THE ROLE OF STANDARDS-BASED INTEROPERABLE DIGITAL IDENTITIES IN HEALTHCARE

THREE EXPERT POINTS OF VIEW

LEGAL CONSIDERATIONS: Timothy Reiniger, Esq. member of the Electronic Discovery and Digital Evidence Committee of the American Bar Association and Director, Digital Services Group, FutureLaw, LLC. Richmond.

SIGNING ePRESCRIPTIONS: Lee Ann Stember, President, National Council for Prescription Drug Programs, Inc. (NCPDP), an ANSI-accredited standards development organization leading transformation in the pharmacy services sector by creating and promoting standards for electronic healthcare transactions. NCPDP represents 1600+ members.

PROVIDING IDENTITY SOLUTIONS FOR HEALTHCARE: Tracy Hulver, Chief Strategist, Enterprise Identity Solutions, Verizon Enterprise Solutions, a leading provider of communication, security and IT services to a majority of Fortune 1000 healthcare companies.

INTRODUCTION

Mollie Shields-Uehling, President and CEO, SAFE-BioPharma Association which manages the global SAFE-BioPharma® digital identity and digital signature standard. SAFE-BioPharma was created to meet security and confidentiality needs specific to the life sciences and to healthcare.

WHITE PAPER

Research collaboration in the cloud: How NCI and Research Partners are using Interoperable Digital Identities, Digital Signatures, and Cloud Computing to Accelerate Drug Development

This document can be downloaded at www.safe-biopharma.org/infocenter/HIMSS.pdf
INTRODUCTION

The ability to trust online identities is the foundation of transforming healthcare to a paperless and fully electronic business environment. It is the primary consideration when providing individuals with ways to authenticate into systems and to apply legally-binding digital signatures to a host of forms and other documents – especially in heavily regulated environments.

Trust also is the main driver behind the global SAFE-BioPharma digital identity and digital signature standard. SAFE-BioPharma was created to meet security and confidentiality needs specific to the life sciences and to healthcare. It was developed with participation from the US Food and Drug Administration and the European Medicines Agency and has been cited by the US Drug Enforcement Agency as compliant with DEA rules governing electronic signatures on prescriptions for controlled substances.

When the White House announced the National Strategy for Trusted Identities in Cyberspace (NSTIC) initiative, it referenced a study in which National Cancer Institute researchers and private sector cancer researchers collaborated using cloud computing. The collaboration was made possible because participating researchers were able to trust their respective digital identities [government researchers used government-issued digital identities; company researchers used SAFE-BioPharma digital identities]. The mutual trust was possible because SAFE-BioPharma has cross-certified with the government system. Indeed, any SAFE-BioPharma digital identity will be trusted within government agencies.

There are many learnings from this study that apply to the healthcare community (a white paper describing the study appears at the end of this document). All are based on trust.

- Electronic access to confidential records requires a secure form of authentication that is tightly bound to the user’s actual identity
- Eliminating the inefficiencies and inaccuracies of paper records requires use of digital signatures, also tightly bound to the user’s identity
- Interoperability – the ability of a digital identity from one system to be accepted and trusted within another system – is essential to communicating across healthcare entities.

To advance appreciation for the use of standards-based interoperable digital identities in the healthcare arena, I asked three authorities to submit their thoughts.

- Timothy Reineger, Esq., a member of the Electronic Discovery and Digital Evidence Committee of the American Bar Association, and Director of the Digital Services Group of FutureLaw, LLC, Richmond, Virginia, writes about the legal considerations for interoperable digital identities and their advantages in healthcare.

- Lee Ann Stember, President, National Council for Prescription Drug Programs, Inc., discusses the importance of identity and trust in transforming healthcare and the potential value of standards-based digital signatures for signing electronic prescriptions.

- Tracy Hulver, Chief Strategist, Enterprise Identity Solutions, Verizon Enterprise Solutions, describes his company’s new Universal Identity Services for healthcare, which supports the SAFE-BioPharma standard.

We hope you find this information helpful and encourage you to learn more about the SAFE-BioPharma digital identity and digital signature standard.

