Author of Record Workgroup Charter

Challenge Statement

The Centers for Medicare and Medicaid Services (CMS) and other Health Plans/Payers need a standardized, implementable, machine-interoperable electronic solution to reduce the time, expense, and paper required in current manual processing of both medical documentation request letters and the relevant medical documentation exchanged between Healthcare Providers and Health Plans/Payers. The challenge at hand is to identify the requirements to verify the origin and authenticity of data submitted to CMS and other Health Plans/Payers for proper medical documentation processing.

Purpose Statement

The purpose of this workgroup is to investigate and develop operational solutions to address Author of Record, Identity Proofing, Digital Identity Management, Encryption (encryption only as it pertains to protecting the confidentiality of payloads containing Personal Health Information (PHI)), Digital Signatures, and Delegation of Rights within a healthcare context. The solution must support the digital signature and identity proofing requirements that allow healthcare Providers to register for and receive Electronic Medical Documentation Requests (eMDRs) from CMS and other Health Plans/Payers. This solution must also provide support for CMS and other Health Plans/Payers to accurately authenticate the author of documentation within the medical record, and trust the validity and authenticity of submitted medical documentation.

Value Statement

The value of the esMD Initiative will be to provide consensus-based use cases, functional requirements, standards references and implementation specifications representing combined input from a broad range of stakeholders, including CMS, commercial Health Plans/Payers, Providers, and vendors. This will promote a nationally standardized approach to medical document request letters, claims attachments, and the proof of validity and authorship of medical documentation.

Health Plans/Payers and Providers will benefit from this Initiative's recommendations and implementation guidance on Digital Signatures attached to patient information and electronic transactions. This will enable communications regarding the administrative claims processing between Providers and Health Plans/Payers to occur in a secure electronic format. Additional benefits include:

- Standardized formats, processes, and technology approaches
- Increased security of information exchange involving PHI
- Improved ability to identify and verify authorship of medical documentation for administrative purposes, clinical decision making, and care coordination
- Providing industry best practices for other domains within healthcare where PHI is exchanged

- Making the process of sending and receiving PHI less burdensome on Health Plans/Payers and Providers
- Identifying security breaches or tampering of information sent or received that are not always evident in the paper process
- Saving time, money and resources for CMS, Commercial Health Plans/Payers, and Providers
- Elimination of the paper process and its associated labor and error rate
- Improved timeliness results in improved accounts receivable cycle for Providers, so payments are received sooner
- Reduced improper payments
- Guidance and recommendations on EHR Certification criteria as it relates to document submission

Objective

The workgroup will conduct an environmental scan to understand what viable standards and practices are currently in place to support proof of authorship and digital signatures. With the knowledge obtained from the environmental scan, the workgroup will discuss and document requirements relevant to CMS and other Health Plans/Payers regarding signatures for submitted medical documentation. This will include vendors' input with regards to what EHR systems can realistically support, and also include input from healthcare Providers to ensure the solution is not overly burdensome to healthcare Providers and healthcare Provider organizations. Additionally, the Provider Profiles Authentication and Structured Content/Secure Transport of the eMDR use cases will be supported in this workgroup by the following:

- Cryptographic (or equivalent) verification of all participants (Providers, Intermediaries, and Health Plans/Payers)
- Prevention of tampering
- Encryption of Patient Health Information (PHI) contained in the eMDR

This workgroup will define the Use Case and Functional Requirements, Analyze and Harmonize standards relevant to author-level signatures that support pilot implementations of the solutions, while taking into account the two Use Cases developed as part of the Standards and Interoperability Framework's (S&I) esMD initiative. Business requirements and standards will focus on the needs of CMS and the CMS Review Contractors, while also considering options to enable re-use by other Health Plans/Payers.

Workgroup Scope

This workgroup will investigate and recommend solutions on various levels of Author of Record needs:

- AoR Level 1 – Digital signature on aggregated documents (Document Bundle - to be defined during Use Case development)
- AoR Level 2 – Digital signature on an individual document

- AoR Level 3 – Digital signature to allow traceability of individual contributions to a document

The scope of effort includes the five focus areas for the Author of Record Workgroup identified during the initial pre-discovery efforts: 1) Identity Proofing, 2) Digital Identity Management, 3) Digital Signatures, 4) Delegation of Rights, and 5) Encryption (encryption only as it pertains to protecting the confidentiality of payloads containing PHI).

The workgroup will focus on Identity Proofing, Digital Identity Management and Digital Signatures for NIST E-Authentication SP 800-63 Level 3 Authentication.

