HIT Standards Committee

Privacy and Security Workgroup joint meeting with Clinical Operations Workgroup:
Digital Signatures for CMS Electronic Submission of Medical Documentation (esMD)

August 8, 2013

Agenda

3:00 pm	Call to Order/Roll Call *Michelle Consolazio, ONC*
3:05 pm	Welcome and Agenda Review *Dixie Baker and Walter Suarez, Co-Chairs Privacy & Security Workgroup*
	Welcome and Comments *Jamie Ferguson and John Halamka, Co-Chairs Clinical Operations Workgroup*
3:15 pm	Overview of CMS Plans for Electronic Submission of Medical Documentation (esMD) *Melanie Combs-Dyer and Bob Dieterle*
3:45 pm	DEA and CMS Digital Signature Requirements Side-by-Side *Debbie Bucci (ONC)*
4:00 pm	Workgroups Discussion
4:25 pm	Public Comment
4:30 pm	Adjourn

Electronic Submission of Medical Documentation

electronic submission of Medical Documentation (esMD) Author of Record

Presentation to HITSC

August 8, 2013

MELANIE COMBS-DYER, RN
Deputy Director,
Provider Compliance Group
Office of Financial Management, CMS

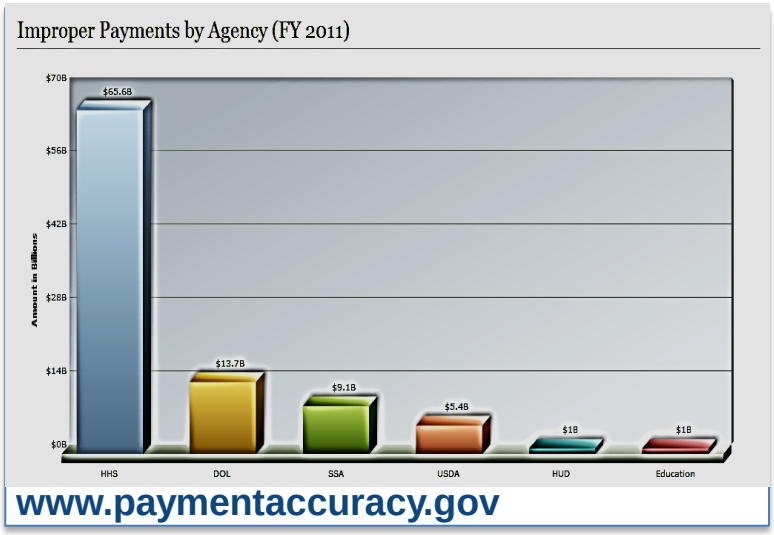
ROBERT DIETERLE
esMD Initiative Coordinator
Signature Consulting Group

Overview

1. esMD Background
2. S&I esMD Initiative
   a) Sending a secure eMDR to a provider
   b) Replace “wet signature”
   c) Move to structured documentation submissions
3. AoR workgroup recommendations
4. AoR Level 1 (Digital Signature on transactions and document bundle)
5. AoR Level 2 (Digital Signature on C-CDA)

Improper Payment

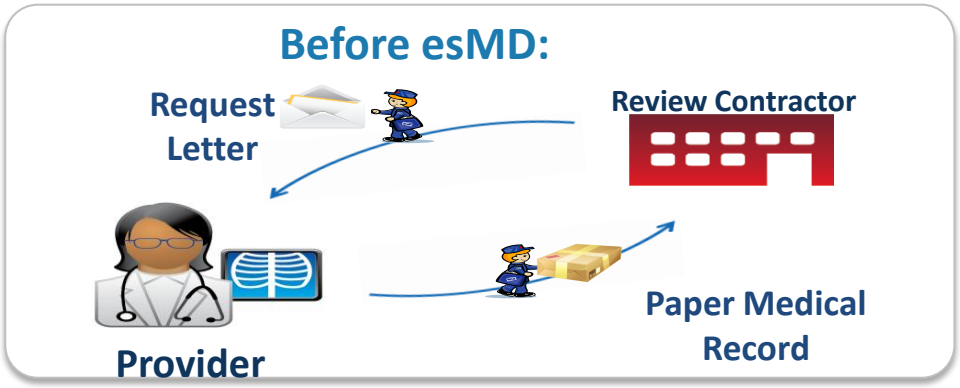
- Medicare receives **4.8 M** claims per day.
- CMS' Office of Financial Management estimates that each year
  - the Medicare FFS program issues more than **$28.8 B** in improper payments (error rate 2011: **8.6%**).
  - the Medicaid FFS program issues more than **$21.9 B** in improper payments (3-year rolling error rate: **8.1%**).
- Most improper payments can only be detected by a **human** comparing a **claim** to the **medical documentation.**



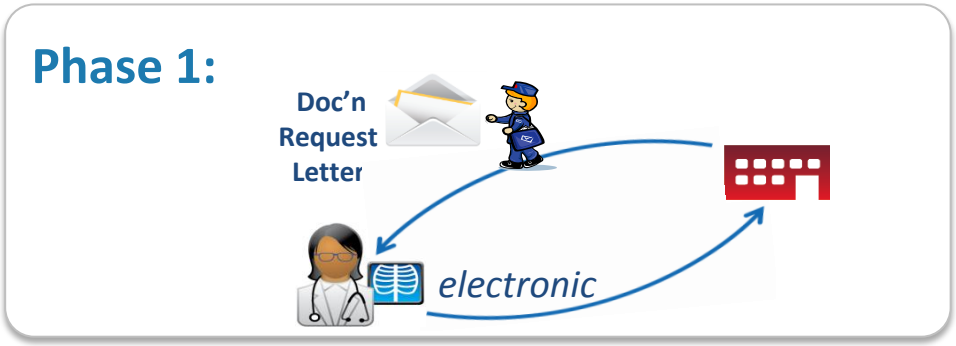
- **Medical Documentation Requests are sent by**:
  - Medicare Administrative Contractors (MACs) Medical Review (MR) Departments
  - Comprehensive Error Rate Testing Contractor (CERT)
  - Payment Error Rate Measurement Contractor (PERM)
  - Medicare Recovery Auditors (formerly called RACs)
- Claim review contractors issue over **1.5 million** requests for medical documentation each year.
- Claim review contractors currently receive most medical documentation in **paper** form or via fax.

eSMD Electronic Submission of Medical Documentation

esMD Background

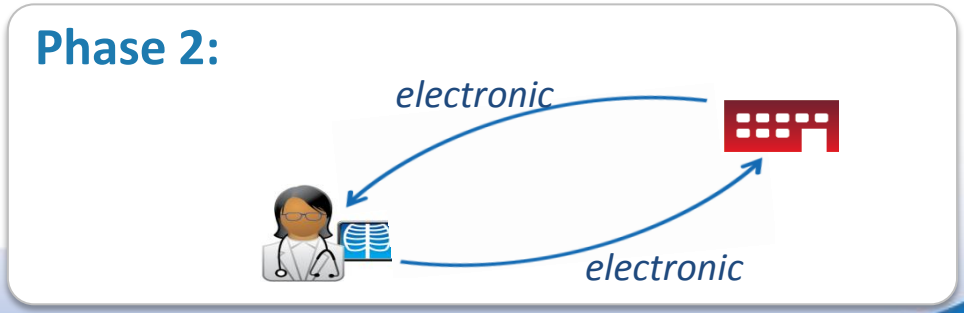


Healthcare payers frequently request that providers submit additional medical documentation to support a specific claim(s). Until recently, this has been an entirely paper process and has proven to be burdensome due to the time, resources, and cost to support a paper system.



Phase I of esMD was implemented in September of 2011. It enabled Providers to send Medical Documentation electronically

The ONC S&I Framework Electronic Submission of Medical Documentation (esMD) initiative is developing solutions to support an entirely electronic documentation request.



