Innovation and Problem Solving: Technical and Developer Perspective

Center for Program Integrity
Centers for Medicare and Medicaid Services

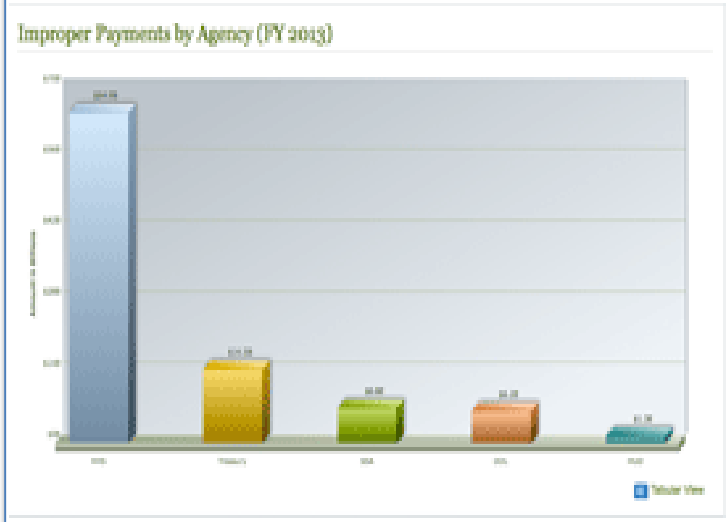
November 29, 2016

Improper Payments

- Medicare receives 1.2 B claims per year.
- CMS' Office of Financial Management estimates that each year (based on 2015 audit information)

FY 2015 Medicare FFS Program Improper Payments – 12.1%

- **$43.3 B -** Total in improper payments
- **$29.2 B -** Improper payments due inadequate/insufficient documentation to support payment for services billed
- **$8.8 B -** Improper payments is due to services that were not medical necessary based on Medicare coverage policies