In Scope

AoR Level 1

- Solutions to support the signature artifacts identified for esMD Use Case 1 and 2
- Solutions for digital signatures are intended for the Document Bundle level, to attest to the validity and authenticity of the patient information within the Document Bundle (or other relevant medical documentation) - and will be agnostic regarding format of the document content in the Document Bundle.
- This workgroup may provide suggestions to CMS regarding policies and regulations needed to support the recommended solution
- Digital Identity Management
- Encryption (encryption only as it pertains to protecting the confidentiality of payloads containing PHI)
- Delegation of Rights function as related to the registration transaction or the Document Bundle-level signature
- Privacy, Security and Delegation of Rights requirements between the **Provider Entity** (which could be Provider, Health System, or Agent/HIH) and **Payer Entity** (which could be Payer, Payer Contractor, or someone else on their behalf)

AoR Level 2

TBD

AoR Level 3

TBD

Out of Scope

AoR Level 1

- Digital signature on an individual document and other items to be defined
- Digital signature to allow traceability of individual contributions to a document and other items to be defined

AoR Level 2

TBD

AoR Level 3

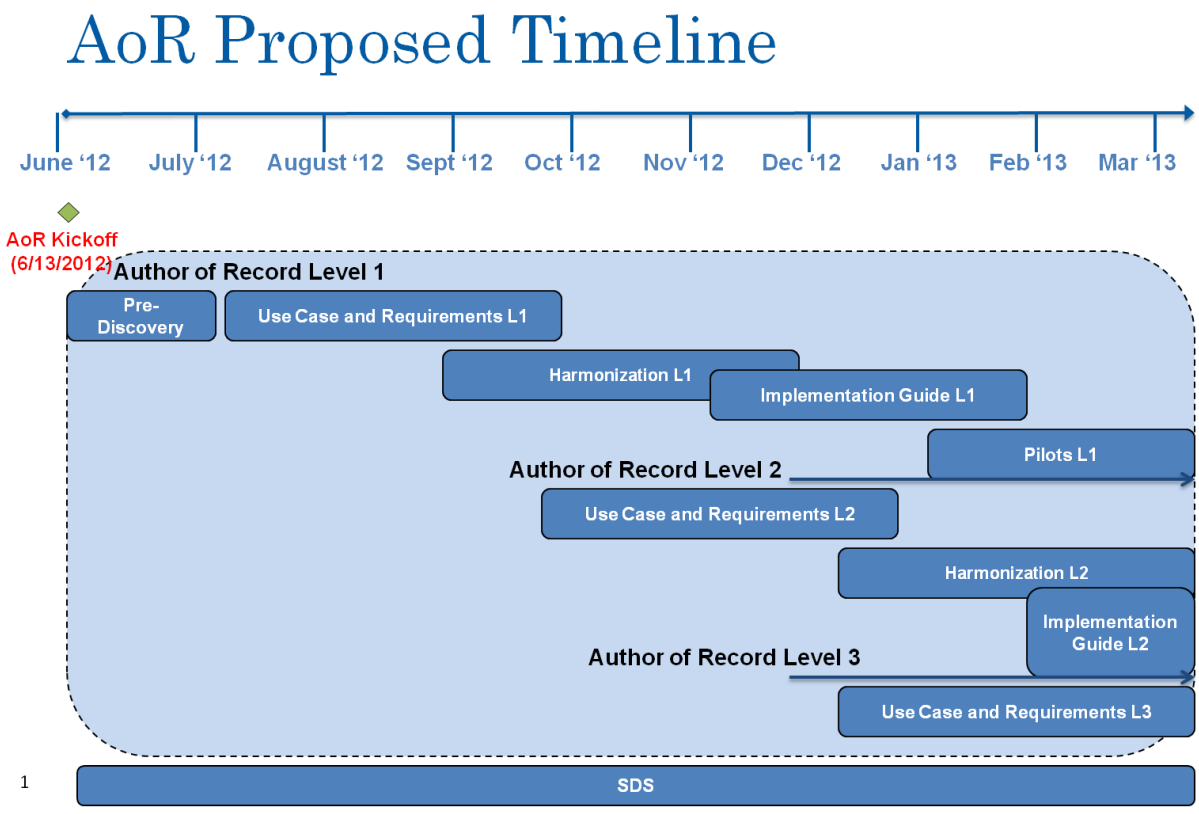
TBD

Targeted Goal & Outcome

- **Goal –** Achieve highest level of Provider authentication for AoR using available technology
- **Outcome –**
  - Satisfy Statute requirements for AoR
  - Medicare error rate reduction to meet CMS requirements set by Congress
  - Reduction in improper payment

Timeline

The work group will use an incremental approach for addressing AoR Level 2 and Level 3 that will build on the foundation of AoR Level 1, and will coordinate the Discovery, Implementation and Pilot phases for completing each successive AoR level, per the proposed timeline below.