Electronic Submission of Medical Documentation

6

Goals of esMD

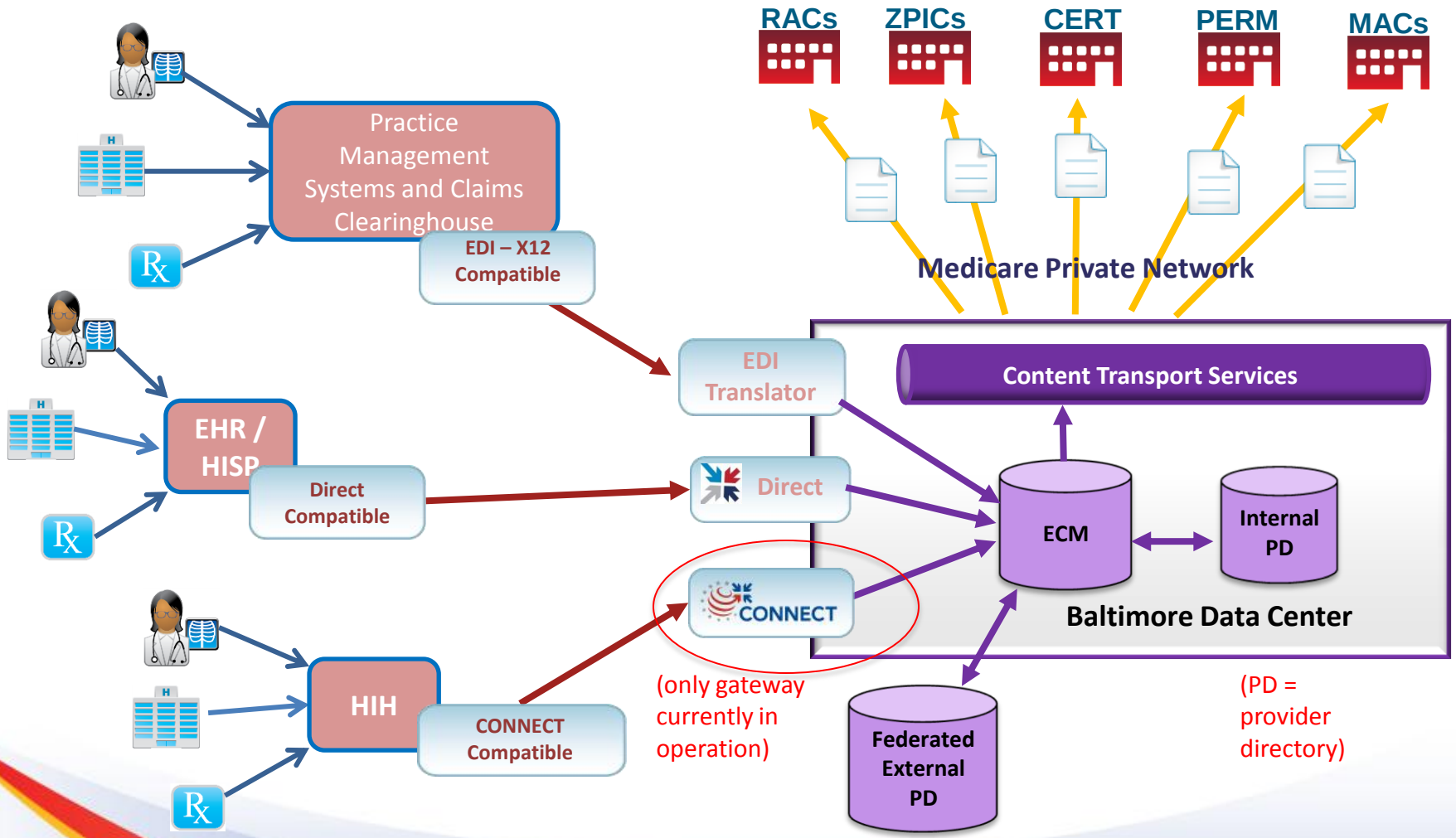
1) Reduce administrative burden
2) Reduce improper payment
3) Move from “post payment audit” to prior-authorization or pre-payment review

Requirements

1) Move from paper to electronic communication
2) **Replace “wet signatures” with digital signatures**
3) Migrate from unstructured data to structured data over time

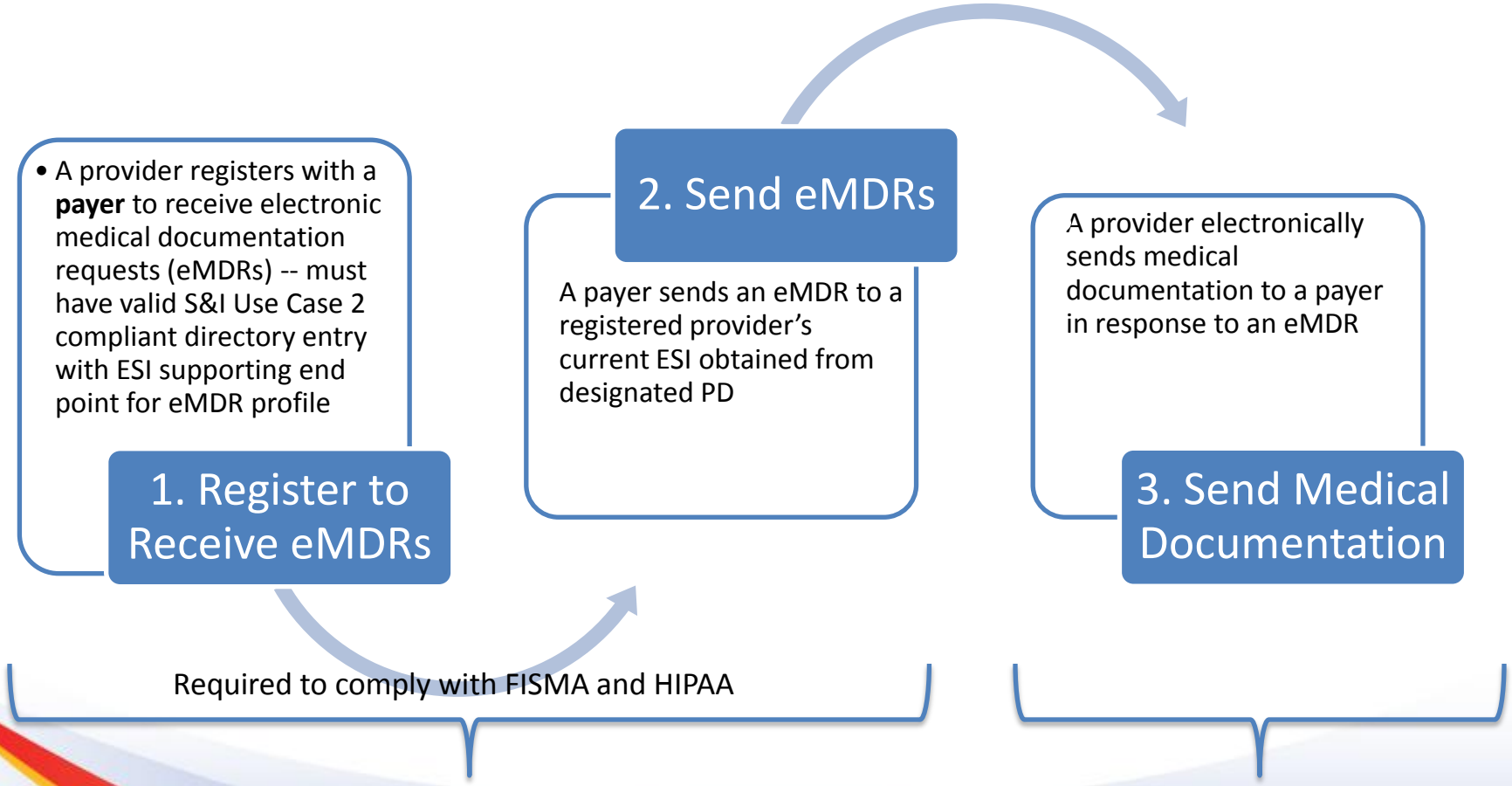
Electronic Submission of Medical Documentation

Electronic Submission of Medical Documentation (esMD) Supporting Multiple Transport Standards and Provider Directory