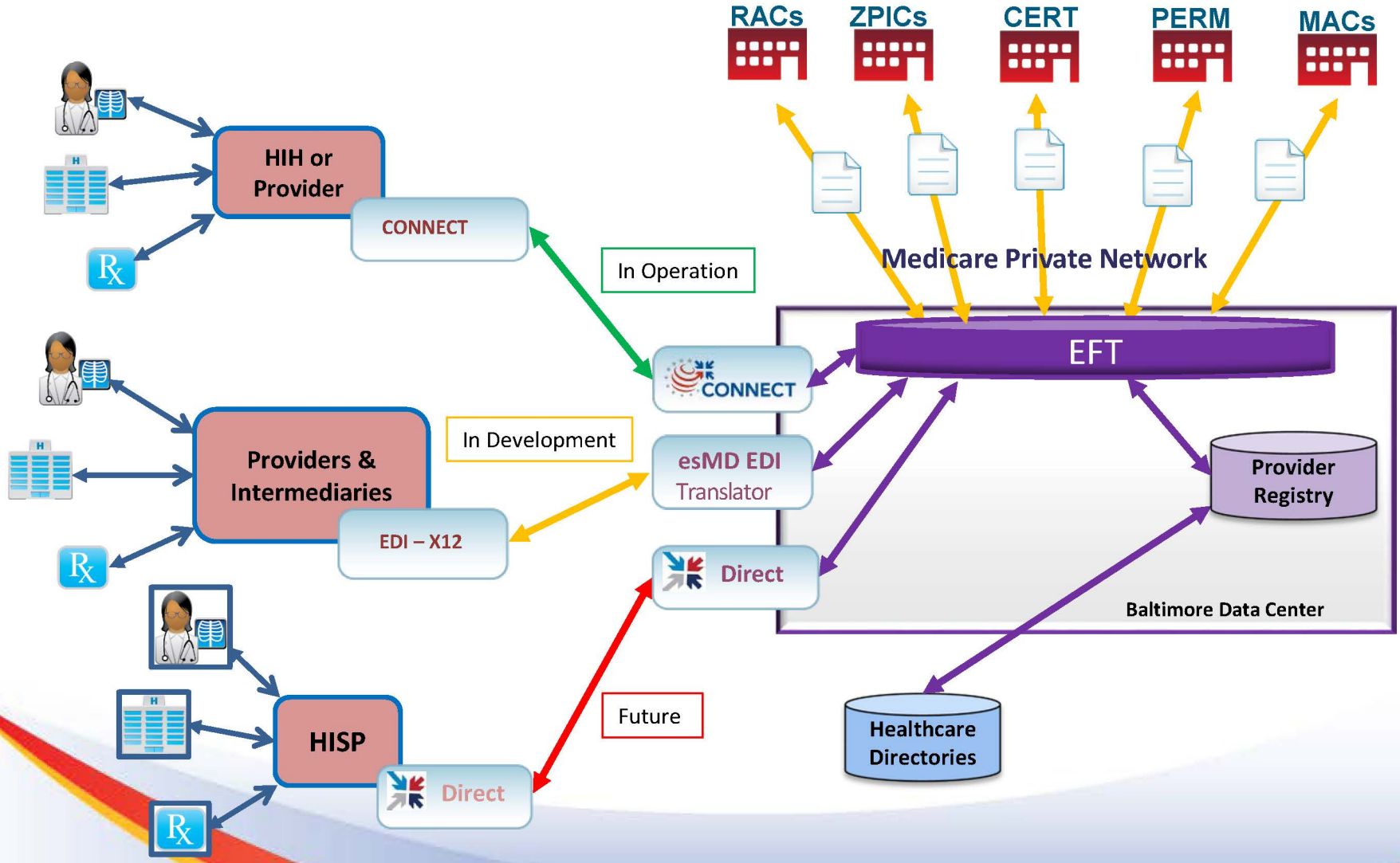
www.paymentaccuracy.gov

- Over 3 million Claim Reviews in response to Medical Documentation Requests are sent annually by:
  - Medicare Administrative Contractors (MACs) Medical Review (MR) Departments
  - Comprehensive Error Rate Testing Contractor (CERT)
  - Payment Error Rate Measurement Contractor (PERM)
  - Medicare Recovery Auditors (formerly called RACs)

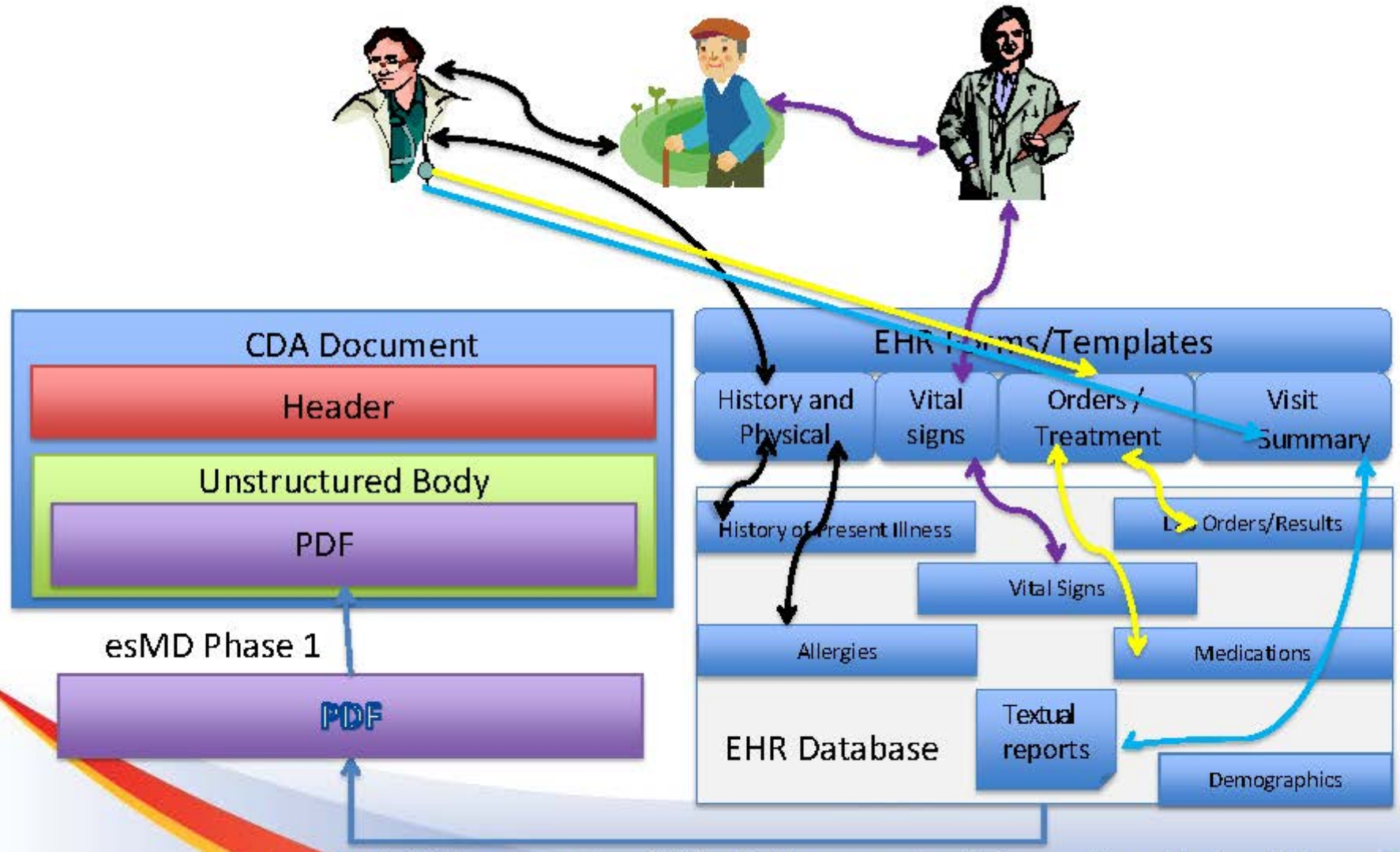
Standards to address incomplete documentation