Mollie Shields-Uehling, President and CEO
SAFE-BioPharma Association
mollie.shields.uehling@safe-biopharma.org
www.safe-biopharma.org

SAFE-BioPharma® is a trademark of SAFE-BioPharma Association. Any use of this trademark requires approval from SAFE-BioPharma Association.
THE NCI – SAFE-BIOPHARMA PILOT FOR CLOUD MANAGEMENT OF CLINICAL TRIAL PAPERWORK: LEGAL BENEFITS OF USING INTEROPERABLE DIGITAL IDENTITIES AND ADVANTAGES FOR ELECTRONIC HEALTH RECORDS

By Timothy S. Reiniger, Esq.

The strategic management of information assets in the digital network-based global economy must be based on reliable digital identity credentials and access control. For a digital identity to be deemed legally interoperable, it must be capable of enabling strong two-factor authentication, encryption, and standards-based digital signatures. This will ensure compliance with applicable property, confidentiality, and evidentiary requirements.

Network economics depend on clear legal rights in the form of access and use rights to systems and records. Key to this is access control. In particular, interoperable digital identities, such as those issued and maintained in accordance with the global SAFE-BioPharma® digital identity and digital signature standard, give data holders the capability of exerting legal control over access to information assets to prevent unauthorized viewing and for detecting content-level changes, including for records stored in the cloud.

LEGAL CONSIDERATIONS FOR INTEROPERABLE DIGITAL IDENTITIES

The SAFE-BioPharma standard establishes minimum criteria for issuing, managing, validating, and securing the interoperable digital identity. To ensure that communications, electronic signatures, and records are reliable and resistant to fraud and manipulation, access control should rely upon a high assurance interoperable digital identity over which the sender or signer has sole control by means of a two-factor authentication process.

1. Legal Controls: Strong Authentication

The use of interoperable digital identities for strong authentication has three purposes: access, attribution, and adoption. First, a digital identity can be used as, in effect, a key to allow authorized individuals to electronically obtain access to secure networks such as a health information exchange or to records stored in the cloud. Second, a digital identity should attribute the origin of a message so that the recipient can trust the identity of the sender as an approved member of a network. This is vital to secure information exchange and supply chain collaboration. Third, a digital identity provides a means for a signer to adopt the contents of an electronic document with the intent to render a legally enforceable signature.

2. Legal Controls: Reliable Signatures

Digitally signing electronic records with an interoperable digital identity ensures the capability for relying parties, over time, to test the authenticity and reliability of the information that was intended to be the equivalent of a paper original. Consistent with the SAFE-BioPharma standard, a United States federal magistrate for the District of Columbia has adopted a process for issuing official court orders in digital form. By means of a digital signature, the magistrate includes a detective control in the document so that relying parties may test the document’s origin, integrity of contents, and date and time of issuance. No external evidence is necessary because all the validation evidence is included in the digital signature itself.

3. Evidentiary Authentication of Digital Records

Digital evidence is subject to the same admissibility tests as paper records. However, the ephemeral nature of digital evidence and the ease with which digital objects can be undetectably modified make the problem of authentication much more complex than that of paper records. A successful argument to establish a foundation of authenticity relies on a combination of application and system access controls (by the use of strong authentication) and content-level controls to detect modification (by the use of digital signatures).

4. Compliance with International Requirements

An international e-document authenticity standard has emerged for an electronic public document that reflects the evidentiary need for electronic documents to have the capability of testing the authenticity of the document. Establishing the authenticity of an electronic official record from another nation thus requires the capability, in perpetuity, of independently authenticating the origin of the document, and verifying whether the content of the electronic document is complete and unaltered. The SAFE-BioPharma standard complies with this international standard, the European Union’s electronic signature directive, and US laws.

5. Legal Controls: Cloud Computing

Use of the cloud raises important security considerations for digital records at rest, in use, and in transit. While operational responsibility shifts from data holders to cloud service providers, the data owners and holders now have greater responsibility for setting the legally necessary data level protections, including access and usage controls. Interoperable digital identities provide a means for a data holder to establish legal control over digital records in the cloud by using persistent content-level protective controls, such as encryption and digital signatures, before storing the records.

ADVANTAGES TO THE USE OF INTEROPERABLE DIGITAL IDENTITIES IN HEALTHCARE

The challenge facing the global move toward electronic health records (EHR) is establishing a uniform and trustworthy approach for issuing and managing digital identity credentials and signatures. Key
to achieving integrated and productive flow of EHRs will be enabling data holders to 1) classify the records, 2) allocate access rights, and 3) determine why such access rights are being granted. For these purposes, leveraging interoperable digital identities can provide significant advantages for EHRs.

