OFFICE OF THE NATIONAL COORDINATOR

HEARING ON

TRUSTED IDENTITY OF PHYSICIANS IN CYBERSPACE

JULY 11, 2012

PREPARED REMARKS
OF
SURESCRIPTS, LLC

The following prepared testimony is submitted by Surescripts, LLC to the Office of the National Coordinator and the Health IT Policy Committee's Privacy and Security Tiger Team and the Health IT Standards Committee's Privacy and Security Workgroup in connection with a hearing on Trusted Identity of Physicians in Cyberspace.

Introduction – About Surescripts

The Surescripts network supports the most comprehensive ecosystem of health care organizations nationwide. Pharmacies, payers, pharmacy benefit managers, physicians, hospitals, health information exchanges, and health technology firms rely on Surescripts to more easily and securely share health information. Guided by the principles of neutrality, transparency, physician and patient choice, open standards, collaboration and privacy, Surescripts operates the nation's largest health information network. By providing information for routine, recurring and emergency care, Surescripts is committed to saving lives, improving efficiency and reducing the cost of health care for all.

The Surescripts e-prescribing network connects approximately 390,000 prescribers, 57,000 community pharmacies, six of the largest mail order pharmacies, and over 25 of the nation's largest pharmacy benefit managers ("PBMs") for the purpose of exchanging prescription-related information in the ambulatory setting. Today, Surescripts provides access to prescription benefit and history information for more than 66 percent of patients in the United States on behalf of payers and pharmacies. Approximately 91 percent of community pharmacies in the United States are connected for prescription routing. More than 300 technology vendors' systems have been certified to connect to and access the Surescripts network.

Far more than technology is required in order to have a safe, efficient, and successful network. Other services and programs are essential components of the overall e-prescribing ecosystem such as certification, audit and compliance measures, e-prescribing network technology assets and capabilities such as provider and pharmacy directories, patient locator services, and quality improvement efforts.

In 2010, Surescripts announced the expansion its nationwide e-prescribing network to support and enable the electronic exchange of all types of clinical information, including referrals and up-to-date summaries of patients' recent visits with their health care providers. The Surescripts Network for Clinical Interoperability allows healthcare providers to securely send and receive clinical information with peers locally, regionally, nationally as well as between electronic health records ("EHRs") and across health systems and networks. The Surescripts Network for Clinical Interoperability improves clinical workflows, increases collaboration, improves quality and lowers costs by allowing all providers involved in a patient's clinical care to make more informed decisions.

Surescripts, in conjunction with the American Hospital Association, and the College of American Pathologists, has recruited hospitals to participate in a laboratory interoperability cooperative funded by a grant from the Centers for Disease Control and Prevention (the "Lab Interoperability Cooperative" or "LIC") to connect hospitals laboratories with public health agencies. Establishing this connection will enable hundreds of hospitals to engage in electronic reporting that helps public health officials act more rapidly and efficiently to control disease. During the two-year grant period, the LIC will recruit, educate and connect to the appropriate public health agencies a minimum of 500 hospital labs - at least 100 will be critical access or rural hospitals.

Surescripts' operations and principles have a foundation in the concepts of privacy and security – the imperative to safeguard the privacy and security of information that is transmitted across the network. Surescripts is very supportive of the vision and goals articulated by the National Strategy for Trusted Identities in Cyberspace (NSTIC), especially as it pertains to digital identities in healthcare. NSTIC's emphasis on security, efficiency, ease-of-use, and increased privacy for individuals are consistent with the key tenets of the Surescripts network.

Current Day – Security and Credentialing

With e-prescribing today, the industry maintains a chain of trust from prescriber to EMR vendor to pharmacy through contractual means. Surescripts holds prescriber technology vendors accountable for identity proofing and credentialing prescribers enabled for e-prescribing. In addition, Surescripts holds network participants (i.e., EMR vendors, pharmacies, and payers) accountable for compliance with the HIPAA Security Rule and best practices thereunder. The pharmacies and payers rely on Surescripts to hold EMR vendors accountable to these requirements through both our Certification and Compliance functions. In the current model, the prescriber technology vendor – either an EMR or a stand-alone e-prescribing application - maintains the direct relationship with the prescriber issuing credentials that can be used only in connection with that vendor's application.

Recently, the Drug Enforcement Agency (DEA) of the Department of Justice (DOJ) has raised the security bar for e-prescribing of controlled substances. The Interim Final Rule ("IFR") promulgated by the DEA requires prescribers to undergo Assurance Level 3 Identity Proofing in order to obtain a two factor authentication token, which is intended to be used to create an electronic signature for each prescription of a controlled substance. Thus, once through the identity proofing process, the prescriber now has a strong credential that can be used for Electronic Prescribing for Controlled Substances (EPCS). The IFR requires use of the credential for authentication for electronic signing prior to transmitting the controlled substance prescription. Under this model, the prescriber technology vendor remains responsible for

identity providers and managing the prescriber's credential in conjunction with their trust partners (e.g. credential service providers).

