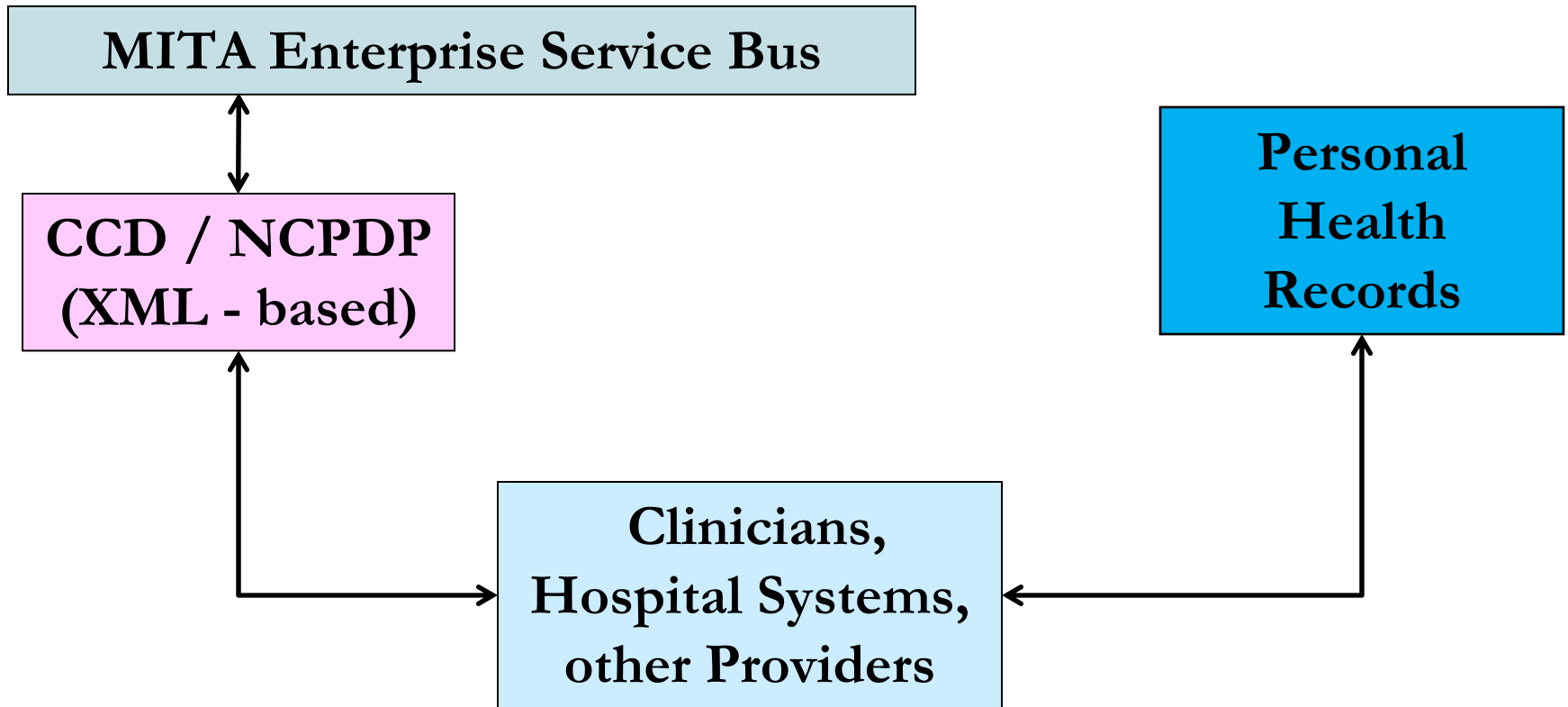


# Medication History Data Standards

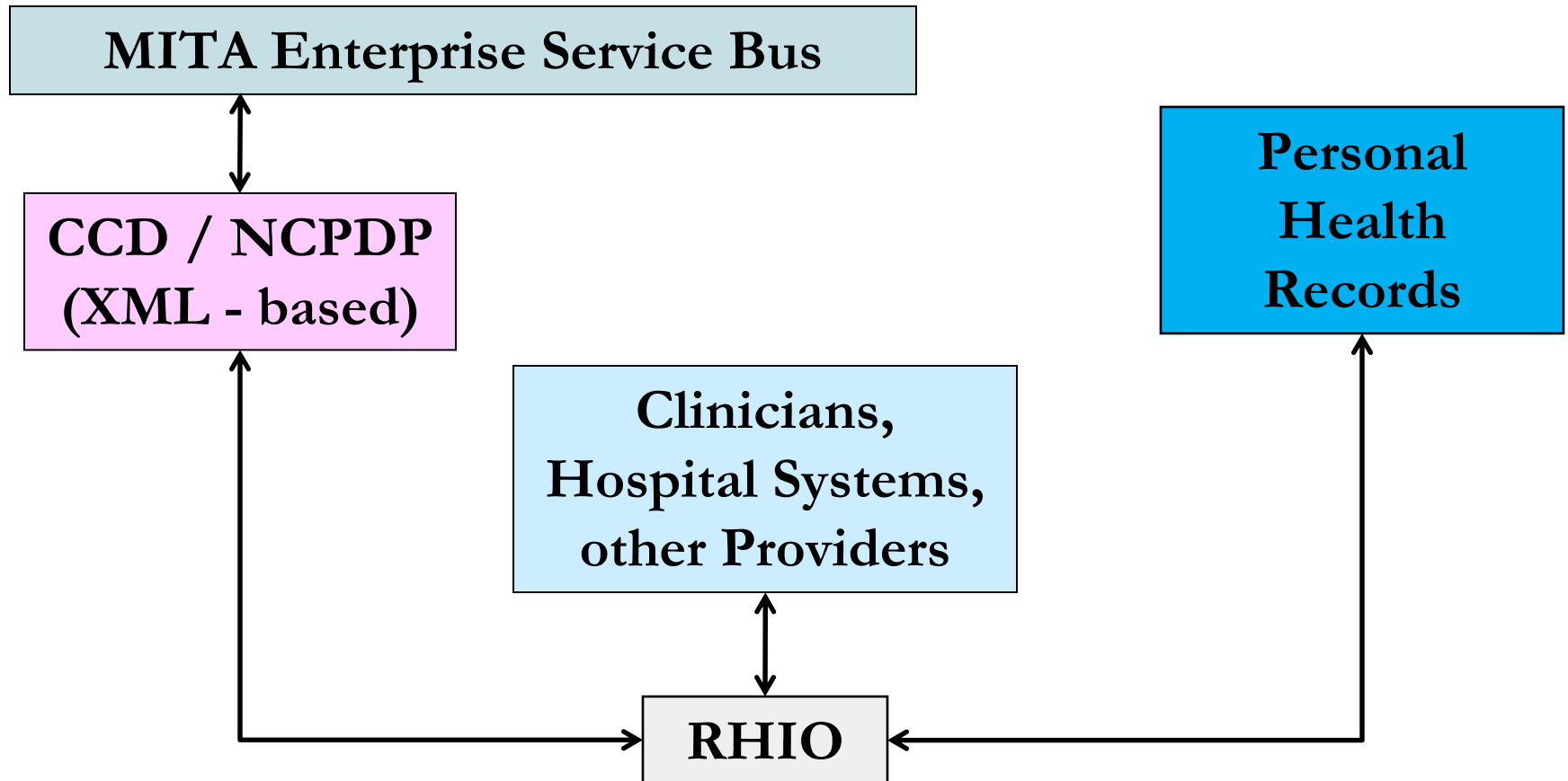
---

- NCPDP Script 10.5 (XML implementation) with plan to migrate to Script 10.6.
- HL7 Continuity of Care Document (CCD).