Relevant Policies

- CMS Internet Only Manuals (IOM)
- CMS National Coverage Determination (NCD) / CMS Local Coverage Determination (LCD)
- Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy and Security Rules
- Applicable SSA Statute
- Applicable State regulations and laws
- Applicable Federal regulations and laws

Potential Standards for Consideration

General (multiple categories)

- CAQH CORE Connectivity 270 Rule v2.2.0 (Transport, Envelope, and Security)
- NwHIN X12 Document Submission Specification
- NwHIN-Exchange specifications (IHE: XDS,XCA,XDM,XDR,XUA,XCPD,ATNA)
- HPD+ (Healthcare Provider Directory with S&I Framework PD extension)

Transport

- DIRECT Project SMTP/SMIME
- NwHIN Exchange (Connect)
- SOAP (Simple Object Access Protocol)
- REST (Representational State Transfer)

Message/Content

- X12 274 (Healthcare Provider Information)
- X12 277 Request for Additional Documentation
- X12 275 Additional Information to Support a Healthcare Claim or Encounter
- IHE XD* (XDM,XDS, XDR)
- HL7 CDA r2 (Including Claims Attachment Workgroup work-product)
- HITSP CCD (multiple standards)

Security

- Security Assertion Markup Language (SAML)
- Cross-Enterprise User Assertion (XUA)/Enterprise User Authentication (EUA)
- Records Management and Evidentiary Support (RM-ES) Functional Profile
- IHE Digital Signatures Profile (DSG)
- NIST SP 800-63
- X.509 v3

Potential Stakeholders

Standards Groups (supply/support/extend relevant standards)

- Health Level Seven International (HL7)
- Integrating the Healthcare Enterprise (IHE)
- Direct
- National Institute of Standards and Technology (NIST)
- National Strategy for Trusted Identities in Cyberspace (NSTIC)
- Federal Bridge/ Federal Public Key Infrastructure (FPKI)
- National Committee on Vital and Health Statistics (NCVHS)
- National Council for Prescription Drug Programs (NCPDP)
- ASC X12
- CAQH CORE

Exchange Partners (Create / Consume/ Utilize relevant transactions, payloads and specified standards)

- Health Plans/Payers – CMS, Commercial Payers
- Healthcare Providers and Provider Organizations
- Drug Enforcement Agency (DEA)
- Social Security Administration (SSA)
- Department of Defense
- Veterans Affairs (VA)
- TRICARE
- Substance Abuse and Mental Health Services Administration (SAMHSA)

Policy Organizations (create relevant policies)

- Federal Government
- States

Service Providers (provide services to facilitate transactions and information exchange)

- Health Information Exchanges (HIE)
- Registration Authorities/Identity Verifiers
- Certificate Authorities/Credential Providers
- Electronic Health Record (EHR) Vendors
- Health Information Handlers (HIH)
- Healthcare Provider Directory Services
- Other Insurance, Healthcare, Intermediaries, Third Party Administrators (TPAs), Contractors, and Representatives

Note - A complete list of stakeholders will be developed as part of the Use Case

Dependencies

- National standards for identity, credentials, and transaction/document authentication Industry technology and expertise
- Current standards and policies set by CMS and Commercial Health Plans/Payers
- Certificate Authorities / Registration Authorities ("Trust Anchors")
- EHR Technologies
- Payer and contractor technologies
- State regulations and laws
- Federal regulations and laws

Relevance outside of esMD

- Drug Enforcement Administration (DEA) – DEA has implemented solutions for similar requirements, and we will seek their input and participation to evaluate if their solutions and lessons learned can be re-used within the scope of this workgroup
- SSA has implemented solutions for similar requirements, and we will seek their input and participation to evaluate if their solutions and lessons learned can be re-used within the scope of this workgroup
- Health Plans/Payers – They will benefit from a standardized signature process to confirm validity and authenticity of the submitted medical documentation
- Providers / Provider Organization – It is expected that Providers will be able to implement and use this solution, in order to support medical documentation submission, and potentially other transactions requiring signatures. This could enable a common approach by Providers and therefore may enhance the business justification for enabling the solution.
- Vendors
- Patients – They would benefit from the standardized signature process to enhance validity, trust, and privacy of health information, in addition to prevention of identity theft via secure transport of patient information.

Potential Risks

- Ensuring secure, trustable communications between Health Plans/Payers and Providers
- Compliance with FISMA in sending PHI from Health Plans/Payers to Providers
- Establishing policy regarding signatures or proof of content authorship within structured content
- Identifying implementable solutions to prove authorship that minimize burden to both Providers and Health Plans/Payers

- Potential Related Workgroups esMD Use Cases developed within the S&I Framework
    - Use Case1 - Provider Registration with a Payer to receive electronic medical documentation requests (eMDRs) from Payer to Provider

  - Use Case 2 - Secure Transportation and Structured Content of eMDRs
- Input from S&I initiatives that have similar needs to those identified for esMD
- S&I Modular Specifications workgroup (esMD Phase I)
- External to S&I (including): HL7 Records Management & Evidentiary Support (RM-ES), DEA, SSA, IHE, Federal Bridge, Federal Identity, Credential, and Access Management (FICAM), CMS, Electronic Healthcare Network Accreditation Commission (EHNAC)