

**SAFE-BioPharma Association's Comments on 21 CFR Parts 1300, 1304, et al.,
Electronic Prescriptions for Controlled Substances; Proposed Rule
Docket No. DEA-218**

25 September 2008

General Comment

SAFE-BioPharma™ Association is pleased to review and comment upon the DEA proposed changes to 21 CFR Parts 1300, 1304, 1306, and 1311, [Docket No. DEA-218P], RIN 1117-AA61, Electronic Prescriptions for Controlled Substances.

As background, SAFE-BioPharma Association is a non-profit collaboration created by the biopharmaceutical industry to establish and manage a digital identity and signature standard. The standard was created be a catalyst in the transformation of the biopharmaceutical sector and its partners in the healthcare community to a fully electronic environment. It is used to mitigate legal, regulatory and other business risk associated with business-to-business and business-to-regulator electronic transactions. It facilitates interoperability by providing a secure, enforceable, and regulatory-compliant way to verify identities of parties involved in electronic transactions. The three-year old standard is being used on a broad scale. Current implementations include the application of digital signatures to electronic regulatory submissions and patent-related documentation, contracts, authentication of external partners, and a wide variety of research and development applications.

The Association's members are Amgen, AstraZeneca, Bristol-Myers Squibb, Genzyme, GlaxoSmithKline, Johnson & Johnson, Merck, the National Notary Association, Organon/Schering-Plough, Pfizer, Procter & Gamble, Roche and Sanofi-Aventis. The Association operates a Bridge Certification Authority which is cross-certified with the Federal Bridge Certification Authority (FBCA). SAFE-BioPharma Certificate Issuers include Citi Group, Verizon Business, Chosen Security, TransSped, J&J and BristolMyers Squibb. Vendors supporting the standard include Adobe, Aladdin Knowledge Systems, Arcot, ARX, Gemini Security Solutions, Hitachi, IBM, IDBS, Microsoft, MXI Security, NorthropGrumman, nCipher, SAIC, TriCipher, and Xyzmo. These organizations have extensive experience in providing digital identities uniquely linked to non-repudiable digital signatures to the U.S. Government, financial services organizations, the biopharmaceutical industry, researchers and others. The recommendations and comments that follow are based on our collective experience in developing an interoperable standard and providing trusted, secure digital identities and signatures to the biopharmaceutical and healthcare communities.

SAFE-BioPharma Association recommends that DEA revisit its analysis of the use of PKI-based digital identity certificates for e-prescribing. We recommend that the DEA require the use of digital signatures on e-prescriptions for controlled substances. The U.S. Government has a highly secure, interoperable digital identity system for Federal agencies and cross-certified entities through the Federal Bridge Certification Authority (FBCA). We recommend that this system provide the framework for DEA's rule for ePrescribing controlled substances. It is a widely available and supported system and it provides the level of security, non-repudiability,

interoperability, and auditability required by legislation covering the prescribing of controlled substances. Such a system would provide strong evidence that the original prescription was signed by a DEA-registered practitioner, that it was not altered after it was signed and transmitted, and that it was not altered after receipt by the pharmacist.

As the healthcare system moves into the digital world, there will be many requirements for high identity trust and non-repudiable signatures. There should be only one digital identity for each healthcare professional. The single digital identity could be used for ePrescribing, authentication to healthcare networks, access to health records, ordering diagnostic tests, and a myriad of electronic functions in multiple and disparate settings. Interoperable identity assurance and non-repudiable signatures are fundamental to the shift from slow, cumbersome paper-based processes to a fully electronic system and the potential improvements in healthcare quality that electronic media permit. Through the FBCA, these digital identities will interoperate with applications across government agencies, including the Department of Health & Human Services, Centers for Medicare and Medicaid Services, FDA, NIH, VA, Defense, Homeland Security as well as the private sector. The FBCA framework meets the requirements for privacy, security and confidentiality required by the healthcare sector for the exchange of sensitive healthcare information. It also meets DEA's requirements for identity trust assurance, non-repudiable digital signature, date-time stamping, record integrity and auditability in ePrescribing controlled substances.

