augmented identity

IDEMIA USA Response to:

Strategy on Reducing Regulatory and Administrative Burden Relating to the Use of Health IT and EHRs

DRAFT FOR PUBLIC COMMENT

As Required by the 21st Century Cures Act
Public Law 114-255, Section 4001

Submitted by:
Steve Miu, Chief Mobile Strategist
Direct: 978-215-2400
Email: steve.miu@us.idemia.com

IDEMIA USA (Formerly, Morphotrust USA)
296 Concord Road, Suite 300
Billerica, Massachusetts 01821
www.IDEMIA.com

IDEMIA

TABLE OF CONTENTS

IDEMIA Comment – Using Identity as a Means to Ease Administrative Burden 3

IDEMIA Comment to the Message Prologues of Mr. Azar, Dr. Rucker, and Mr. Verma 5

IDEMIA Comment to Strategies and Recommendations 6

Issues and Challenges 9

Clinical Documentation 10

Health IT Usability and the User Experience 11

EHR Reporting 12

About IDEMIA and Our Expertise with "Augmented Identity" 13

IDEMIA COMMENT – USING IDENTITY AS A MEANS TO EASE ADMINISTRATIVE BURDEN

Throughout the ONC-authored draft for public comment (Strategy on Reducing Regulatory and Administrative Burden Relating to the Use of Health IT and EHRs), "burden" is implied to be present and to be minimized at the provider/point of service. The committee fairly assumes that technology and technology integrations will catch up – permitting data interoperability between disparate EHRs – and that operating protocols around participants of the TEFCA framework will be resolved.

However, has the authoring committee considered why "burden" even exists? Of course, there are compliance reasons, audit requirements, and "good business" reasons that have been propagated over several decades. But when one peels away these procedural justifications, at its essence, burden exists because of a lack of *accountability* within the electronic realm. This was an unintended consequence of the shift to electronic health records in the 1980s. As health records moved from paper to electronic, expectations of faster data exchange yielded to a paradigm biased towards data protection because data administrators were now unable to control the data flow, nor hold accountable the transacting parties or confirm their reasons for the data request. The size and magnitude of data breaches moved from a rogue office worker viewing an individual's medical file without permission or need, to highly visible and mass theft of millions of individual data records, like the Anthem Blue Cross breach in 2015. As late as July 2018, HIPAA Journal reports that there were 33 breaches in the month, with another 2.3M records exposed.[1] The root cause in both cases are the same: no verification of the individual gaining access to the files, with simple reliance on a username and password to gain "legitimate" access to the network.

Accountability should be highlighted within TEFCA by the ONC, and should be defined as the ability to identify the unique transacting parties and verify their **identity** – that they are who they say they are. Technology exists now to ensure that **identity verification** can be integrated into key points in the workflow, seamlessly in the day-to-day activities such as patients asserting their identity, administrators handling and requesting data, and patient providers creating treatment records.

Accountability is *not* block chain. It is *not* AES 256-bit encryption. It is *not* SSL/TLS networking. Security, encryption, and privacy are of course important in creating a viable ecosystem, but **identity** is the final piece that ensures the overall **trustworthiness** of the entire value creation stack.

At the ONC annual meeting, there was no mention of being able to identify or authenticate parties participating in TEFCA. In a post-plenary conversation with Dr. Rucker, he stated, "that the identity problem would work itself out". IDEMIA disagrees with this statement. TEFCA and the 21st Century Cures Act offer the committee, the states, and the entire industry the unique opportunity to define minimum requirements for asserting identity and

[1] https://www.hipaajournal.com/july-2018-healthcare-data-breach-report/

methods at all phases of medical services provisioning, medical records facilitation, and insurance payments.

As experts in identity – with driver's license contracts in 37 states; passport card contracts with the Department of State; Common-Access-Card contracts with all branches of the military; and NIST-validated biometrics contracts with intelligence agencies, federal law enforcement agencies, and 50 states' law enforcement; and the nation's **first** state contracts for mobile driver's license and purely electronic ID credential for online tax return submissions – we urge the ONC to take advantage of its unique positioning and **complete** the policy steps necessary to ensure that the TEFCA operating environment and its participants contribute to a **trusted ecosystem** where **identity** is used to reduce the overall day-to-day burden for everyone involved.

IDEMIA COMMENT TO THE MESSAGE PROLOGUES OF MR. AZAR, DR. RUCKER, AND MR. VERMA

In the published prologues, the focus of TEFCA is on reducing costs through electronic data interoperability. Within government programs, the size and scale as envisioned is truly bold and novel. It is attainable through technology and the proper incentives at the commercial level. However, this raises the concern around unintended consequences, and whether we are merely shifting the cost of healthcare away from data interchange to data accessibility. That is, as communication and exchange protocols standardize and evolve into open-standard APIs, how do we ensure that parties using these APIs are in fact eligible to do so, and (conditionally) authorized to do so? How do we ensure a technological solution is trustworthy and thus robust enough to be long-lived?