1. Secure Exchange Standards
   - eHealth Exchange – esMD
   - Direct
2. Exchange Content Standards
   - Structured information to simplify reporting and review
   - Standard format and content C-CDA / CDP
3. eClinical Templates
   - Based on HL7 FHIR ®
   - Defined clinical data elements
   - Electronic templates to support information collection
4. Digital Signatures

esMD Interoperability Direction



Today – Typical Response to Request for Documentation

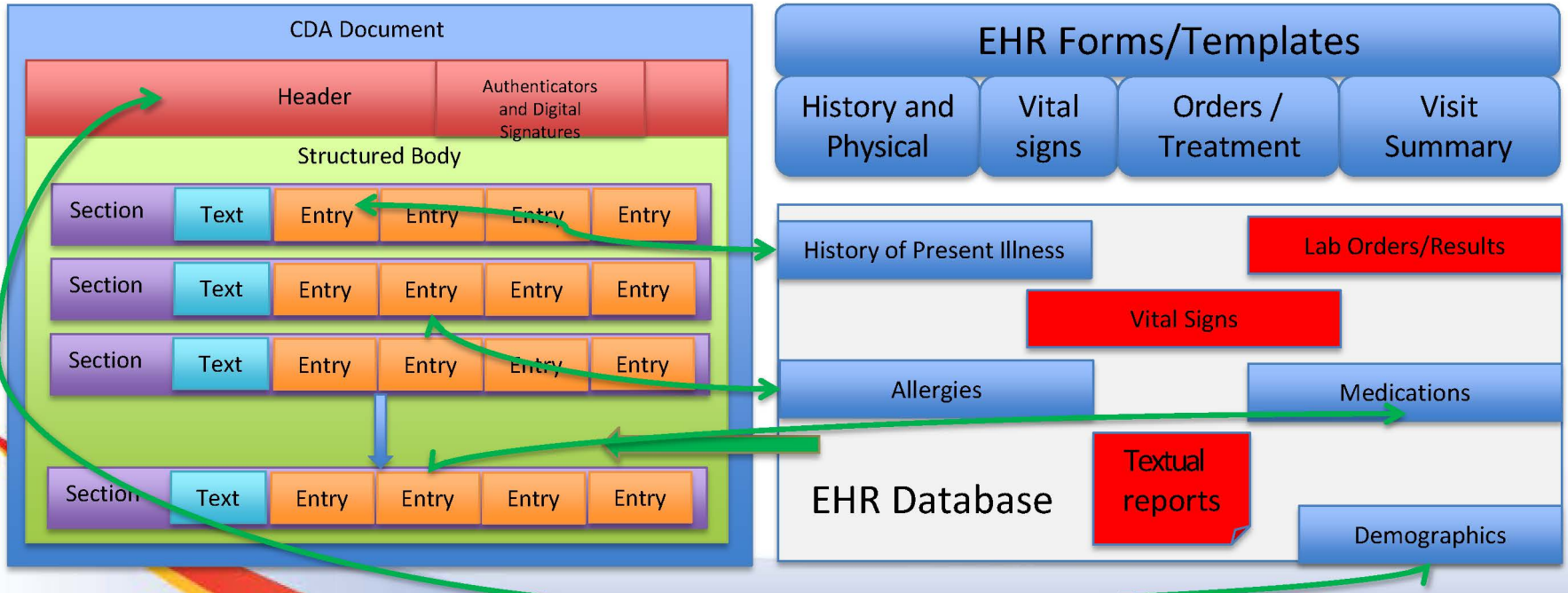


Current Templates

Use of Current Templates

Create Structured CDA

1) Works for required sections
2) Optional sections may not be supported by all EHR vendor
3) How does the provider meet documentation requirements?
4) Recipient of the document does not know if data does not exist or data is being withheld