1. Enables Compliance with L3 Credential Assurance Level Requirements
   The SAFE-BioPharma standard enables issuance of interoperable digital identities to individuals at the L3 assurance level (the National Institute of Standards and Technologies has established four graduated assurance levels and related polices for authenticating identity and protecting sensitive information, labeled as L1, L2, L3, and L4). In the biopharma industry, there is already significant use of Level of Assurance 3 digital identity because of the need to protect proprietary corporate information. For e-prescribing of controlled substances, the US Drug Enforcement Agency stipulates two-factor L3 credentials for strong authentication of physicians. This may become prevalent in healthcare as well due to HIPAA security requirements and the pending Notice of Proposed Rulemaking, from the Office of the National Coordinator for Health IT, which may require two-factor, L3 authentication to applications including EHRs and potentially for both citizens and practitioners. The Virginia Health Information Exchange already requires two-factor, L3 authentication.

2. Enables Access Control Necessary for Effective Encryption
   Consistent with the HIPAA Security Rule’s call for encryption, interoperable digital identities are capable of adding a layer of content protection by means of encryption, hashing, and other content controls. However, encryption, by itself is not enough to adequately protect against criminals who access the applications to steal access rights and keys to decrypt the data. Access controls, based on interoperable digital identities, are necessary to ensure that any changes to records are authorized and logged.

3. Enables Assignment of Access Rights and Integration of EHRs
   The use of interoperable digital identities contemplates a system of decentralized decision making and control with respect to digital identity issuance and access rights. Therefore, determinations of legal rights and duties are necessarily contextual according to 1) the relative access controls of each data holder; 2) control and reliability of the digital identity; and, 3) the nature and superiority of the property interests in the digital information being collected, used, or disseminated. Interoperable digital identities are intended to enable the identity ecosystem participants to determine the context and relevance of digital information for purposes of access rights, usage rights, and duties of protection. Identification enables third parties to recognize an individual’s identity in the context of relationships.

4. Enables Custodians of EHRs to Fulfill Legal Control Obligations
   EHR custodians can leverage interoperable digital identities to ensure the ongoing integrity of digital records and to fulfill confidentiality and lawsuit records’ retention requirements. Access controls and document-level detective and preventive controls offer several benefits — the ability to verify the source and authenticity of records, the ability to preserve evidence of access history and usage activity, the ability to establish chain of custody, and the ability to prevent unauthorized access.

5. Enables Compliance with Signing Requirements
   The SAFE-BioPharma standard establishes a trustworthy process for binding the identity of an individual to a digital credential. This is crucially important when taking into account that the integrity of the content of the electronic document and the signatures, such as a patient consent form, rests on the capability of identifying the actual signer or sender of the document in a trustworthy manner.

6. Enables Use of the SAFE-BioPharma Standard for Cloud Applications
   Virginia has become the first state in the United States to authorize cloud-based online notarization by means of a two-way live video recorded teleconference. An archived log will be created of signer consent for powers of attorney, advance health directives, and other witnessed records. In addition, the new Virginia law empowers notaries to provide more convenient and available identity proofing services to meet L3 vetting requirements for the issuance of large numbers of interoperable digital identities.

CONCLUSION

Without an interoperable digital identity that is aligned to the various state, national, and international signature laws and emerging industry access control and secure messaging requirements, healthcare professionals everywhere face the need to own multiple electronic credentials. At the same time, every party who relies on EHRs should know that the digital identity and signature used are legally valid and enforceable.

ABOUT THE AUTHOR: TIMOTHY S. REINIGER, ESQ.

Timothy Reiniger, a member of the Electronic Discovery and Digital Evidence Committee of the American Bar Association, is an attorney currently serving as Director of the Digital Services Group of FutureLaw, LLC in Richmond, Virginia where he recently authored Virginia’s online notarization law, the first of its kind in the United States. He specializes in information law and policy and is a contributing author to George Paul’s book, FOUNDATIONS OF DIGITAL EVIDENCE. Mr. Reiniger is licensed to practice in California, New Hampshire, and Washington, D.C. He graduated from Georgetown University School of Foreign Service and the University of Michigan Law School.

Direct inquiries to treiniger@futurelaw.net
PLANNING TODAY FOR TOMORROW’S HEALTHCARE DEMANDS

By Lee Ann Stember, President, National Council for Prescription Drug Programs, Inc.