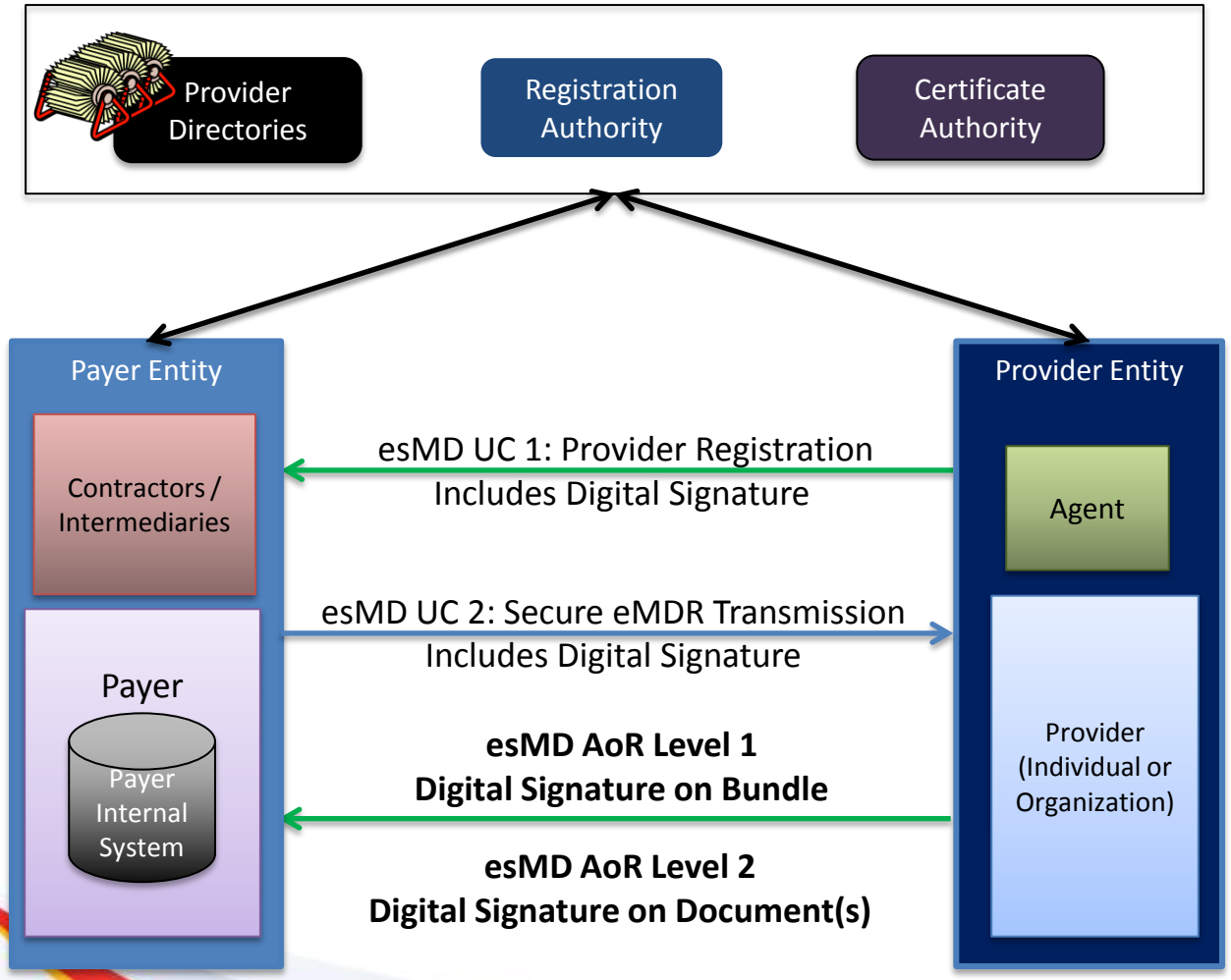


esMD eMDR Process Flow

The overall esMD eMDR process can be divided into three steps:



S&I Framework esMD eMDR Overview

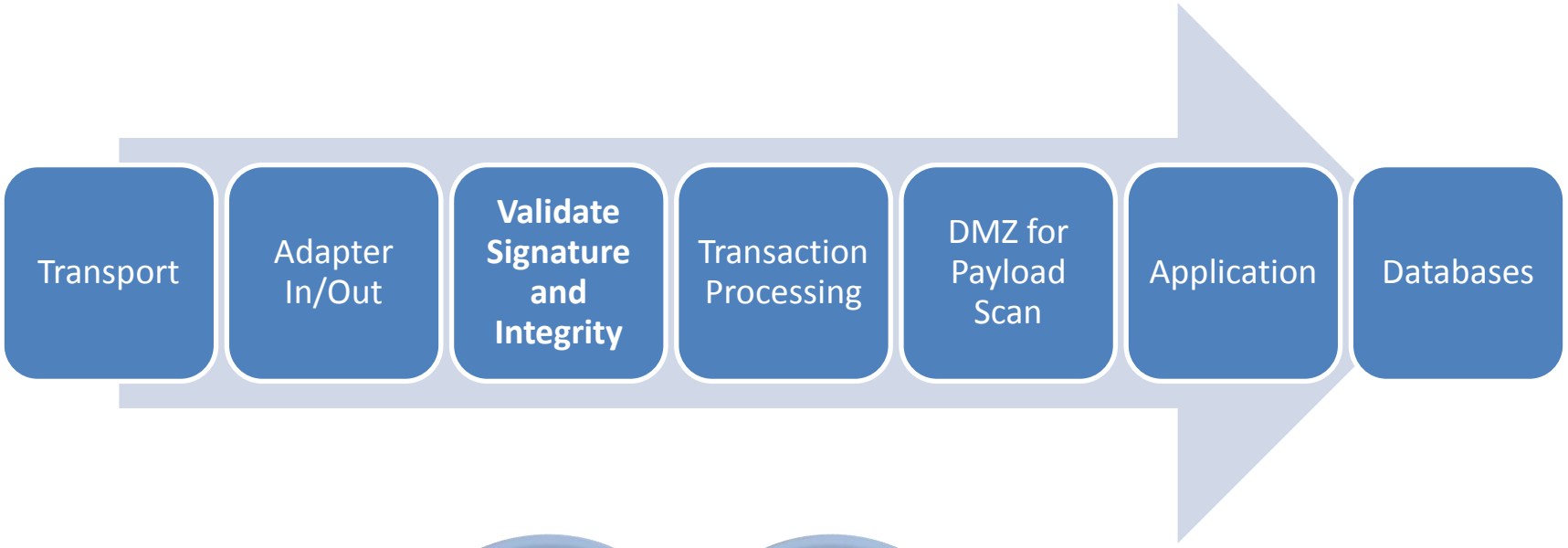


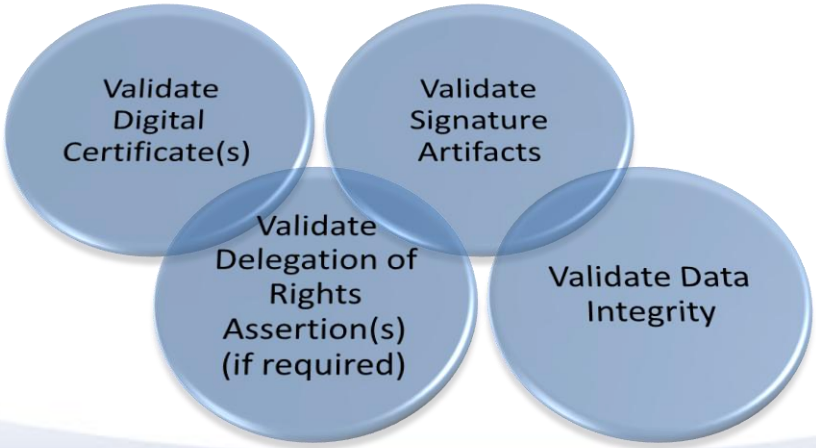
User Story

- **All Actors obtain and maintain a non-repudiation digital identity**
- **Provider registers for esMD (see UC1)**
- **Payer requests documentation (see UC2)**
- **Provider submits digitally signed document (bundle) to address request by payer**
- **Payer validates the digital credentials, signature artifacts and, where appropriate, delegation of rights**
- **If Documents are digitally signed, then payer validates document digital signature artifacts**

Electronic Submission of Medical Documentation

General esMD Flow





Definitions

Identity (Proposed)

A set of attributes that uniquely describe a person or legal entity within a given context.