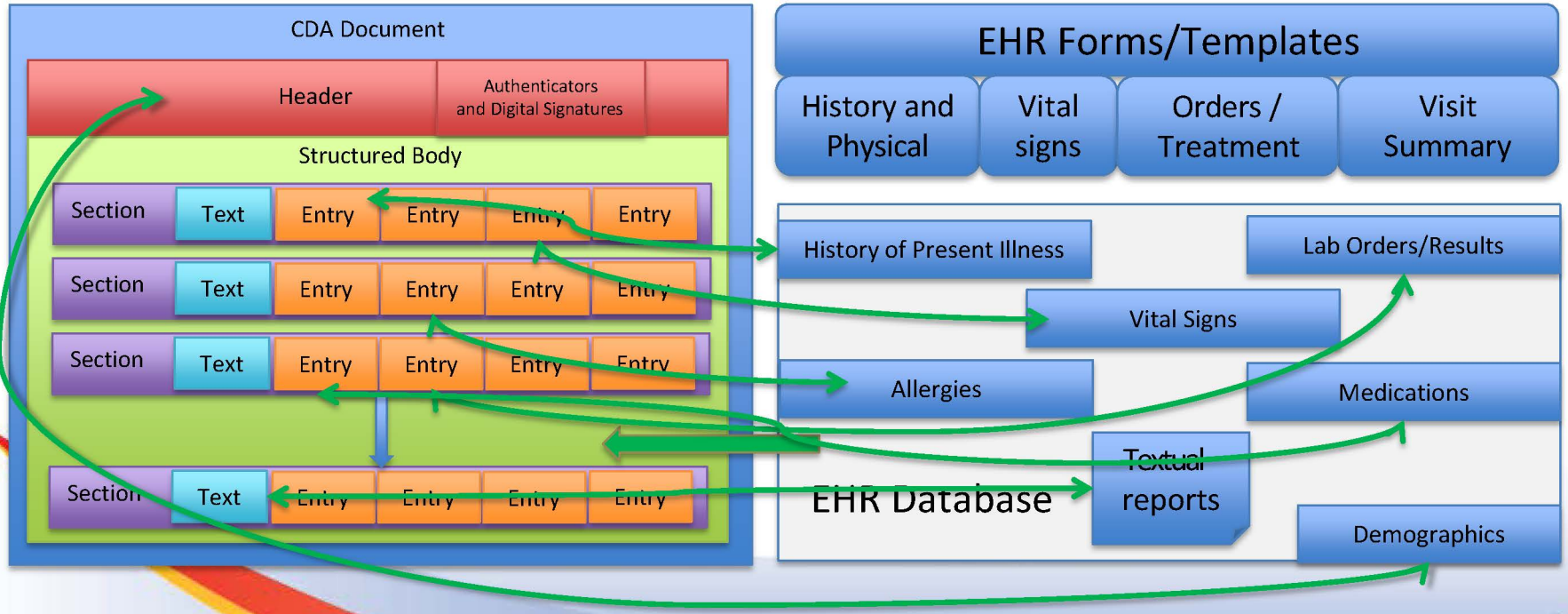


Create "Complete" CDA

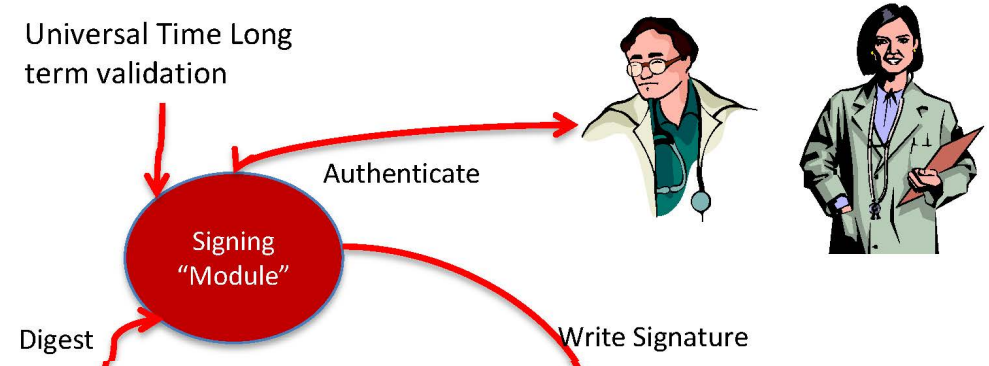
Prior to or at time of signing – create CDA from Complete Document Template