NCPDP (National Council for Prescription Drug Programs) has been a mainstay at the forefront of enabling a real-time environment for the pharmacy industry. Eighteen years before The Office of the National Coordinator for Health Information Technology (ONC) made it a core requirement of Meaningful Use, we began planning for electronic prescribing (e-Prescribing), and in 1999 NCPDP’s SCRIPT became an ANSI-approved standard. A success story 35 years in the making, we continue to provide innovative and forward-thinking solutions to streamline and automate the business of pharmacy, and for the ultimate benefit of the patient and healthcare consumer.

IDENTITY AND TRUST

Identity management is a critical issue in healthcare. This goes well beyond verifying and authenticating individuals from a technology standpoint – it delves deeper into the question of how do we know that the individual for whom the information is intended is the actual person at the receiving end?

The HIPAA-mandated national provider identifier (NPI), a unique identification number for covered health care providers, and the Drug Enforcement Administration (DEA) number, which is required for prescribing controlled substances, are both used to identify prescribers. In cases of e-Prescribing there is an additional provider routing number along with other DEA mandated requirements. Still, we are mindful that the complexity of resolving the issues around identity will continue to be a priority, particularly as healthcare moves beyond its traditional boundaries and new care teams and collaborations are established, requiring the exchange or sharing of health information. The technology and collaborations must ensure the privacy and security of health information and will require stakeholder trust.

Not to be underestimated, trust may be as big of a challenge as technology itself. The pharmacy industry has proven that trust and true collaboration can be achieved. Moreover, they are both fundamental to transforming healthcare.

REAL WORLD APPLICATIONS FOR DIGITAL SIGNATURES

NCPDP, the not-for-profit, ANSI-accredited standards development organization for the pharmacy industry, also serves as the industry’s forum for hosting and exploring a broad range of issues brought forth by all segments of healthcare. While the organization performs extensive due diligence on all issues, it is particularly vested in patient safety issues as well as initiatives that help move healthcare from a paper-based to a real-time electronic environment.

The project success demonstrated by the National Cancer Institute’s Cancer Therapy Evaluation Program and Bristol-Myers Squibb Company using the Federal Bridge and SAFE-BioPharma to pilot interoperable digital identities and digital signatures validates yet another way to simplify and automate a time consuming, costly process.

We see the value and potential for the application of the SAFE-BioPharma standard and the technology. In 2011 NCPDP and SAFE-BioPharma announced a strategic alliance to advance use of their respective standards within the life sciences. The collaboration can add another layer of authentication to the Telecommunication Standard as well as e-Prescribing standards [NCPDP SCRIPT Standard]. SAFE-BioPharma digital signatures may also support the need for certainty around prescribers in Risk Evaluation and Mitigation Strategies (REMS), electronic prior authorizations (ePA) and more. We will continue to explore such synergies with SAFE-BioPharma as part of our global efforts to support industry-wide adoption of meaningful, innovative and sustainable technologies.

ABOUT THE AUTHOR: LEE ANN STEMBER, PRESIDENT, NCPDP

As President of the National Council for Prescription Drug Programs, Inc. (NCPDP), Stember represents the Council and its strategies, issues, and policies through her work with government agencies, pharmaceutical and health care organizations, academia, standards development organizations, and others actively involved in standards development for the pharmacy industry. Stember has been an integral part of NCPDP for 30 years as it has progressed into international acceptability and advanced in the standards setting arena.

Stember utilizes her professionalism and leadership skills to effectively operate the Council office and act as a liaison to the Board of Trustees, Work Group and Committee Co-Chairs, and other pharmacy industry executives. Stember is also an active member in several health care associations, including the American Managed Care Pharmacy (AMCP) Association, National Association of Chain Drug Stores (NACDS), National Community Pharmacists Association (NCPA), American Pharmaceutical Association (APhA), Workgroup for Electronic Data Interchange (WEDI), American Management Association (AMA), American Society of Health-System Pharmacists (ASHP), American Society of Consultant Pharmacists (ASCP) and the American Society of Association Executives (ASAE).

Currently, Stember serves on the WEDI Board of Directors, and has previously served on the PharmData Foundation and the PharmaSMenu.com Board. Stember has also served on the Editorial Board for Group Practice Managed HealthCare News and was a former member of the Board of Directors for Computerized Patient Record Institute (CPRI). Stember is a 1979 graduate of the University of Arizona College of Business.