Identity Proofing (Proposed)

The process by which a CSP and a Registration Authority (RA) collect and verify information about a person or legal entity for the purpose of issuing credentials to that person or legal entity.

Digital Signature (NIST)

The result of a cryptographic transformation of data that, when properly implemented, provides a mechanism for verifying origin authentication, data integrity and signatory non-repudiation.

Data Integrity (NIST)

Data integrity is a property whereby data has not been altered in an unauthorized manner since it was created, transmitted or stored. Alteration includes the insertion, deletion and substitution of data.

Non-repudiation (NIST)

Non-repudiation is a service that is used to provide assurance of the integrity and origin of data in such a way that the integrity and origin **can be verified by a third party**. This service prevents an entity from successfully denying involvement in a previous action.

Delegation of Rights

The ability to delegate rights or authority to another to act in a specific capacity on behalf of the grantor of the right. Must include the digital identity of the grantor, the digital identity of the grantee, the rights granted, duration of grant in a format that is usable in transaction and AoR signature events and is verifiable by a third party for non-repudiation purposes.

AoR -- Phased Scope of Work

Level 1 – Current Focus

Digital signature on *aggregated* documents (bundle)

- Focus is on **signing a bundle of documents** prior to transmission to satisfy an eMDR
- Define requirements for esMD UC 1 and UC 2 Signature Artifacts
- May assist with EHR Certification criteria in the future

Level 2 - TBD

Digital signature on an *individual* document

- Focus is on **signing an individual document** prior to sending or <u>at the point of creation by providers</u>
- Will inform EHR Certification criteria for signatures on patient documentation

Level 3 - TBD

Digital signature to allow traceability of *individual contributions to a document*

- Focus is on **signing documents and individual contributions** at the point of creation by providers
- Will inform EHR Certification criteria for one or multiple signatures on patient documentation

esMD AoR Sub-Workgroups

1. Identity Proofing

- Define required process for identity proofing of healthcare individuals and organizations for esMD
- Proof of identity requirements
- Allowed proofing processes

2. Digital Credentials

- Define required process for issuing and managing digital credentials for esMD
- Credential Life Cycle (issuance, maintenance and revocation)
- Credential uses (Identity, Signing, Proxy, Encryption, Data Integrity)
- Specific use credentials (e.g. Direct)

3. Signing and Delegation

- Define process, artifacts and standards for transaction and document bundle digital signatures and delegation of rights for esMD
- Signature and Delegation artifacts
- Workflow issues
- Delegation process

Deliverables from all SWGs include:

- Statement of problem and assumptions
- Review of Standards
- Recommended standards
- Operational/Implementation Considerations
- Analysis of Gaps in standards and policy

Identity Proofing

Standards

Document Link	Title & Version / Notes	Date
FBCA X.509 Certificate Policy	*X.509 Certificate Policy for the Federal Bridge Certification Authority*, Version 2.25	Dec 9 2011
FICAM Roadmap and Implementation Guidance	*Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance*, Version 2.0	Dec 2 2011
NIST SP 800-63-1	*Electronic Authentication Guideline*	Dec 2011

Federal Bridge Certification Authority – Medium Assurance

Level	Identification Requirements
Medium	Identity shall be established by in-person proofing before the Registration Authority, Trusted Agent or an entity certified by a State or Federal Entity as being authorized to confirm identities; information provided shall be verified to ensure legitimacy. A trust relationship between the Trusted Agent and the applicant which is based on an in-person antecedent may suffice as meeting the in-person identity proofing requirement. Credentials required are one Federal Government-issued Picture I.D., one REAL ID Act compliant picture ID1, or two Non-Federal Government I.D.s, one of which shall be a photo I.D. (e.g., Non-REAL ID Act compliant Drivers License). Any credentials presented must be unexpired. ...

Identity Proofing Recommendations and Gaps

Recommendations

- Identity Proofing compliant with FBCA Medium Assurance
- In-person or acceptable antecedent event
- Must include verification of NPI or alternative provider ID if used for Author of Record (not required for recipient of delegation of rights)
- One Identity Proofing for all credentials as same level of assurance or lower from all CSPs
- Federation of RAs to achieve required scale through use of current in-person healthcare verification process
  - Credentialing
  - Licensure
  - HR functions

Gaps

- Policy for Individual Identity Proofing acceptable to all cross-certified CSPs that participate
- Policy for Organizational Identity Proofing (e.g. for group certificate)
- Policy for RA Accreditation (including duration and termination)
- Policy for Certification of RA Accreditors
- Agreement by FBCA cross-certified CA's to recognize the policies and process
- Policy for acceptance of prior in-person verification (antecedent)

Standards for Signing Credentials

Standards for Signing Credentials

Document Link	Title & Version / Notes	Date
FBCA X.509 Certificate Policy	*X.509 Certificate Policy for the Federal Bridge Certification Authority*, Version 2.25	Dec 9 2011
FICAM Roadmap and Implementation Guidance	*Federal Identity, Credential, and Access Management Roadmap and Implementation Guidance*, Version 2.0	Dec 2 2011

Digital Credential Recommendations and Gaps

Recommendations

- X.509v3 signing certificates with the non-repudiation bit set must be used to sign all AoR Transactions, Bundles and Documents
- All CSP/CAs must be cross-certified with FBCA
- There may only be one level of sub-CAs (e.g. sub-CA may only issue end user certificates)
- Providers must authenticate to the signing module with at least one additional authentication factor prior to the actual signing event

Gaps

- Long term validation (see XAdES-X-L)

Digital Signatures and Delegation of Rights (DoR)

Standards for Digital Signatures and Delegation of Rights Assertions

Standard and Link	Issued by	Version / Date
FBCA X.509 Certificate Policy	*X.509 Certificate Policy for the Federal Bridge Certification Authority*, Version 2.25	Dec 9 2011
FIPS PUB 186-3	*Digital Signature Standard*	Jun 2009
XML DigSig / XADES-XL	*XML Signature Syntax and Processing (Second Edition), W3C Recommendation*	Jun 10 2008
OASIS SAML Assertions ***All SAML v2.0 files***	*Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML), Version 2.0*	Mar 15 2005

Digital Signature and DoR Recommendations

Digital Signature

- XML DigSig
- XADES-X-L includes:
  - Digest of Message
  - Time stamp (UTC)
  - Role
  - Long term validation

Delegations of Rights Assertion

signed SAML 2.0 Assertion containing the following elements:

- Time stamp (UTC)
- Issuer and Right recipient X.509v3 ID number
- Valid date range
- Right(s) delegated