Create Structured CDA from Complete Document Template

1) All Document sections are populated or use appropriate nullFlavor
2) Ensures that all captured documentation is in the CDA prior to signing

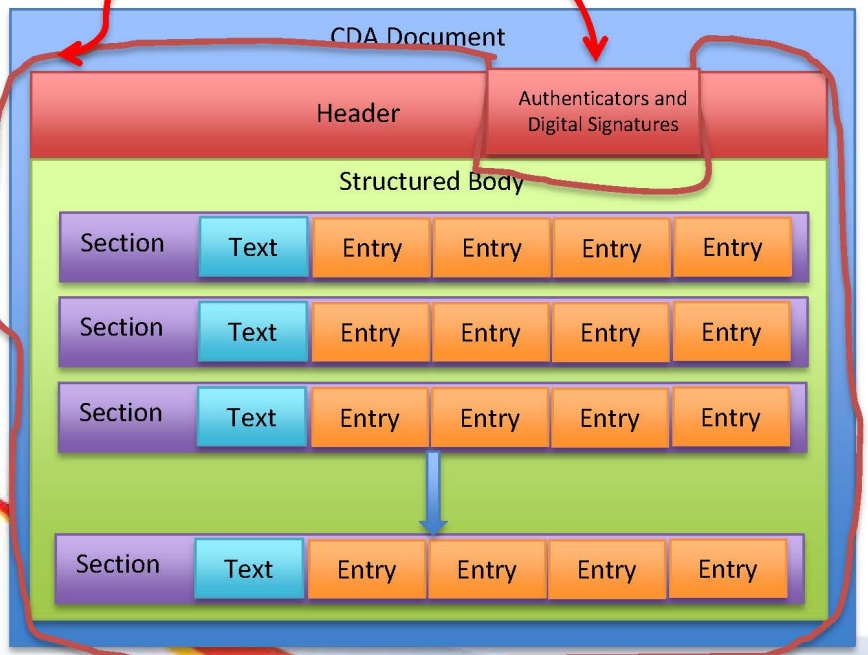


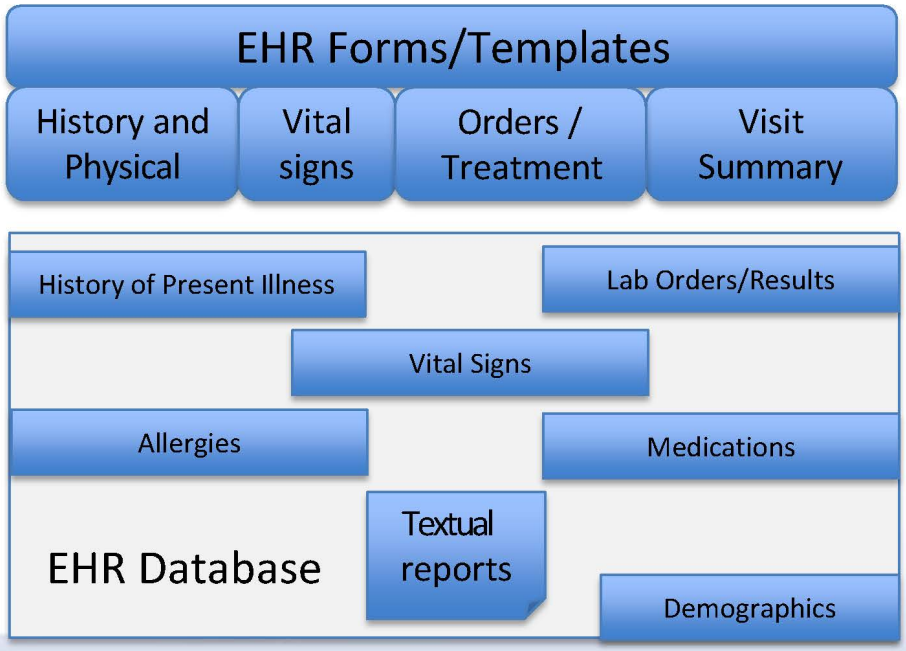
Sign CDA (based on policy)