We "burden" our clinicians with multiple data systems to collect their treatment notes – and with multiple log-in profiles to access those systems – to the point that a 10-minute appointment with a Primary Care Physician (PCP) may find 2 to 3 minutes of that time waiting for the PCP to properly log into each required system to take notes and observations. This is because in the competitive nature of EHR systems, the providers of these systems are not under any obligation or incentive to make the systems talk to each other. Some innovative third parties have created such intermediating systems to help ease the burden associated with logging into each system by creating a login "layer" emulating LDAP (lightweight directory access protocol) that can be used in conjunction with a directory service to provide access to a desired system. However, neither LDAP nor directory services filter or challenge the individual in the directory to assert their identity. As a result, even with such technical implementations, it is possible and in fact easy to spoof. Dongles or keycards may provide some accountability confidence when accessing such systems, assuming (1) the providers have had their identities properly vetted at time of issuance of the token; and (2) the token is disabled in the event the token is lost.

Still, in the case of Medicare recipients, it is unreasonable to assume that CMS will issue more than 53 million new cards or tokens to the population of eligible recipients such that they can assert their identity when they arrive at a provider office. And it is unfathomable that CMS would consider the creation of yet another central database of "identity tokens."

As a result, IDEMIA believes that CMS/ONC/TEFCA should echo the best practices as published by the Department of Commerce/NIST when it comes to identity and identity management – that is, to recommend the use of multi-modal biometrics to establish identity among all individual participants of the ecosystem. Technology now exists to easily "rank" identity thresholds when considering "something you are" (i.e., biometric); with "something you have" (i.e., a driver's license, ID card, or physical token); with "something you know" (i.e., password, PIN); with "something you have established" (i.e., a medical history of treatments).

Identity along with interoperability will be the key to TEFCA's long-term effectiveness, and the ONC's legacy.

IDEMIA COMMENT TO STRATEGIES AND RECOMMENDATIONS

P14. CLINICAL DOCUMENTATION STRATEGIES

- *Reduce regulatory burden around documentation requirements for patient visits.*
- *Continue to partner with clinical stakeholders to encourage adoption of best practices related to documentation requirements.*
- *Leverage health IT to standardize data and processes around ordering services and related priority authorization processes.*

IDEMIA – The clinical experience and the promise to help others is arguably the most important piece of the healthcare system – it is the forefront of the doctor-patient relationship. And it is true that there are too many disparate systems, with incompatible means for providers to access those systems.

Documentation and compliance are obviously important in today's world, but the real burden in the clinical sense is requiring the healthcare professional to retain and assert their identity to several EHR systems, sometimes simultaneously, sometimes facing automatic log-out after computer inactivity is sensed.

Data and process standardization through expanded acceptance of HL7 will not be as effective as desired, largely because HL7 does not address the tactical authorization activities – namely identity. Continuing the prior train of thought, healthcare IT as an industry has not adopted the NIST-published definition of identity – henceforth, that username and password are not verifiable back to the credential-assigned individual, and hence a very weak identity attribute.

IDEMIA believes that the solution is to suggest hospital groups and other medical partners promote the use of a single-access technology that can be tied to a directory/authorization service and the LDAP communication protocol.

P15. HEATH IT USABILITY STRATEGIES

- *Improve usability through better alignment of EHRs with clinical workflow; improve decision making and documentation tools.*
- *Promote user interface optimization in health IT that will improve the efficiency, expertise, and end user satisfaction.*
- *Promote harmonization surrounding clinical content contained in health IT to reduce burden.*

- *Improve health IT usability by promoting the importance of implementation decisions for clinician efficiency, satisfaction and lowered burden.*

IDEMIA – Since "burden" has been described herein specifically as the provider's interaction with the systems necessary for documenting patient treatments, "usability" is the key area for improvement.

When considering the large number of disparate EHR's and Clinical Decision Support (CDS) tools in use today, along with their unique deployment policies and methods in operation with their employers, this strategy may be the most difficult to implement without more specificity from the ONC and RCE.

While each healthcare provider may have different corporate and state licensing requirements dictating the types of data to keep track of, the end-user (provider) workflow that can be made easier and more efficient is the specific use of biometrics to perform mundane but extremely important functions like logging in and authorizing transactions. Here, any number of technical solutions exist as augments to the traditional LDAP-standardized single sign-on user management systems. These solutions free the provider from distracting the doctor-patient interaction by remembering usernames/password combinations, carrying multiple system access tokens/dongles/keycards, recalling access PIN numbers, or, in extreme cases, introducing avoidable bacteria into the clinical examination room by using their mobile phones as an SMS text-back device.