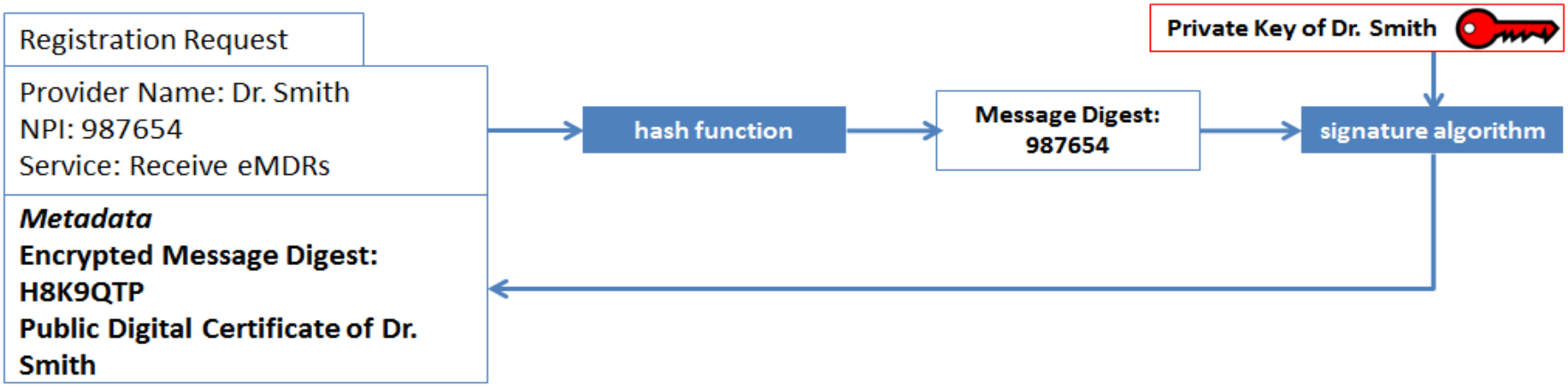
Gaps

- Validation/Revocation of Assertion (Validate at time of use)

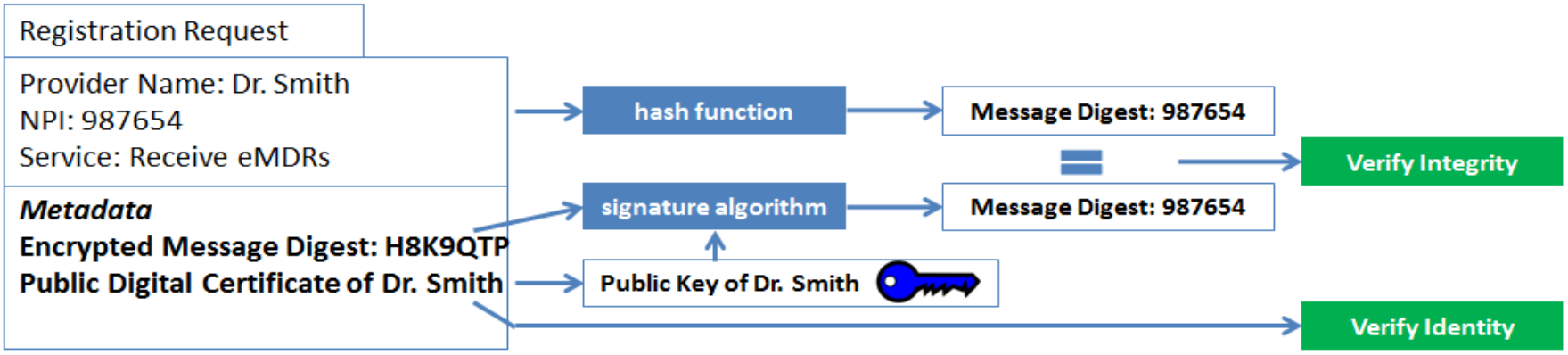
Signature Artifact Example

Signature on a transaction

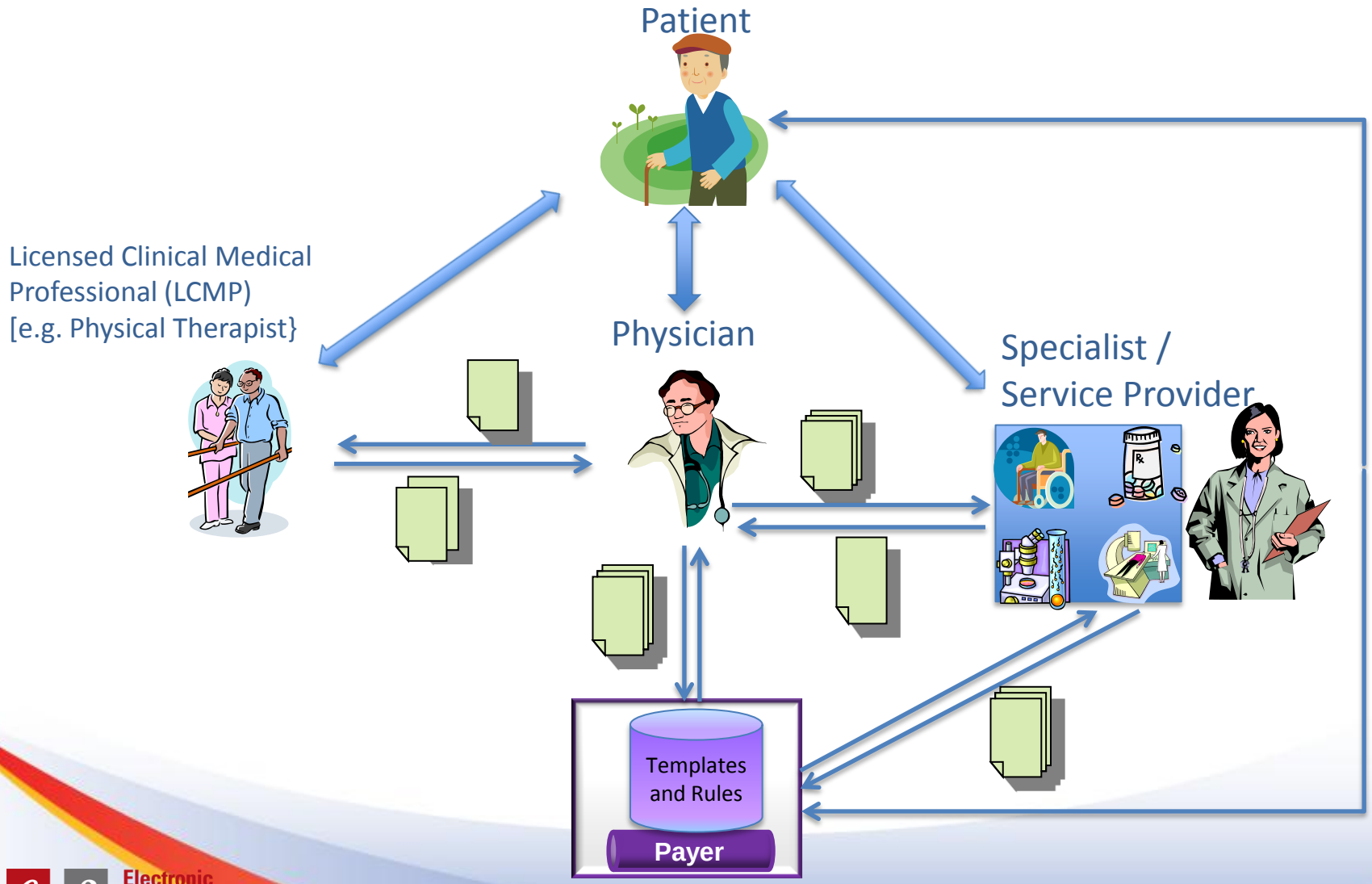
1. **Dr. Smith attaches signature artifact to Request to Register to Receive eMDRs**



2. **Payer verifies the Request came from Dr. Smith and has not been tampered with**



electronic Determination of Coverage (eDoC) Generic Workflow



Electronic Submission of Medical Documentation

Author of Record Level 1

Digital signature on bundle of documents

1) Standards
   a) PKI: X.509v3 Signing Certificates (FBCA Medium)
   b) IHE DSG (XAdES)
   c) SAML Assertion for delegation of rights

2) Environment (example)
   1) Created as part of sending documents from provider to payer
   2) Validated upon receipt
   3) One signer (submitter) only for the full bundle of documents
   4) Delegation of rights as required to support authorization chain