Notes:

1) Attestation as to authorship of document
2) Fixes the content, role and signature purpose at time of signing



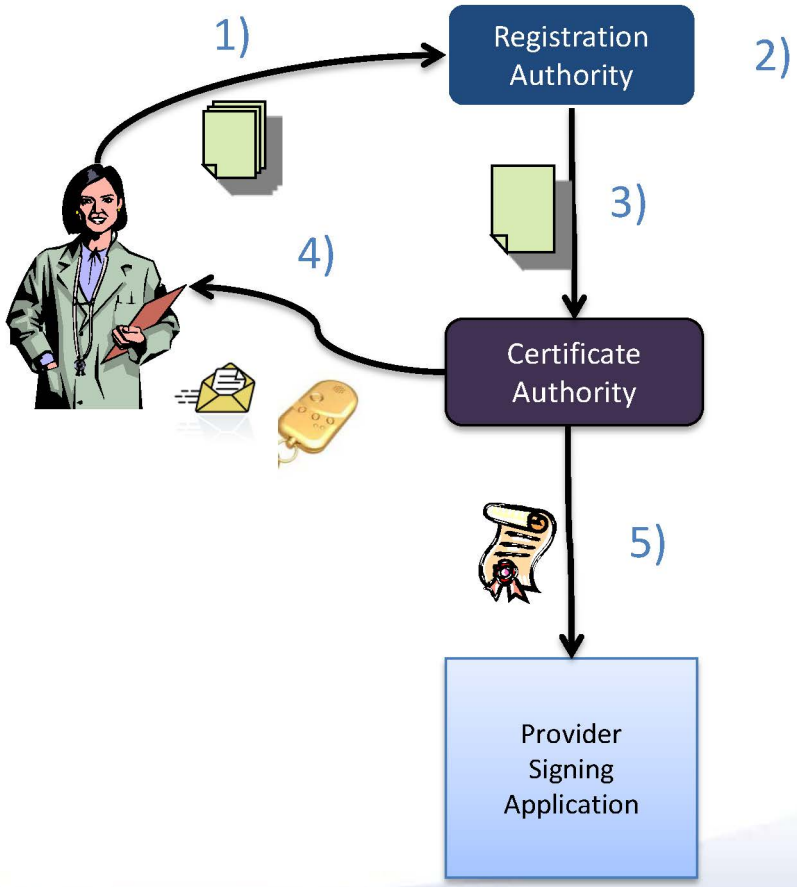


Why Digital Signatures

- Wet Signatures
  - Standards are based on legal precedence
  - Non-repudiation inherent in wet signature
  - Often requires an attestation to determine validity
  - Timing of signature is difficult to determine
- Electronic Signatures
  - Standards are based on technology and legal precedence
  - Require audit of signing system (e.g. EMR) installation, policies, and audit logs – significant burden on both parties
  - May require an attestation to determine validity
- Digital Signatures
  - International and US Federal standards -- based on cryptography
  - Identity proofing and certificate issuance/use ensure non-repudiation
  - Time stamp on document is evidence of when signing occurred
  - Data integrity is ensured – any change in information voids the signature