Direct inquires to Lee Ann Stember, President, NCPDP, at lstember@ncpdp.org or to John Klimek, Senior Vice President, Industry Information Technology, NCPDP, at jklimek@ncpdp.org.
PROVIDING IDENTITY SOLUTIONS FOR HEALTHCARE

By Tracy Hulver, Chief Identity Strategist, Verizon

Healthcare faces many business and regulatory challenges in its quest to provide a positive authentication experience for its identity credential users. These include controlling costs, reducing healthcare identity fraud, and meeting increasingly stringent requirements for strong authentication of healthcare professionals.

Recognizing the need to help healthcare professionals rapidly and cost-effectively address these challenges, Verizon has developed Universal Identity Services (UIS), a cloud-based identity-as-a-service solution that provides an identity ecosystem, without having to implement new complex technologies. This comprehensive solution includes identity proofing, credential issuance, strong authentication, and digital signature services. Services that can typically take weeks to perform can be handled in minutes —without paper-based processes or manual updates for multiple applications.

UIS’ capabilities directly support the findings in the 2010 pilot study which, in utilizing interoperable digital identities, digital signatures and cloud computing, demonstrated results in the acceleration of the initiation of clinical trials while at the same time lowering associated costs.

As an example, UIS enables healthcare practitioners with the flexibility to approve and digitally sign electronic prescriptions when away from their desks—providing patients with fast access to necessary medications with high-assurance identity credentials. These digital signatures also can be used for other transactions, such as patient release, records release, insurance processing, etc. Essentially, any activity that requires a legally recognized signature can be processed with the digital signature services available on the mobile application. Practitioners also have immediate access to all past transactions processed by the ID Message Center and can provide answers to questions about past prescriptions.

UIS is based on Verizon’s broad experience supporting the healthcare industry. Verizon provides communications, security, network and IT services to thousands of customers, including a majority of Fortune 1000 healthcare companies. Verizon enables healthcare providers to transform the delivery of care, better manage costs, enhance access to services, and provide data privacy.

FOLLOWING IS A SUMMARY OF THE KEY COMPONENTS OF VERIZON UNIVERSAL IDENTITY SERVICES FOR HEALTHCARE:

Identity Proofing
UIS includes identity proofing in a fully electronic process, including verification of US medical license and DEA numbers. UIS also supports enterprise antecedent data load or a bulk upload using web services. After users complete identity proofing, they can update their information, reset passwords and

PINs in a fully electronic process, and register new authentication credentials such as a new email or new mobile device. For administrators, UIS includes an interface to enable customization and a dashboard for tracking service use.

Credential Provisioning
UIS enables users to use credentials they already have—such as an email or a mobile device. Organizations can choose specific credentials or can simply enable all UIS options. UIS supports phone calls, text messaging, and interactive voice response (IVR) around the globe.

Authentication
UIS provides a strong, yet flexible, authentication gateway, supporting enterprise and user preferences for delivery of one-time passcodes (OTP) within timeout and lockout policies, helping limit organizational risks. UIS includes support of SAML 1.x—2.0, and Juniper Networks or Citrix VPN support via SAML. The UIS mobile application and ID Message Center allow practitioners to access and approve transactions anytime, virtually anywhere. Users have an easily accessible record of past transactions—approved and rejected—as well as pending transactions. Enterprises can enable an online version of the ID Message Center, providing the same features as the mobile application.

Digital Signature Services
Universal Identity Services include digital signature services that enable electronic prescriptions for controlled substances and also meet enterprise needs. The digital signature on a document—prescription, W-9 form, or internal corporate document—is legally recognizable as a wet signature. Users can also use digital signatures for other healthcare activities, such as signing pages in electronic lab notebooks—which could be vital in patent defense. Enterprise users can apply digital signatures to essential corporate documents, such as employment, financial, or other materials.
UIS Mobile Application and ID Message Center
UIS includes a mobile application that is available on BlackBerry (touch and non-touch), Google Android, Microsoft® Windows® Phone, and Apple iOS devices (iPhone, iPad, and iPod Touch). This mobile application provides an OATH soft-token for providing one time passwords (OTP) to authenticate a transaction. Users access the mobile application by providing their PIN, which they define as part of registering their UIS identity. UIS combines the user-supplied PIN with the OTP, and authenticates the user to their ID Message Center queue of transactions.

ABOUT THE AUTHOR: TRACY HULVER, CHIEF STRATEGIST, ENTERPRISE IDENTITY SOLUTIONS, VERIZON ENTERPRISE SOLUTIONS

Tracy Hulver is chief enterprise identity strategist for Verizon Enterprise Solutions with responsibility for driving the strategy and delivery of Verizon Enterprise Identity Services and helping the company manage millions of identities around the globe by helping Verizon customers reduce the risks of identity fraud through better protection of online credentials.