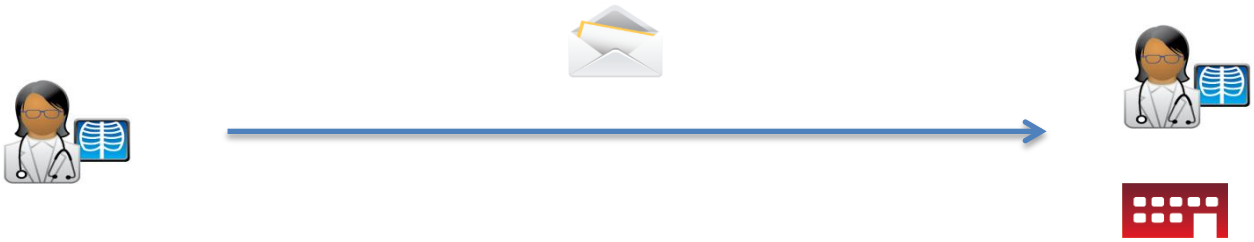
Author of Record Level 2 Requirements

1. Digital signature on documents for provenance (clinical and administrative)
   - Meets requirement for encapsulated non-repudiation
2. Signature should be applied at time of document creation, modification, review (Administrative – must be applied prior to claim submission)
3. Multiple signatures on same “document”
4. Certificate must be validated at time it is used (OCSP or CRL)
5. Support for validated delegation of rights assertion
6. Signature and delegation of rights must travel with document
7. Signature bound to signed document for life-time of document
8. Supports transition from unsigned to signed documents over time

Example: Multiple signatures in a pdf document (decoupled from transport)

Provider with Signed Documents

Document with embedded signature and delegation



Accepted and stored by all recipients regardless of AoR support

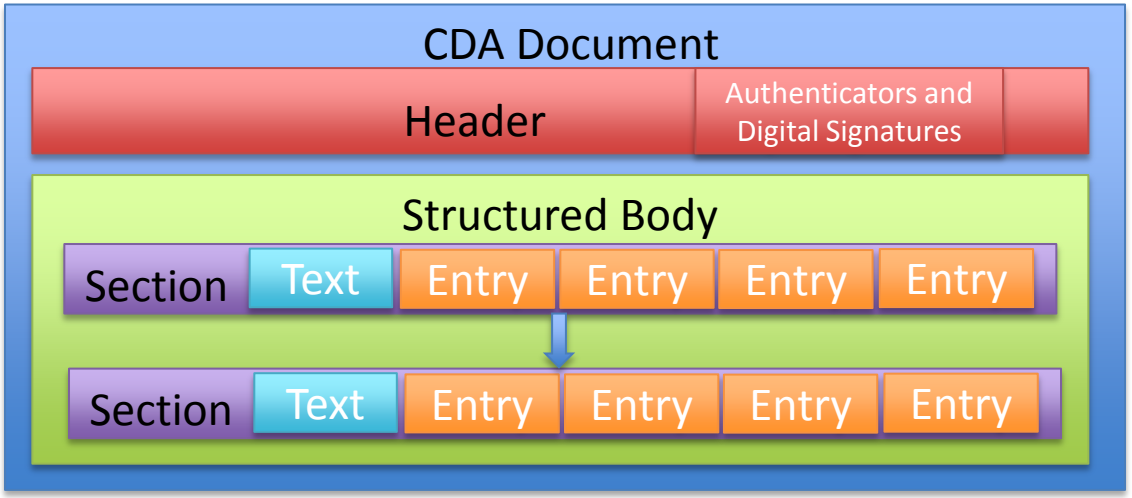
Document Delegation Signature

Signature and delegation only accepted by systems with AoR support
May drop only signature and delegation or error on entire transaction

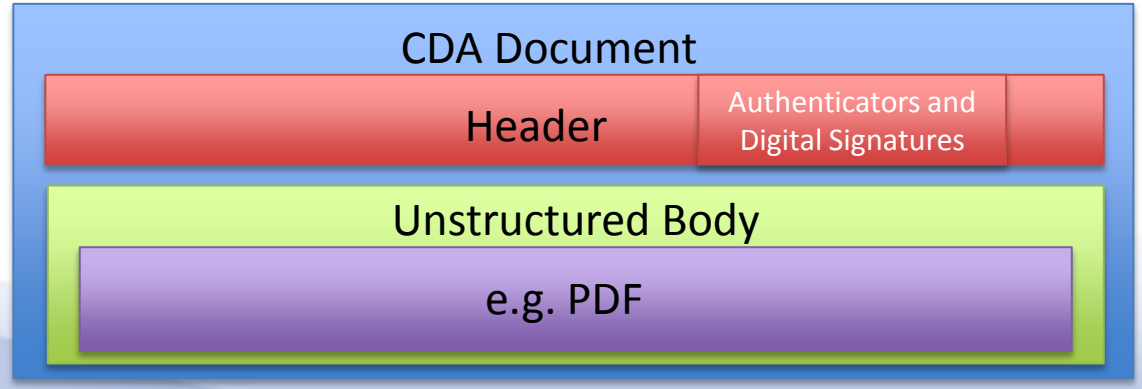
Signature on CDA

Solution: Add "signatureText" attribute to Participation occurrences for legalAuthenticaor and authenticator in the CDA Header to hold Digital Signature and Delegations of Rights Assertion artifacts -- exclude these Participation occurrences from the calculated digest

Structured Body

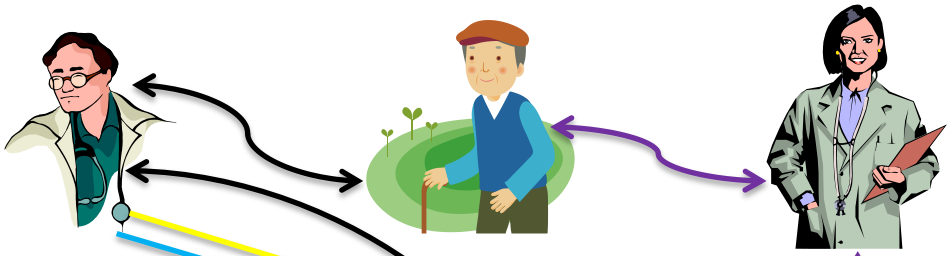


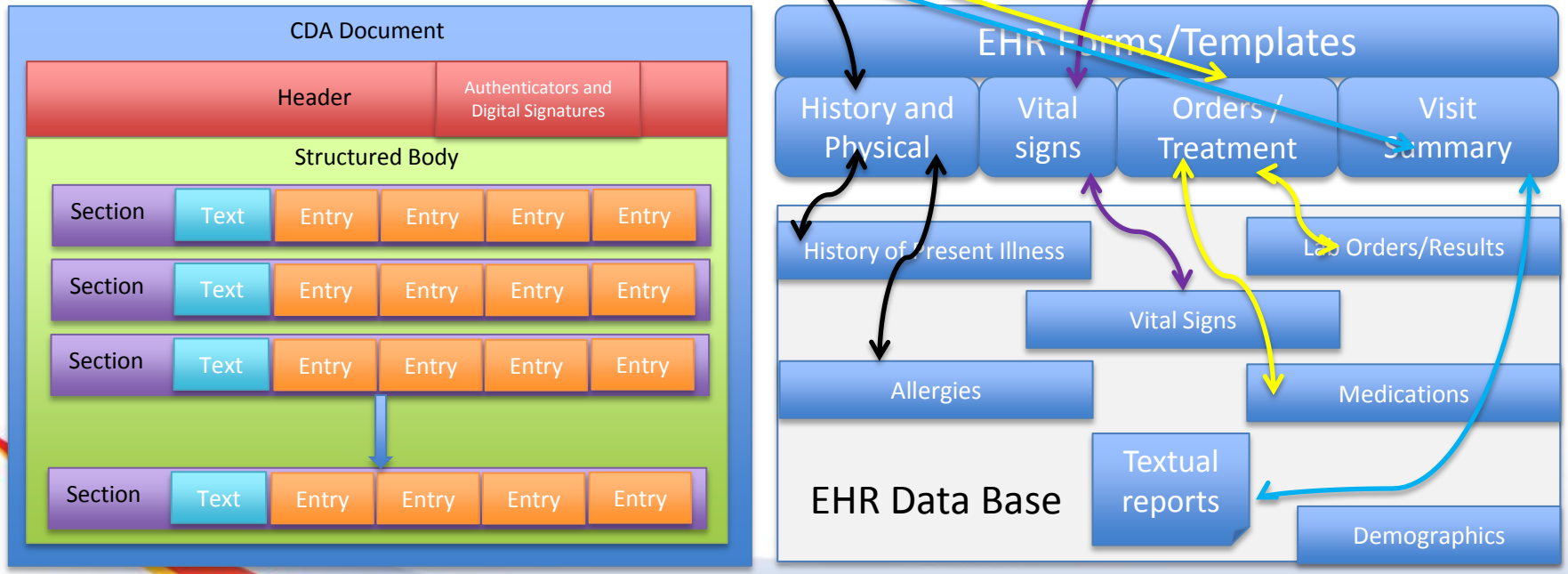
Unstructured Body



Document Encounter

Documentation collected via EHR forms and templates and stored in the EHR Database