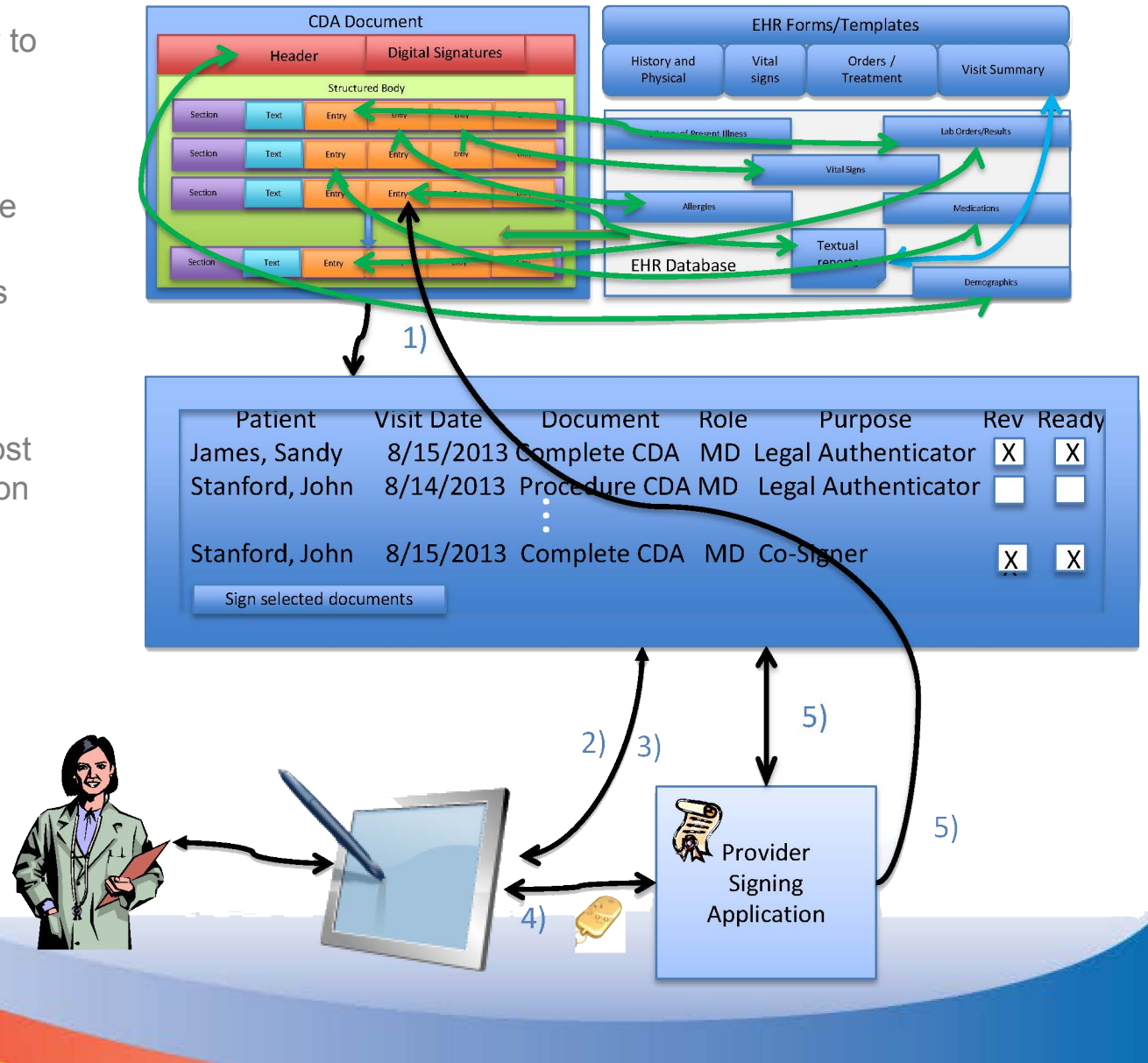
Provider Setup for Digital Signatures

1) Individual provider supplies IDs and other information as part of credentialing or to a standalone Registration Authority (RA)
2) RA verifies credentials
3) Certificate Authority (CA) receives providers information from the RA
4) CA issues access information (e.g. hard token) to the individual provider
5) CA issues encrypted key to the signing application key store



Signing Process -- Suggested

1) C-CDA created for activity to be signed (system or on-demand)
2) Signer views list of documents (C-CDAs) to be signed
3) Signer reviews documents and indicates ready for signature and where appropriate role and signature purpose (will most likely be defaulted based on signer)
4) Signer authenticates to Signing Application
5) Signer signs list of all reviewed and accepted documents