To maintain true **identity** accountability, IDEMIA suggests that the ONC/RCE consider the work that NIST and the National Strategy for Trusted Identities in Cyberspace (NSTIC) have already invested in studying and defining best practices associated with identity, and electronic applications thereof. For instance, technology and methods (patents) exist now for licensing that can verify identity all the way back to the proofing/vetting event when a physical, government-issued identity credential was issued – not a hospital badge, not an insurance card, not a credit card, or any other types of physical credentials that are commonly used as forms of identity but have no verifiable tie-back to the initial identity proofing event.

P17. EHR REPORTING STRATEGIES

- *Address Program Reporting and participation burdens by simplifying program requirements and incentivizing new approaches that are easier and provide better value to clinicians.*
- *Leverage Health IT functionality to reduce administrative and financial burdens associated with quality and EHR reporting programs.*
- *Improve the value and usability of electronic clinical quality measures while decreasing healthcare provider burden.*

P18. PUBLIC HEALTH REPORTING STRATEGIES

- *Increase adoption of electronic prescribing of controlled substances (EPCS) and retrieval of medication history from state PDMP through improved integration of health IT into provider workflow.*
- *Inventory reporting requirements for federal healthcare and public health programs that rely on EHR data to reduce collection and reporting burden on clinicians. Focus on harmonizing requirements across federally funded programs that impact a critical mass of healthcare providers.*

IDEMIA – Considered traditionally, “reporting” is a tool for management and compliance purposes, not at clinical provider activity; that is, “reporting” is not “patient history.” While we agree with the spirit of these strategies, it is unclear as to their value to clinicians.

Value to back-office, payments administrators, and public health policy-makers, however, is clear. As such, with access to the entire patient case files, the same concern around identity and identity verification exist – thereby suggesting that the ONC and RCE consider the best practices published by NIST and NSTIC, which are currently in use in other industries where “identity matters.”

ISSUES AND CHALLENGES

P23. CLINICAL DOCUMENTATION

- *Documentation filed satisfies administrative and billing.*

P30. HEALTH IT USABILITY AND UX

- *User-centered design.*

P34. CONFIGURATION AND IMPLEMENTATION OF EHR SYSTEMS

- *User Authentication.*

P36. EHR REPORTING

- *P38 – 15.1 hours/physician/week entering info into EHR.*

IDEMIA – These issues and challenges are specific low-hanging fruit that a biometrically enabled identity solution can directly solve.

First, in regards to documentation required to satisfy administration and billing, an auditable provider identity should be asserted when accessing any system. A NIST-compliant, multi-factor identity enrollment can be first completed by the provider when joining the healthcare practice. Their “verifiable identity” is then converted to an auditable but non-PII dependent electronic representation. Similar to LDAP, these “identities” are then registered into a policy-server, which defines the systems and the fields that they have access to and are required to navigate for any purpose – administrative, billing, or TEFCA.

Keeping clinical efficiency in mind, the provider-centric UX can be such that mouse clicks and screen scrolling are optional. Not needing to fumble for physical cards or memorized usernames/passwords/PINs (note, these are **not** identity credentials), navigating EHR reporting and documentation screens can be reduced, which provides more clinical patient time.

CLINICAL DOCUMENTATION

P46. STRATEGY 1

- *Recommendation 1: reduce overall regulatory burden around documentation of patient encounters.*

P49. STRATEGY 3

- *Recommendation 2: Support automation of ordering and prior authorization processes for medical services and equipment through adoption of standardized templates, data elements and realtime standards-based electronic transactions between providers, suppliers and payers.*

IDEMIA – As before, we wish to emphasize that automation without accountability is a shortcoming that will have the opposite effect as the goals of TEFCA – ultimately leading to increased burden to participants in the ecosystem, as regulators try to solve the unintended consequences of standardization and automation. The only way to reduce burden is to proactively address these concerns, and introduce accountability into the day-to-day operating paradigms of all the participants in the ecosystem.

Identity must be considered at the same time as the standardization activities, and the design of those standards. Privacy, encryption, security – all are important, but the ecosystem **must** include **identity** if the ecosystem is to be trusted, and the transactions auditable.

HEALTH IT USABILITY AND THE USER EXPERIENCE

P54. STRATEGY 3

- *Recommendation 3: Improve internal consistency within health IT products.*

P57. STRATEGY 4

- *Recommendation 3:Optimize system log-on for end users to reduce burden.*

IDEMIA – Again, we believe improving the user experience will have the biggest impact in terms of reducing burden.