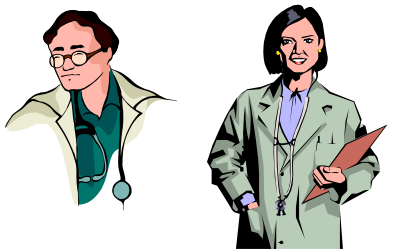


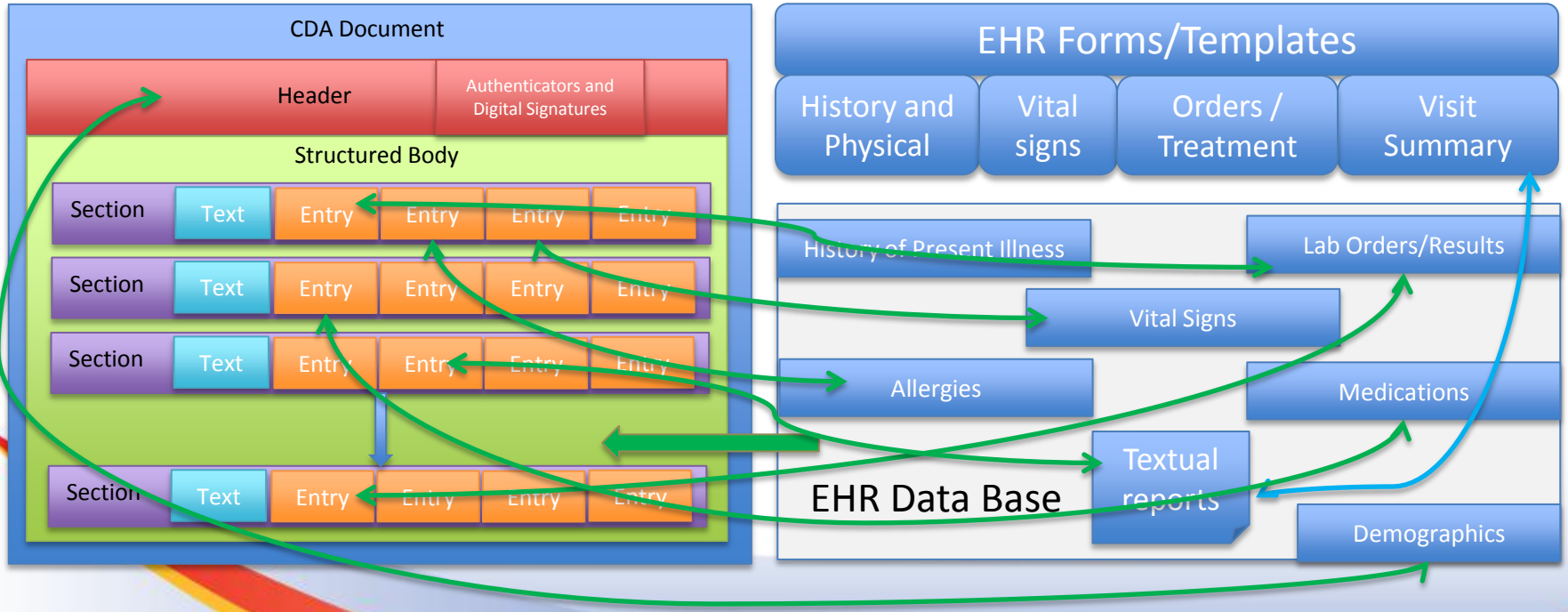


Create CDA

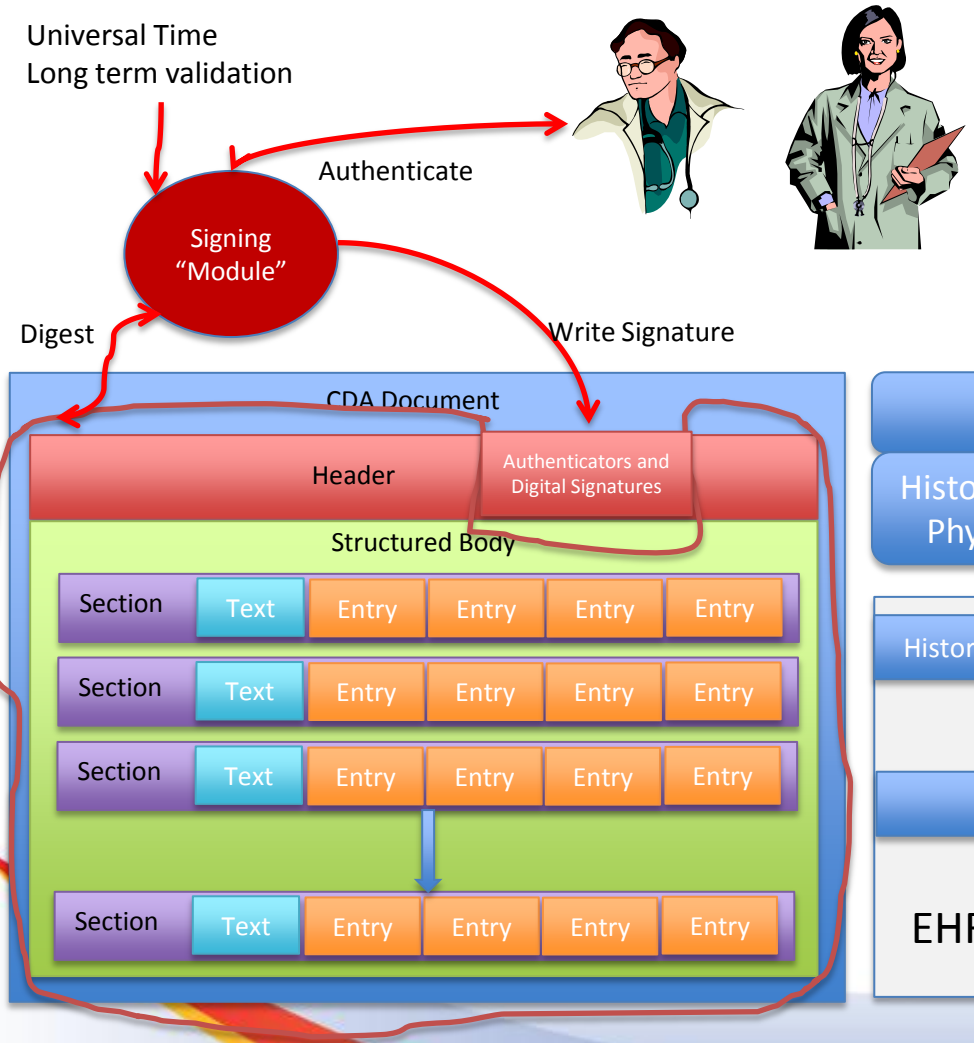
Prior to or at time of signing – create CDA

Create CDA
1) May be structured (e.g. Operative Note) or unstructured
2) CDA sections and entries are populated or use appropriate nullFlavor