SAFE-BioPharma recommends that the DEA require the use of an FBCA cross-certified PKI-based system on a pre-announced phased-in timetable. Such an approach would provide an incentive to application providers and others in the ePrescribing space to evolve their products in a way that would not create serious disruption and would not require wholesale immediate restructuring. Products could be revised to support the use of digital identity certificates and digital signatures as a normal upgrade. The sections of the rule that allow the use of digitally signed prescriptions by Federal Healthcare Agencies indicate the DEA recognizes that such use is possible where systems achieve the required level of interoperability. The use of PKI-based technology would help in driving interoperability with the Federal Government requirements in-place as a result of Homeland Security Presidential Directive 12 and the FIPS 201, Personal Identity Verification program.

Requiring the use of the existing FBCA-based trusted network would allow DEA to achieve the level of identity trust, non-repudiable digital signature, and record integrity that controlled substance ePrescribing law and regulations require. This approach is supported by the Technical Committee of Integrating the Healthcare Enterprise (IHE), the leading organization addressing healthcare issues, in a whitepaper specifically noted the following:

“Transactions are protected using point-to-point solutions like TLS or message level solutions like XML Encryption and XML Signature. These solutions ensure that the conversation is not intercepted or modified. These mechanisms can ensure that the systems involved are trustworthy to handle sensitive data. There are needs to provide a trusted security token that contains identity information that allows the service to authenticate the identity of the user related to the request. The valid security token

allows the service to make appropriate authorization decisions based on the subject of the token.”¹

The use of the FBCA trusted identity system is supported by its use for ePrescribing within the Federal Government healthcare system and by its use by the world’s leading pharmaceutical companies and their external partners. Additionally, many EU Member States, as part of their e-government initiatives, are moving to digital identity based solutions for many day-to-day government transactions between citizens and their respective governments.

Authentication using digital identity certificates is also supported by a recent GSA report. GSA conducted a cross organization authentication pilot across multiple Regional Health Information Organizations (RHIOs) with the Healthcare Information and Management Systems Society (HIMSS). It resulted in the following findings:

- Multiple RHIOs can agree and implement a common framework for the policies, procedures and standards for federated identity authentication across multiple use cases.
- The federal e-Authentication infrastructure is relevant and applicable to use-cases for RHIOs in diverse operational environments.
- PKI, as a standard for strong authentication, can be deployed uniformly across multiple RHIOs.
- The federal PKI and its trusted Federal Credential Service Providers can be leveraged for use in multiple use-cases across multiple RHIOs.
- For RHIOs, local registration authorities and local enrollment are viable for large-scale deployments to provide for strong authentication using federal e-Authentication components.
- Hardware tokens (i.e., smart cards, flash drives) are viable for RHIO deployment of Level 4 authentication assurance.
- The service was usable, tested and implemented regardless of the RHIO or HIE use-case realization.
- The GSA’s risk-assessment process for identification of the sensitivity level for information exchanged was learned and understood by the participants.²

We commend the DEA for its efforts in developing a proposed rule for ePrescribing of controlled substances. We recommend that DEA require the use of the existing FBCA identity trust network for ePrescribing. This network encompasses a growing series of trusted communities. It is well supported. And it is increasingly recognized as the highly trusted, secure interoperable digital identity across government and industry.

¹ **IHE IT Infrastructure Technical Framework White Paper 2006-2007, For Public Comment , Cross-Enterprise User Authentication (XUA), Version 2.0**, 2006-08-15, lines 120-127

² **HIMSS/GSA, National e-Authentication Project Whitepaper**, June, 2007 Copyright 2007 by the Healthcare Information and Management Systems Society

Specific Comments

1. Part: 1300

Proposed wording: *Hard token* means a cryptographic key stored on a special hardware device (e.g., a PDA, cell phone, smart card) rather than on a general purpose computer.

Suggested wording: *Hard token* means a cryptographic key stored on a special hardware device (e.g., a PDA, cell phone, smart card, **USB fob**) rather than on a general purpose computer. We also suggest the use of the term Key Storage Mechanism vice hard token as this is the more standard industry term in current use.

Rationale: Specifically allows USB devices which are used in lieu of smart cards in many applications.