A well-known industry leader and globally sought-after speaker in the areas of cyber attacks and security intelligence, Hulver was most recently honored as a 2010 Security “Superstar” by CRN.

Hulver is a member of the Computer Security Institute, the National Cyber Security Alliance, the Armed Forces Communications and Electronics Association, the Information Systems Security Association, and the Cloud Security Alliance. In 2002, he served on the Department of Homeland Security’s National Cyber Security task force.

Hulver holds a bachelor’s of science in business administration with a minor in computer science from Strayer University.

Direct inquiries to tracy.hulver@verizonbusiness.com

White Paper

Research collaboration in the cloud:
How NCI and Research Partners are using Interoperable Digital Identities, Digital Signatures and Cloud Computing to Accelerate Drug Development

Contributors:
Executive Summary

A 2010 pilot study involving government and industry cancer researchers indicates that using interoperable digital identities, digital signatures and cloud computing will accelerate initiation of a clinical trial while lowering its costs. They participated in the first phase of a pilot study examining use of interoperable digital identities and cloud-based digital signatures to eliminate reliance on paper forms in clinical trials.

The ongoing study involves researchers at the National Cancer Institute's Cancer Therapy Evaluation Program (NCI/CTEP) and Bristol-Myers Squibb Company. NCI/CTEP is the world's largest sponsor of cancer treatment clinical trials.

The researchers were provisioned with interoperable digital identity credentials, a form of software installed on a computer, cell phone or other device, which establishes a close link with the user's proven identity and allows for the application of digital signatures to electronic documents. Unlike their simple electronic counterparts, digital signatures cryptographically guarantees the integrity of documents to which they are affixed. In the pilot study, the electronic documents were placed in the cloud, where the researchers were able to access and sign them immediately. Prior to the study, the signature process was delayed by use of courier service, fax, travel, etc.

The digital credentials exist within legally-binding and regulatory-compliant cyber-communities, known as identity trust hubs.

- All US federal agencies are served by the Federal Bridge identity trust hub, which provided the NCI researchers with their digital identity credentials.
- The biopharmaceutical and healthcare industries are served by an identity trust hub known as SAFE-BioPharma, through which the Bristol-Myers Squibb researchers received their credentials.

The Federal Bridge and SAFE-BioPharma cross-certified to become interoperable, allowing a digital identity asserted by one to be trusted by the other. Both the Federal Bridge and SAFE-BioPharma are part of a matrix of identity trust hubs serving governments, industry sectors and higher education. These identity trust hubs are affiliated through the Four Bridges Forum (www.the4BF.com).

Phase I (July 2010 – October 2010) demonstrated the use of digital identities for authentication and the application of digital signatures to electronic documents

Phase II (underway) expanded the study to include researchers in sanofi-aventis.

Phase III (expected to start mid-year) will include researchers at universities and academic cancer research centers. Their digital identities will be part of the Research Education Bridge Certification Authority (REBCA), an identity trust hub serving the country's higher education sector and which currently is in the process of cross-certifying with other trusted cyber-communities.

The pilot successfully demonstrated the ease with which interoperable digital identities could be deployed and used to access electronic documents and apply digital signatures to them. It eliminated use of paper copies and allowed signed documents to be exchanged rapidly and securely on-line for business processes initiated by the NCI/CTEP’s Protocol and Information Office (PIO).

Background

Numerous forces are driving public and private sectors to exchange confidential documents via Internet faster, more economically and with greater security. Pharmaceutical companies are highly collaborative and require a constant flow of confidential information with researchers, healthcare providers, and regulators worldwide. R&D productivity is one of the major challenges facing life sciences. Time lost in starting or conducting clinical trials results in substantial financial losses and delays delivery of new therapies to patients. NCI has been mandated to more quickly initiate clinical trials to patient accrual, to reduce costs, to streamline document management while assuring greater document security, and to have environmentally sound procedures.

SAFE-BioPharma and Federal Bridge Certification Authorities

The SAFE-BioPharma standard and the Federal Bridge Certification Authority (FBCA) use public key infrastructure (PKI) technology. PKI is used by numerous stakeholders (particularly governments and regulated industries) to verify identities and to protect information exchanged via the Internet. When PKI communities, also known as “identity trust hubs,” cross-certify with each other, they become interoperable, thereby allowing a digital identity asserted by a user from one community to be relied upon and accepted by a relying party from another community.