# Conceptual Data Flows for Medication History – Pattern 1: Direct



# Conceptual Data Flows for Medication History - Pattern 2: via RHIO/HIE



# Security: NIST Authentication Levels



---

- Requirement: authenticate the identity of HIE participants over an open network (Internet).
- Authentication is the process of establishing confidence in user identities when electronically presented to an information system.
- NIST identifies 4 levels of assurance; level 4 is most stringent.

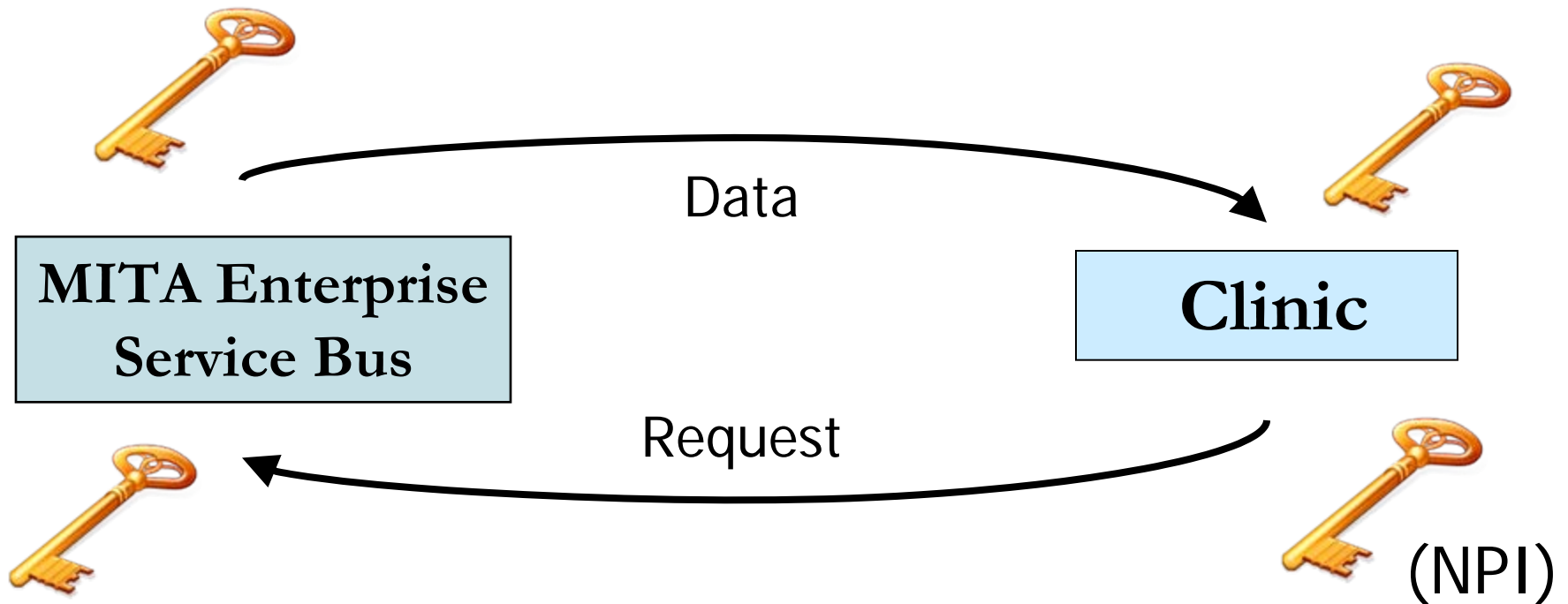
# Security: NIST Authentication Levels (cont'd)

---

- Organizations will conduct a risk assessment and map identified risks to the appropriate assurance level.
- Organizations will then select appropriate authentication protocols to implement the required assurance level.

# Security: Cryptographic Methods (Public Key Infrastructure)

- Process authenticates the identity of HIE participants.
- NPI numbers are linked to cryptographic keys.