2. Part: 1300

Proposed: None

Suggested: *Registration Agent (RA)* means a delegated party trained to perform Applicant identification and authentication (I&A) on behalf of the CA. The RA is responsible for Applicant I&A and certificate life cycle management activities and is the interface to the certificate authority (CA).

Rationale: Defines the role suggested in response to section 1311.105

3. Part: 1300

Proposed: None

Suggested: *Trusted Agent (TA)* means A person or Entity authorized to act as a representative of an Registration Agent in confirming Applicant identification during the registration process.

Rationale: Defines the role suggested in response to section 1311.105

4. Part: 1311.105(a)

Proposed: (a) Before permitting access to the electronic prescription system for signing controlled substance prescriptions, the service provider must receive a document prepared by an entity permitted to conduct in-person identity proofing listed in paragraph (b) of this section. If a practitioner wishes to electronically prescribe controlled substances in more than one State, the service provider must receive a document prepared by an entity permitted to conduct in-person identity proofing that indicates each of the State licenses and DEA Certificates of Registration. Such document shall be prepared either on the identity proofing entity's letterhead or other official form of correspondence or the service provider may design a form for use by the identity

proofing entity. Regardless of the format of the document, the document must contain all of the following information:

- (1) The name and DEA registration number, where applicable, of the entity which conducted the in-person identity proofing of the practitioner;
- (2) The name of the person within the entity who conducted the in-person identity proofing of the practitioner;
- (3) The name and address of the principal place of business of the practitioner whose identity is being verified;
- (4)(i) For each State in which the practitioner wishes to prescribe controlled substances electronically, the name of the State licensing authority and State license number of the practitioner whose identity is being verified, or ...
- (5) Except as provided in paragraph (a)(6) of this section, for each State in which the practitioner wishes to prescribe controlled substances electronically, the DEA registration number and date of expiration of DEA registration of the practitioner whose identity is being verified;
- (6) For individual practitioners who prescribe controlled substances using the DEA registration of the institutional practitioner, a statement by the institutional practitioner acknowledging the authority of the individual practitioner to prescribe controlled substances using the institution's DEA registration, and the specific internal code number assigned to the individual practitioner;
- (7) The type of government-issued photographic identification checked (e.g., the practitioner's driver's license, passport) and a statement that the photograph on the identification matched the person presenting the photographic identification;
- (8) The date on which the practitioner's in-person identity proofing was conducted;
- (9) The signature of the person within the entity who conducted the in-person identity proofing;
- (10) The signature of the practitioner who is the subject of the in-person identity proofing.

Suggested: (a) Before permitting access to the electronic prescription system for signing controlled substance prescriptions, the service provider must receive a document prepared by an entity permitted to conduct in-person (~~delete in-person~~) identity proofing listed in paragraph (b) of this section. If a practitioner wishes to electronically prescribe controlled substances in more than one State, the service provider must receive a document prepared by an entity permitted to conduct in-person (~~delete in-person~~) identity proofing that indicates each of the State licenses and DEA Certificates of Registration. Such document shall be prepared either on the identity proofing entity's letterhead or other official form of correspondence or the service provider may design a form for use by the identity proofing entity. Regardless of the format of the document, the document must contain all of the following information:

- (1) The name and DEA registration number, where applicable, of the entity which conducted the in-person (~~delete in-person~~) identity proofing of the practitioner;
- (2) The name of the person within the entity who conducted the in-person (~~delete in-person~~) identity proofing of the practitioner;
- (3) The name and address of the principal place of business of the practitioner whose identity is being verified;
- (4)(i) For each State in which the practitioner wishes to prescribe controlled substances electronically, the name of the State licensing authority and State license number of the practitioner whose identity is being verified, or ...

- (5) Except as provided in paragraph (a)(6) of this section, for each State in which the practitioner wishes to prescribe controlled substances electronically, the DEA registration number and date of expiration of DEA registration of the practitioner whose identity is being verified;
- (6) For individual practitioners who prescribe controlled substances using the DEA registration of the institutional practitioner, a statement by the institutional practitioner acknowledging the authority of the individual practitioner to prescribe controlled substances using the institution's DEA registration, and the specific internal code number assigned to the individual practitioner;
- (7) The type of government-issued photographic identification checked (e.g., the practitioner's driver's license, passport) and a statement that the photograph on the identification matched the person presenting the photographic identification;
- (8) The date on which the practitioner's in-person (~~delete in-person~~) identity proofing was conducted;
- (9) The signature of the person within the entity who conducted the in-person (~~delete in-person~~) identity proofing;
- (10) The signature of the practitioner who is the subject of the in-person (~~delete preceding in-person~~) identity proofing.

