Trusted Identity of Physicians in Cyberspace Hearing

Tony Trenkle
Chief Information Officer &
Director, Office of Information Services
Centers for Medicare & Medicaid Services

July 11, 2012
Drivers CMS Faces For Healthcare Provider Credentialing and Validation

- Exchange of healthcare information among healthcare providers
- Healthcare provider access to CMS systems to get enroll in Medicare and other programs.
- Access to healthcare data for analytics in support of quality and cost measurements
- Access to decision support data to deliver optimal care
Provider Sources and Destinations

• CMS healthcare providers are also served by other Federal Government Agencies, States, and the Private Sector:
  – Social Security Administration
  – Department of Veterans Affairs
  – Department of Justice, Drug Enforcement Administration
  – TRICARE
  – State Medical Boards
  – Health Plans

• CMS healthcare providers require access to:
  – Health Information Exchanges
  – Accountable Care Organizations (ACO)
  – Many CMS online applications

• Unique Credentials for each combination cannot support the future (expensive, cumbersome, etc.)
 CMS is tracking NSTIC AND FICAM closely

CMS believes its role is a “relying party” in the identity ecosystem defined by NSTIC

In partnership with other Government Agencies and the Office of National Coordinator (ONC), CMS has actively participated in the Federal Cloud Credential Exchange (FCCX) workgroup

NSTIC AND FICAM principles have been baked into the CMS Enterprise Identity Management (EIDM) project that will integrate access controls, authorization and federation for CMS systems that service healthcare providers

Results from risk assessments conducted on CMS online systems show that many are rated at NIST Level of Assurance (LOA) 3

CMS intends to leverage FICAM certified Credential Service Providers (CSP) for the more robust credentialing processes that are required by LOA3
CMS EIDM

- EIDM will serve the identity management needs of new systems and consolidate legacy systems
- EIDM will allow for the use of remote identity proofing services, queries to outside-agency provider sources or cloud-based, certified CSPs
- EIDM may also act as a translation layer between CMS online systems and CSPs
- Goal is to allow healthcare providers to use one credential to access multiple applications
- Use cases include getting a National Provider Identifier (NPI), enrolling in Medicare and getting quality reports.
EIDM Implementation Schedule

WEB SERVICES: Remote Proofing; Registration; Authorization; ID Lifecycle & Access Mgmt
*MULTI FACTOR AUTH
*FEDERATION
*PORTAL INTEGRATION