There are numerous initiatives evolving in the healthcare sector for the exchange of healthcare information that likely will require strong credentials and identity management to ensure security, privacy, and trust. In addition to the DEA's IFR described above, these include Health Information Exchanges (HIEs) being deployed around the country, ONC's Direct effort, Health Insurance Exchanges, Accountable Care Organization (ACO) pilots, and "meaningful use" interoperability requirements. The credentials issued and used by these various entities are "siloed" and credentials issued by one cannot be relied upon by another. This creates fragmentation and a burden on users.

The Need for Interoperable Trusted Identities

With the DEA requirement to use of a strong credential for EPCS, Surescripts sees an opportunity to aggregate trust in line with the NSTIC vision. Clinicians can leverage their digital identities for other purposes beyond their practices, whether making rounds at the hospital, volunteering at the free clinic, accessing state/HIE immunization registries, or potentially even accessing their bank accounts. Applications relying on clinician authentication can more readily trust the use of a credential for their purpose. Instead of managing one-off relationships, vendors and credential service providers could connect to a broker to reduce integration, legal, and administrative costs, all the while benefiting from a competitive marketplace of identity service providers. Clinicians no longer need a credential or password for every different application they use wherever they may practice. Health care stakeholders would be able to electronically interact in a trust community utilizing a trusted identity that follows them wherever they are and for whatever use they may need.

The HIPAA Security Rule and Trusted Identities

Surescripts believes that the concept of interoperable trusted identities compliment the HIPAA Security Rule provisions relating to individual authentication (45 CFR 164.312(d)) and can assist in streamlining the process for individuals to authenticate themselves in an electronic environment. The Security Rule requires entities to protect against any reasonably anticipated uses or disclosures of electronic PHI not permitted or required under the Privacy Rule and to implement procedures to verify that a person or entity seeking access to ePHI is who they say they are. As part of this, the Security Rule requires that an individual or entity be authenticated. However, the Security Rule does not mandate a specific framework or specify how to implement the standard.

As noted previously, a provider may be required to go through numerous different authentication processes in order to access her EMR at the practice location, from a mobile device, and from a hospital system, and has to maintain multiple digital identities to access non-EMR hospital systems or applications. In each of these scenarios, a provider could be required to submit and comply with duplicative requirements (and in some cases, differing requirements). In order to reduce the burden on providers to comply with HIPAA authentication requirements, Surescripts (and others) are working to develop an identity infrastructure to support digital identities that can be used across multiple mediums with a consistent standard to that can be relied upon by others (e.g., Assurance Level 3 authentication, if the industry accepts this as best practice).

Surescripts does not believe that the HIPAA Security Rule is necessarily insufficient, but rather that a single trusted identity that can "follow" an individual will make compliance easier in the long run, especially given the advent of multiple platforms that providers may access.

Building a Strong Identity Ecosystem

Surescripts is poised to utilize its technology, relationships, and connectivity within the health care ecosystem to drive health care identity interoperability. Specifically, Surescripts submitted a proposal for grant funding under the NSTIC Pilot Grant Program. If selected, Surescripts will conduct a trust broker pilot demonstrating how digital identities can be used in an identity ecosystem for the transmission of clinical and administrative healthcare data with two factor credentials for both governmental and non-governmental use. Our partners in this proposal include Cleveland Clinic, University of Pittsburgh Medical Center (UPMC), Exostar, and ApeniMED. Details and real world use cases are provided later in this testimony.

Health care providers need solutions that are portable and ubiquitous, while health care provider organizations (e.g., integrated delivery systems, physician networks, payers, pharmacies, etc.), need assurance that their affiliated health care providers are trusted to access services and information regarding their mutual patients. Clinical system vendors need a common standard to minimize their operational cost while maximizing options for their customers.

At the heart of identity interoperability are two harmonized and widely accepted standards – the federal government's NIST 800-63 standard and the industry supported Kantara Identity Assurance Framework standard (IAF). These standards describe:

1. Four progressively stronger levels of assurance;

2. The identity proofing requirements for each level of assurance;

3. The types of credentials that can be used at the various assurance levels;

4. The acceptable methods for authenticating these credentials.

If these standards are utilized consistently across health care, then all entities can understand and rely upon the strength of digital identities represented by the digital credential.

The vision of NSTIC is to serve identities across industries making it possible to re-purpose authenticated credentials. While today's digital identities are secure and meet the standards, the identities are not interoperable and cannot be used across disparate healthcare systems or networks. This is where the NSTIC vision comes into play.