Among other trust hubs, SAFE-BioPharma is interoperable with FBCA, the U.S. government’s PKI-based system serving U.S. federal agencies.

SAFE-BioPharma -- The SAFE-BioPharma standard requires that the signatory’s proven identity is captured in a digital certificate and made available to apply digital signatures. The standard also requires each digital identity to adhere to rules that guide and regulate its uses.

SAFE-BioPharma digital signatures offer a greater level of protection than other forms of electronic signature. They provide authentication, non-repudiation and data integrity across every single bit of the information to which the signature is applied. In simple terms this means that if any component of the signed document is ever changed, the signature will be invalidated. The contract-based standard requires all members and users to meet technical requirements, to accept each others’ SAFE-BioPharma identities and signatures, and to enter into the community’s risk mitigation system.

SAFE-BioPharma was created specifically for use in the global biopharmaceutical industry and in the healthcare arena. The US Food and Drug Administration (FDA) and European Medicines Agency (EMA) have been and continue to be active participants in the standard’s development and evolution. SAFE-BioPharma digital identities are recognized and trusted within the SAFE-BioPharma community.

SAFE-BioPharma credentials can be provisioned from a variety of certificate authority infrastructures including Citibank, Exostar, IdenTrust, PGP TrustCenter, Trans Sped, and the SAFE-BioPharma system operated by Verizon Business Systems.
Federal Bridge -- The Federal Bridge Certification Authority is an identity trust hub used by NCI/CTEP. FBCA and SAFE-BioPharma have formalized relationships with each other and each asserts the identity of its participants across the entire federation. This relationship allows biopharmaceutical companies that use the SAFE-BioPharma standard and US Federal agencies that use FBCA to recognize and accept documents that carry each other’s digital signature. This demonstrates the efficiency and security of cross-jurisdictional credentials usable by all participants and secured through a PKI-based infrastructure.

The Federal Bridge and the Federal Public Key Infrastructure Policy Authority (FPKIPA) are, in part, based on standards/guidance provided by NIST.

NCI/CTEP

NCI/CTEP is the world’s largest sponsor of cancer treatment clinical trials, reflecting its mission to improve the lives of cancer patients by finding better ways to treat, control and cure cancer.

The program currently has 900+ active clinical trials testing new cancer treatment regimens. It activates approximately 130 new protocols per year. During the protocol lifecycle, from concept to closure, each protocol produces many signed and exchanged documents among multiple participants, including cooperative groups -- groups of physicians and/or medical institutions cooperating to investigate new treatments, cancer centers and academic institutions.

To pilot the digital signature process, NCI/CTEP selected its randomized Phase 2 and Phase 3 trials conducted through Cooperative Groups.

The protocol process follows:

• A Cooperative Group submits a Concept/ Letter of Intent (LOI) for CTEP review and approval
• After CTEP review a signed letter is sent to the cooperative group along with a consensus review of suggested changes.
• The collaborating pharmaceutical company receives a copy of the LOI or concept and submits a signed drug approval letter allowing CTEP to approve the LOI/Concept so the group can author and submit a protocol.
• Upon CTEP receipt of the protocol, a signed acknowledgement letter is sent to the Cooperative Group.
• Once the protocol is reviewed by CTEP; a signed comment letter is sent back to the Cooperative Group.
• A revised protocol is then resubmitted (there may be multiple revisions before final protocol approval is granted).
• CTEP approval or disapproval of the revised protocol is sent via signed letter.
• Amendments to protocols follow the same last few steps for review, revision, and notification of approval or disapproval.

Business Need

The pilot demonstrated dramatic time savings for all document flows that require multiple signatures from participants working on or off-site. It demonstrated how an all electronic workflow including digital signatures improves the business process flow and thus improves the ability of NCI to speed up research and be more responsive to public health needs.

Documents

The first step was to develop digital signature and workflow capabilities for the following documents:

- Protocol receipt Acknowledgement Letter
- Protocol Approval/Disapproval
- Clinical Trial Agreements
- Contracts

Streamlining the signature workflow of these documents allowed research to get underway more quickly. Depending upon specific documents involved, it eliminated hours to weeks to months in the document workflow process.