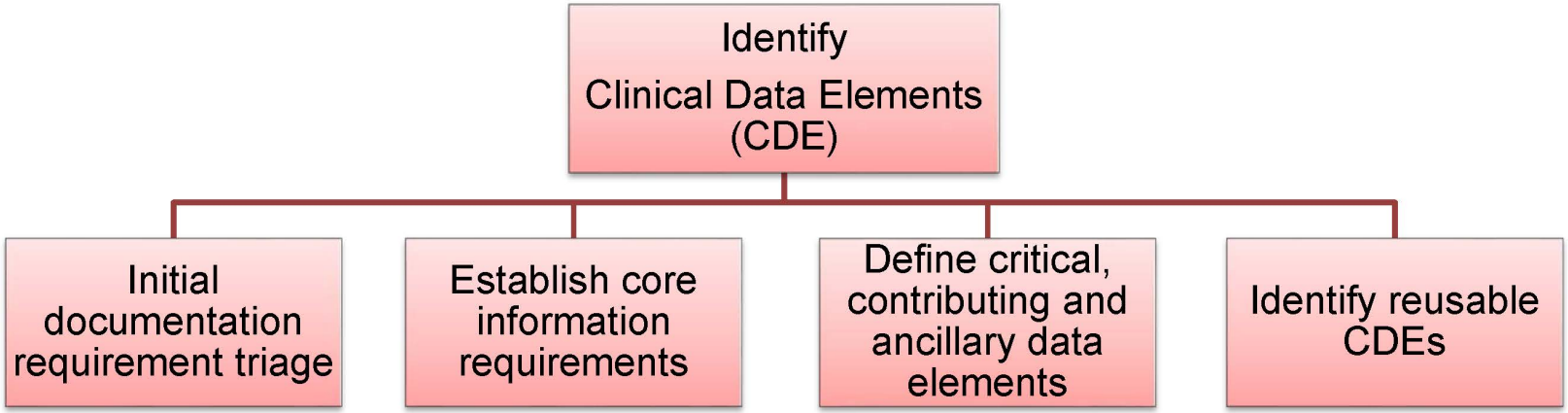


Electronic Clinical Templates

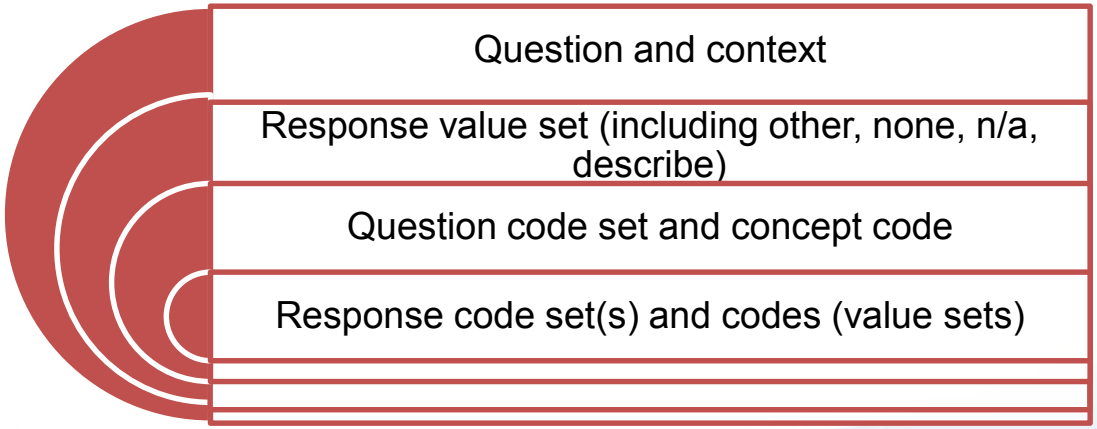
Two paths forward

- Clinical Data elements for incorporation into Electronic Health Records (EHRs)
- Electronic Clinical Templates based on standards with high adoption rates

Clinical Data Elements



Define Data Elements



e-Clinical Templates using ONC's Structured Data Capture (SDC)

Reduces Documentation Burden	• Standardized templates that support pre-population from the provider's EHR • Focus on relevant clinical information to support determination of coverage
Promotes Structured Data	• Information based on defined clinical data elements • Enables evaluation by rules systems
Reduces need for site-specific EHR enhancements	• Enable EHR systems to broadly participate

SDC identified/defined/enhanced **four** required standards to enable EHRs to capture and store structured data:

1. Standard for the structure of the CDEs that will be used to fill the templates
2. Standard for the structure or design of the template
3. Standard for how EHRs interact with the template
4. Standard to auto-populate template

Electronic Clinical Templates

Provider

1. Selects template

EHR

2. Finds template

3.Returns template to EHR System

eClinical Template Library

5. Inputs missing data and approves / digitally signs template

4. Pre-populates and displays template

Template Display

6.Stores "signed" CDEs in EHR System

Patient Medical Record

7. Exchanges structured information with other providers

Provider Referral, Consult, Service (e.g. DME)

CMS

8a. Creates CDP1 from encounter record and sends to CMS

8. Creates CDP1 from encounter record and other documentation and sends to CMS

Summary

Problem:

- Medicare FFS improper payment rate exceeds $43 billion / year
- Incomplete documentation accounts for over $29 billion / year

Solutions

- Standard based approach to structured documentation
- Secure exchange of information for clinical and administrative needs
- Use of electronic templates to remind providers of specific documentation requirements to support covered services
- Digital signatures to ensure data integrity and provenance