But the proprietary nature of most legacy EHR databases make internal consistency difficult, requiring all incumbent systems to create middleware to help bridge the communications and the compatibility of data fields. Once this has been accomplished, however, we must ensure that the entire transaction is performed within a trustworthy framework and infrastructure.

We presume HIPAA and the privacy expected when dealing with patient data at rest. We presume the communication lines that this data is communicated over will be secure. And just in case, we will encrypt the data we are sharing. However, the theme along this overall response has been about identity" and "accountability. How will the identity of the individual parties be asserted, verified, and trusted?

If multiple biometric factors are utilized, then the same solution to trust transaction requests could be used for basic system login.

We ask the ONC not to diminish the important role that identity can play within the TEFCA framework.

EHR REPORTING

P58. STRATEGY 1

- *Recommendation 2: Incentivize innovative uses of health IT and interoperability that reduce reporting burdens and provide greater value to physicians.*

P62. STRATEGY 2

- *Recommendation 3: Implement an open API approach to HHS electronic administrative systems to promote integration with existing health IT products.*

IDEMIA – We believe care needs to be extended as to not rush a published policy or incentives.

While this is all needed and well-intentioned, we believe the ONC/RCE will be hard-pressed to implement the standard by which all databases can be harmonized, and specify which procedural changes will allow providers to remain compliant with both network participants and regulatory/HIPAA requirements, while reducing burden.

While TEFCA seeks to reduce healthcare costs and improve end-patient quality of care, the overall burden as described within this ONC draft is largely clinical, due to poor compatibility among systems, capturing relevant medical notes and diagnosis – as driven by proprietary database implementations. Standardizing these fields requires not just harmonized APIs, but also normalized data fields and character input limitations, which may affect the way providers enter medical “shorthand.”

Nevertheless, in the end, systems access accountability must be offered. Verifiable identity as input as part of the provider UX should be key to acceptance. How will caregivers and providers access the system in order to effectively document the clinical experiences with their patients? Is there a way by which these trained professionals can spend their time and focus on dealing with the patient experience, as opposed to dealing with the system necessary for regulation and compliance? All of this would provide greater value to the healthcare providers and physicians.

ABOUT IDEMIA AND OUR EXPERTISE WITH "AUGMENTED IDENTITY"

IDEMIA USA is the Identity Company, including 3,000 hardworking U.S. citizens focused on delivering solutions and services to commercial businesses and government agencies that enable trusted transactions – in-person or online – wherever identity matters. From individual enrollments, to secure credentials, to document authentication, to biometric/data matching against trusted sources; IDEMIA USA's offerings verify that individuals are who they claim to be before engaging services or exercising privileges. Our solutions produce 80 percent of U.S. driver licenses and IDs – the most trusted identity document in the U.S; 1.2B cards with SIM chips and over 700M financial payment cards; among 1,500 global financial institutions, 500 mobile phone operators, and all major industrial OEMs.

IDEMIA USA has a 40-year history in providing identity and identity credentials to state driver licensing agencies and biometric matching systems to law enforcement at the federal, state, and local levels. Whether issuing the **first** driver's license with an embedded portrait, to the latest in mobile phone-based driver license, to finger-face and iris biometric systems used to catch the Boston Marathon bombers, the company has had a long track record of innovative and effective identity-based policies and products.

IDEMIA USA (as our predecessor companies: MorphoTrust USA, MorphoTrak, and Oberthur Technologies) is a long-time supplier of identity and credentialing systems and solutions to multiple agencies of the U.S. Government and branches of the military. Contracts range from the Department of State-issued U.S. Passport card, to the U.S. military branch common-access card (CAC), to leading biometric matching systems used by the intelligence and law enforcement communities.

To support ongoing federal programs, IDEMIA USA operates the IdentoGO® federal enrollment centers, accounting for over 1,400 locations throughout the U.S., performing fingerprinting and other identity-related services for state governments and federal programs such as the Transportation Workers Identification Credential (TWIC), Hazardous Materials Endorsement Threat Assessment Program (HAZMAT), and the TSA PreCheck program, having enrolled over 7M customers to date.

IDEMIA USA biometric algorithms are commonly ranked #1 or #2 in regular testing by NIST, and many of our multi-modal identity-assertion solutions and methodologies have been deemed "best in class" and recipients of grant funding from the NSTIC.

Keying off all these innovations, and ensuring high-confidence identity assurance in future use cases, IDEMIA USA was awarded the nation's first contract to deliver a mobile-phone driver license credential by the State of Iowa; and the first contract to deliver an all-electronic digital credential to be used by resident online tax submissions by the State of Alabama.