Digital Signature Service

The enhanced services were provided by utilizing FBCA cross-certified, PKI-based, digital certificates with existing SAFE-BioPharma members. In subsequent phases, these certificates will be deployed to all cooperative groups and drug suppliers.

The architecture consists of each signatory having Internet access and a FBCA or SAFE-BioPharma cross-certified digital credential and access to a digital signature service. This project leverages an existing Safe-BioPharma hosted digital signature service (DSS), which replaces handwritten signatures and paper based document routing services such as courier and/or fax. The documents are available only to people signing the documents, with access controlled through a self-provisioned user account based on each user’s email address. Because the address must match the email address in the digital credential, only digital credentials issued from approved Certification Authorities are accepted. Once provisioned, access can be controlled via strong 2-factor authentication.
The DSS works as follows:
• A document requiring signatures is uploaded to the DSS.
• Signatories are alerted via email that a document is awaiting signature.
• Once all signatures are obtained, the document originator is alerted to download the document.

The DSS provides significant value while enhancing security and respecting state and federal privacy laws. The following diagram illustrates the system-level document workflow topology:

Identity Proofing
E-Authentication identity proofing/assurance levels are defined by NIST SP 800-63-1 and cover four assurance levels. Levels 1-2 are single factor with different identity proofing methods as follow:
• Level 1 does not require identity proofing, i.e. the credential holder asserts his identity and proof is not required.
• Level 2 requires proof.
• Levels 3-4 are 2-factor authentication with more rigorous identity proofing methods.

Government identification documents with requirements (Level 4) must be provided to prove the source.

The Federal Bridge Certification Authority – Certificate Policy (FBCA-CP) allows for five different assurance levels (Rudimentary, Basic, Medium, Medium Hardware, and High) for public key certificates. These FBCA-CP assurance levels are a combination of an appropriate identity proofing and credentials, e.g. FIPS 140-2 encryption. (Source: FBCA CP RFC3647.pdf).

The different assurance levels, aligning NIST SP 800-63-1 and the FBCA-CP, require coordination and can be verified with the FPKIPA and its Certificate Policy Working Group. SAFE-BioPharma Association sits on both committees, as a non-voting member, through the FBCA cross-certification.

Additionally, the FPKIPA requires an annual audit by all participants to verify effective implementation of the FBCA-CP. The FBCA-CP is the aligning document that all FBCA participants, e.g. DHHS, DoD and all cross-certified issuers (i.e. SAFE-BioPharma Association), must adhere to in implementing their respective PKI structures and policies.

Results
Cost Savings
Substantial cost savings are anticipated as the pilot moves to production. Using paper forms, an average 10% of the documents are shipped overnight and 10% are shipped by courier service. Using digital signing, those costs are eliminated.

Time Savings
The time savings are significant. Paper processes are time consuming and often require physically shipping documents to signatories. Typically it takes 3 to 5 business days per signature. The pilot demonstrates that each signature can take minutes. Furthermore, NCI/CTEP estimates that in 2010 documents comprising almost 100,000 pages were used to develop and correspond on its clinical trials. While the unit does not track the time involved in scanning, organizing and sending these paper documents to the FDA, it reports that it is extremely labor intensive and, once digitized, will be greatly simplified.

Document Loss
The pilot demonstrates elimination of lost or misplaced documents. Using digital signatures establishes an audit trail of when the document was uploaded, of the email sent to alert the signatory that the document is available for signature, and when the document was actually signed.
Reduced Environmental Impact
Besides saving money, time and reducing document loss, the pilot also is reducing the carbon footprint. Moving to an electronic process eliminates use of paper and ink, eliminates document shipment, and minimizes storage and retrieval needs.

Next Steps
Phase 1 of the pilot was determined a success and Phase II is being initiated with sanofi-aventis and additional BMS staff. Additionally, business workflow processes will expand to include NCI’s Regulatory Affairs Branch. Phase III is under development with requests for involvement going out to Cooperative Groups that are REBCA members.

Summary
Use of interoperable FBCA digital credentials and those based on the SAFE-BioPharma digital standard facilitated the successful implementation of a public/private pilot that showed how paper processes can be eliminated from initiating a clinical trial. As the pilot expands to include other companies and university-associated cancer treatment centers [via the Research Education Bridge Certification Authority], the use of interoperable digital credentials and digital signatures to sign research-associated documents will expand. As a result, medical and clinical trial research will be conducted with greater efficiency and therapeutics will be delivered faster and with lowered environmental impacts.