Surescripts recognizes that the next generation of meaningful identity management in healthcare will necessitate the creation of reliable, interoperable, and trustworthy digital identities.

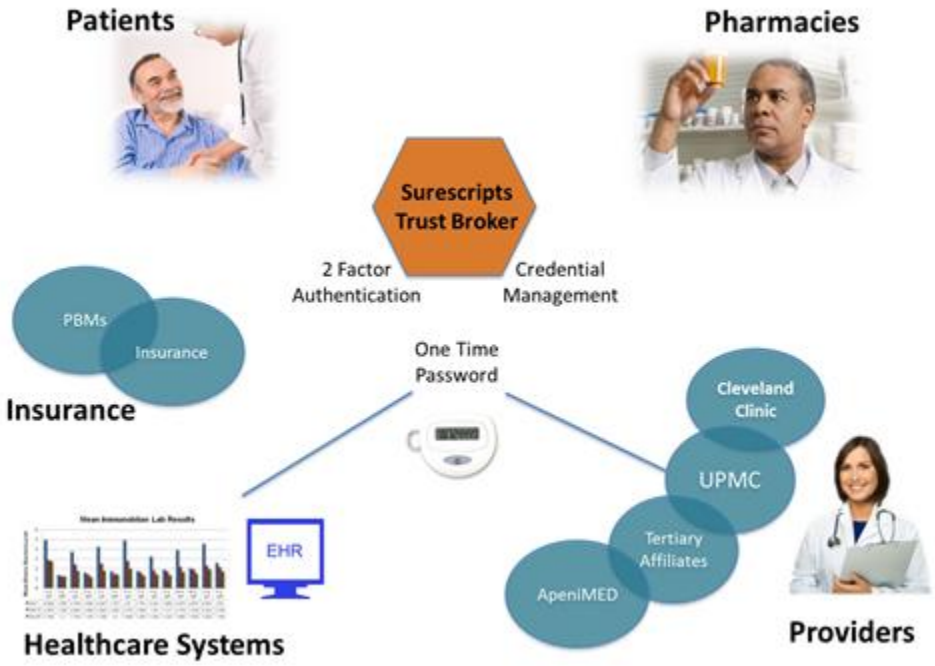
A solution that addresses the complexities of healthcare, however, which includes financial, administrative, and clinical dimensions, is a huge challenge by its self. Currently, there is great disparity across the healthcare industry sectors (the identity ecosystem) relative to organizational maturity, financial ability, and strategic desire to implement robust credentials.

Many provider organizations, already administratively challenged to fulfill federal mandates, are – for the most part— just beginning to develop identity management strategies internal to their organizations; thus are not ready to move to other industries at this time.

Under the proposed pilot, Surescripts would serve as a "trust broker" and will partner with healthcare providers and an identity provider to demonstrate the behavior of an interoperable healthcare identity ecosystem. The proposed Surescripts Trust Broker services are intended to support real life use cases, such as those routinely experienced by a healthcare provider. Some examples include:

- Electronically prescribing of controlled substances from any location;
- Proactively accessing a specific patient record as the provider walks into the patient's room in the hospital;
- Authenticating into the care portal of a different care system across town, to which the provider has admitting privileges;
- Sending a secure message and patient documentation from the EHR to a colleague in another care setting during the referral process;
- Sending audit documents to CMS;
- Filing a care audit report with state Medicaid; and
- Gaining admittance into the physician parking ramp at the hospital and transfer funds to pay for parking and meals in the hospital dining room.

Trust Broker Pilot Identity Ecosystem Roles



Although the Surescripts pilot will include only one trust broker, we fully expect others will emerge if this approach demonstrates value.

Recommendations for Trusted Identity Governance

Federal and state level programs and timelines are driving the landscape of the identity ecosystem. The federal government can be even more of a catalyst by:

1) Supporting pilots of the "trust broker" model to jump start innovation;
2) Emphasizing standards and collaboration to refine and/or create new standards. Wherever possible, include standards in regulations;
3) Enabling easier compliance to single identity trust frameworks due to centralized authentication and credential management;
4) Providing recommendations on assurance levels and compliance so that such recommendations could provide a measure of "safe harbor" protection. For example, if Assurance Level 3 is recommended as a best practice, then an individual could be authenticated to and issued credentials to Assurance Level 3. Any entity relying on those credentials will be able to trust that individual identities meet the standard as required by HIPAA without conducting their own identity proofing, authentication, and credential issuance.

In conclusion, Surescripts supports the NSTIC vision and believes NSTIC can play a vital role in ensuring the success in the healthcare sector as it transitions from a paper to digital world. Our industry, with the introduction of EPCS and the identity standards provided by NIST and Kantara, can provide a real life proving ground for this NSTIC vision, while meeting the requirements set forth in HIPAA. This will raise the bar and serve as a catalyst for building a strong digital identity management marketplace.