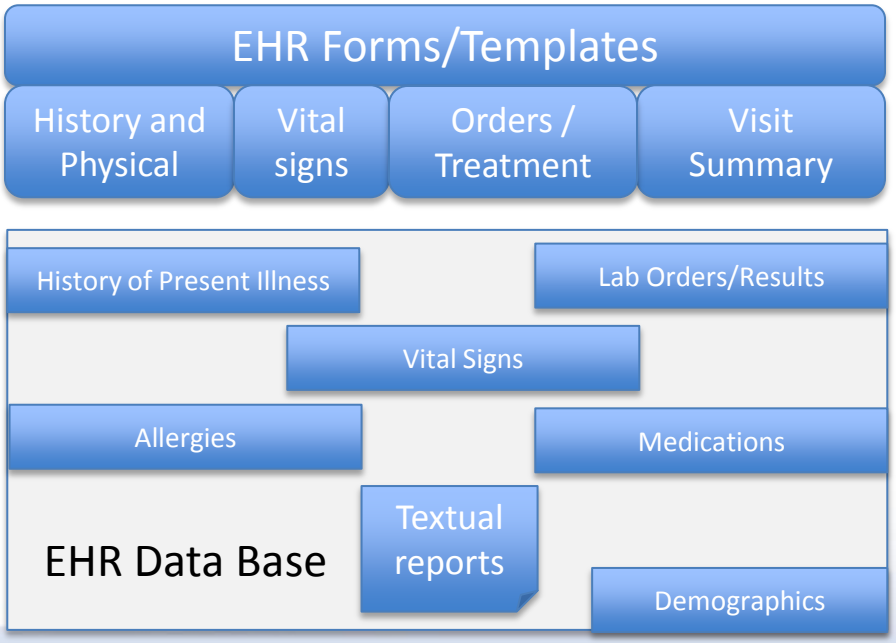


Sign CDA



Notes:

1) Signer may authenticate and then review/sign multiple documents at one session
2) Authentication via acceptable two factors -- something you know, something you hold, something you are (e.g. biometric), etc.



HL7 September Ballot Cycle

- Project Scope Statement for Digital Signature on C-CDA accepted
  - Primary Sponsor Work Group – Structured Documents
  - Co-sponsor Work Groups – Security, Attachments
  - Interested Parties – RMES
- For September 2013
  - May 19 – Project Scope (Done)
  - July 7 – Notification of Intent to Ballot (Done)
  - July 21 – Preview content due
  - July 28 – Reconciliation, Complete and Supporting Content
  - August 15 – Final Content Deadline
  - August 16 – Provisional Ballot Opening

Summary

esMD AoR identifies Best Practice for:

1) Establishing the identity of providers
   a) Identity Proofing of all participants (individual and organizations)
   b) Digital Credential Lifecycle management, including access to private keys,
   c) Digital Signatures Standards, and
   d) Delegation of Rights Standards
2) Addressing Author of Record requirements
3) Defining requirements for structured documentation that includes digital signatures for proof of provenance

CMS esMD and DEA Electronic Prescriptions for Controlled Substances (EPCS) Side-by-Side

(Responding to question posed by Wes Rishel at HITSC meeting)

DEA Electronic Prescriptions for Controlled Substances (EPCS)

DEA's rule, "Electronic Prescriptions for Controlled Substances" provides practitioners with the option of writing prescriptions for controlled substances electronically. The regulations also permit pharmacies to receive, dispense, and archive these electronic prescriptions. These regulations are an addition to, not a replacement of, the existing rules. The regulations provide pharmacies, hospitals, and practitioners with the ability to use modern technology for controlled substance prescriptions while maintaining the closed system of controls on controlled substances.

Side by Side Comparison (1 of 3)

Functions	DEA EPCS	CMS esMD
Prerequisite	DEA Registration (individual or employer DEA form 223) for each location authorized	NPI or alternate Provider ID for billing provider -- None for others (e.g. delegated entities)
	Delegate a Coordinator to manage DEA's digital certificate management for electronic ordering (Schedule I and II controlled substances). Digital certificate replaces for DEA 222	
Application Requirements	Application must have 3rd Party certification and certification audit required	Application certification and audit by 3rd Party are expected
	Delegation via power of attorney by a DEA registrant presented to a coordinator	Application must support delegation of rights (DoR)
	Verification of DEA form 223 for hospitals and qualified organizations (Government Agencies, Military and PHS)	Requirement to identity proof organizations that hold NPI or Alternative Payer IDs
Total number of individuals/organizations	Over 390,000 providers, hospitals, federal agencies, and other qualified organizations and approximately 91% of all pharmacies	Organizations, providers and support staff that may sign estimated at 5-6 million

Side by Side comparison (2 of 3)

Functions	DEA EPCS	CMS esMD
Certificate Type	Controlled Substance Ordering System (CSOS) certificates are appropriate for use with other applications requiring a Medium level of assurance or below, as defined by the Federal Bridge Certification Authority (FBCA).	FBCA Medium
Certificate issuance	Digital certificate issued to each location	Issued to individual or organization -- depending on software capability vendor may request one for each signing software application (not required)
	The CSOS CA shall be operated under the authority of the DEA Office of Diversion Control Policy Management Authority (PMA) as a subordinate CA to the DEA	Issued by any FBCA cross-certified CA or their subordinate CA (one level only)
Certificate renewal	Must renew whenever information on certificate changes or within 45 days of expiration	Intended to be renewed every two years -- no additional identify proofing required if certificate and NPI (if required) are still valid
	May renew twice, maximum of 6 years	
Certificate Verification	Validate the order	Validates credential
	Verify not expired	Verify not expired
	Check CRL for revocation	Check CRL for revocation
	Single trust anchor	Verify trust anchor
Additional Verification	Check extension or associated data file to determine if sender has authority	Validate signature artifacts and, if applicable, delegation of rights

Side by Side comparison (3 of 3)

Functions	DEA EPCS	CMS esMD
Digital Signature	Signed by EPCS application with associated prescriber data file attached or signed by prescriber	Signature on transactions (see use case 1 and 2) using DigSig
	May sign multiple prescriptions for one patient but must address one patient at a time	Signatures on document bundles using XAdES and DSG
		Signatures on documents using XAdES-X-L and SAML assertion (if required) in signatureText attribute of participant occurrences for legalAuthenticator and authenticator in header of C-CDA
Retention	Application orders and linked records for 2 years - FBCA retention records retain certificate information for minimum of 10 years 6 months	Depending on the type of medical record retention requirements- up to 21 years
		Transaction level signature (esMD use case 1/2 and AoR Level 1) does not require extended verification by the signer
Delegation of rights	Via power of attorney by a DEA registrant presented to a coordinator	Cryptographic assignment of right via signed XAdES assertion SAML -- validation may be required at time of delegation signing via XAdES

CMS Possible Transitions

- On an interim basis, esMD to accept identity proofing of DEA certificate holder as sufficient evidence to issue author of record (AoR) signing certificate -- assumes this meets CMS's requirement for in-person identity proofing (CSOS process and FBCA – medium assurance)
- Longer term, DEA accepts AoR Registration Authority process that will include validation of 1) org/individual ID 2) NPI / alternative ID 3) DEA license. Based on this, any FBCA cross-certified CA can issue the X.509 certificate with appropriate OIDs and alt ID information (e.g. direct address, NPI, Alt Payer ID, DEA number) and authentication credentials
- Common certification and audit process for signing applications over time

Appendix

Glossary

Term	DEA EPCS (1311.05)	CMS esMD
Authentication	The system must enable a recipient to positively verify the signer without direct communication with the signer and subsequently demonstrate to a third party, if needed, that the sender's identity was properly verified.	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive, transmit, or sign, specific categories of information
Nonrepudiation	The system must ensure that strong and substantial evidence is available to the recipient of the sender's identity, sufficient to prevent the sender from successfully denying having sent the data. This criterion includes the ability of a third party to verify the origin of the document.	Non-repudiation is a service that is used to provide assurance of the integrity and origin of data in such a way that the integrity and origin can be verified by a third party. This service prevents an entity from successfully denying involvement in a previous action
Message Integrity	The system must ensure that the recipient, or a third party, can determine whether the contents of the document have been altered during transmission or after receipt.	Data integrity is a property whereby data has not been altered in an unauthorized manner since it was created, transmitted or stored. Alteration includes the insertion, deletion and substitution of data