# Security: Cryptographic Methods (Public Key Infrastructure, cont'd)

---

- Cryptographic keys are assigned to authorized enrolled providers who meet security thresholds.
- A facility or individual NPI is associated with each key.
- The requesting clinician's individual NPI, and facility NPI when relevant, must be included with all data requests.
- Two sets of factors are required for authentication:
  - Cryptographic key + valid NPI number(s);
  - User name + password.
- The clinician's individual NPI can be used for automated tracking of activities contributing to "meaningful use".



# ONC IFR Adopted Security Standards and NY Medicaid Implementation – 1

---

- IFR: General Encryption and Decryption of Electronic Health Information.
- NY Medicaid: Advanced Encryption Standard (AES), 128 bit.



# ONC IFR Adopted Security Standards and NY Medicaid Implementation – 2

---

- IFR: Encryption and Decryption of Electronic Health Information for Exchange.
- NY Medicaid: Transport Layer Security (TLS) for encryption of the transmission between two servers; protects against communication eavesdroppers.



# ONC IFR Adopted Security Standards and NY Medicaid Implementation – 2 (cont'd)

---

- The business content, in addition, has Message Level Security (MLS) between the original sender and NY Medicaid to prevent intermediaries in the communication process from tampering with or reading the message payload.
- This is achieved via user-specific digital signatures and encryption/decryption keys.

# ONC IFR Adopted Security Standards and NY Medicaid Implementation – 3

---

- IFR: Audit Log.
- NY Medicaid: A complete audit log will be maintained in the Medicaid Data Warehouse (MDW).



# ONC IFR Adopted Security Standards and NY Medicaid Implementation – 4

---

- IFR: Verification that Electronic Health Information has not been Altered in Transit.
- NY Medicaid: A secure hashing algorithm (SHA-1) is employed.

# ONC IFR Adopted Security Standards and NY Medicaid Implementation – 4 (cont'd)

---

- The business content, in addition, has Message Level Security (MLS) between the original sender and NY Medicaid so that intermediaries in the communication process cannot tamper with or read the message payload.
- This is achieved via user-specific digital signatures and encryption/decryption keys.

# ONC IFR Adopted Security Standards and NY Medicaid Implementation – 5

---

- IFR: Cross-enterprise Authentication.
- NY Medicaid: A public key infrastructure featuring user-specific digital signatures and encryption/decryption keys will be employed.
- The fiscal agent serves as the Certificate Authority (CA).
- Users will present a Username and Password which will be protected by TLS.

# ONC IFR Adopted Security Standards and NY Medicaid Implementation – 5 (cont'd)

---

- When necessary, authentication will be propagated using Security Assertion Markup Language (SAML) assertions issued by the CA after authentication.
- The SAML assertions will be deployed in conjunction with CA-issued certificates for use in Message Level Security (MLS).

# ONC IFR Adopted Security Standards and NY Medicaid Implementation – 6

---

- IFR: Record Disclosures.
- NY Medicaid: a complete audit log will be maintained in the MDW with date, time, patient identification, the requestor's individual NPI, and the contents of disclosed information.



# Development of Consent Policies in NYS

---

- Affirmative informed consent.
- Health Information Security and Privacy Collaboration (HISPC) project.
- Statewide collaborative process - NY eHealth Collaborative (NYeC).



## Sensitive Health Information

---

- Various laws (State and Federal) require more specific consent to disclose sensitive health information to third parties.

# Examples of Specially Protected Information under State and Federal Laws in NYS

---

- HIV – related;
- Mental health;
- Alcohol and substance abuse;
- Genetic testing;
- Medicaid data;
- Certain issues regarding minor children.

# Contact Information

**James J. Figge, MD, MBA**  
**Medical Director**  
**NYS Department of Health**  
**Office of Health Insurance Programs**

**One Commerce Plaza, 8<sup>th</sup> Fl, Suite 826**  
**99 Washington Ave.**  
**Albany, NY 12260**

**Phone: (518) 474 - 8045**

**Fax: (518) 473 - 0601**

**Email: [jjf06@health.state.ny.us](mailto:jjf06@health.state.ny.us)**