Rationale: While we realize the DEA's desire to have the strongest ID proofing available, we suggest that there are capabilities that use other than in-person verification that are as strong as in person. For instance, for medical professionals applying for SAFE-BioPharma identity certificates there are a number of processes that might be used, two of which require in-person verification and two of which rely on antecedent data based on previous in-person identity vetting.

In all cases, the initial request for a credential is made by a Requestor who is an employee of a SAFE-BioPharma Member company authorized by that company to nominate Applicants for a credential. The Requestor accesses the SAFE-BioPharma Registration Authority System (RAS) using their current digital credential. The RAS verifies the credential and allows the Requestor to access the system. The Requestor enters available data related to the Applicant, e.g. name, business address, business telephone number, business e-mail address for the nominated Applicant. The Requestor also selects the most appropriate form of I&A processing : notary, trusted agent, or antecedent. Both the Notary and Trusted Agent processes are in-person.

Risk: A fictitious identity might be created, or an identity stolen, to obtain a credential. Individuals may collude to create fictitious identities.

Risk reduction: SAFE-BioPharma does NOT issue credentials to members of the general public, be they medical professionals or other individuals. To obtain a SAFE-BioPharma credential and Applicant must be sponsored by a SAFE-BioPharma Member company or organization. Risk reduction occurs in that the Requestor and Approvers, in the SAFE-BioPharma system must be an appointed and trained employee of a SAFE-BioPharma Member company who has a valid SAFE-BioPharma digital certificate and has digitally signed a SAFE-BioPharma Subscriber Agreement that binds them to comply with the SAFE-BioPharma rule.

Access to the SAFE-BioPharma RAS is only possible using the digital certificate; user name and password are not allowed. Upon issuance, the SAFE-BioPharma certificate is downloaded to, and protected on a FIPS-140-2, level 3 USB hardware token that requires two factor authentications to access the certificate and private key. (NIST SP 800-63, Level 4 authentication) Risk is further reduced by applying a two-person rule to the process. The requirement for a Requestor and an Approver requires actions by two specific individuals, even in the case of the use of the antecedent process.

The next step in the process is the Approver, again a Member company employee who reviews the nomination for purposes of committing the company to pay for the certificate. To this point in time, the actual applicant may not even be aware that they are being nominated for a certificate. Risk of fraud is reduced by instituting a two-party process that requires both the Requestor and Approver to complete their actions prior to even notifying the Applicant. Upon approval of the nomination by the Approver, the system generates a one-time invitation code which is sent to the Applicant at the business e-mail address entered by the Requestor.

Risk: A fictitious identity might be created, or an identity stolen, to obtain a credential. Individuals may collude to create fictitious identities.

Risk reduction: See access requirements for the previous action. The same apply in this case. In addition, the nomination process required two actions prior to the initiation of the next step. Both the Requestor and Approver must complete their required actions prior to the system creating an invitation code for the Applicant. Both Requestor and Approver are SAFE-BioPharma Subscribers who are bound to the SAFE-BioPharma rule set. As Subscribers sponsored by their company, the company is liable for up to \$10M in case of fraudulent activity on the part of any sponsored Subscriber.

In the next step of the process, the Applicant receives the e-mail which includes data related to the process the Requestor selected for I& and the Invitation Code and a link to the RAS system. The Applicant clicks on the link and uses the unique, one-time Invitation code that was sent to their business e-mail address to access the RAS. The Applicant creates a Profile Password that the RAS uses to identify the Applicant at follow-on steps of the process. The Applicant reviews the information that was entered previously and completes additional information to create a personal profile in the system. When the profile is complete, the Applicant proceeds through one of the I&A processes.

Risk: Possible use of fraudulent identity to obtain digital certificate.

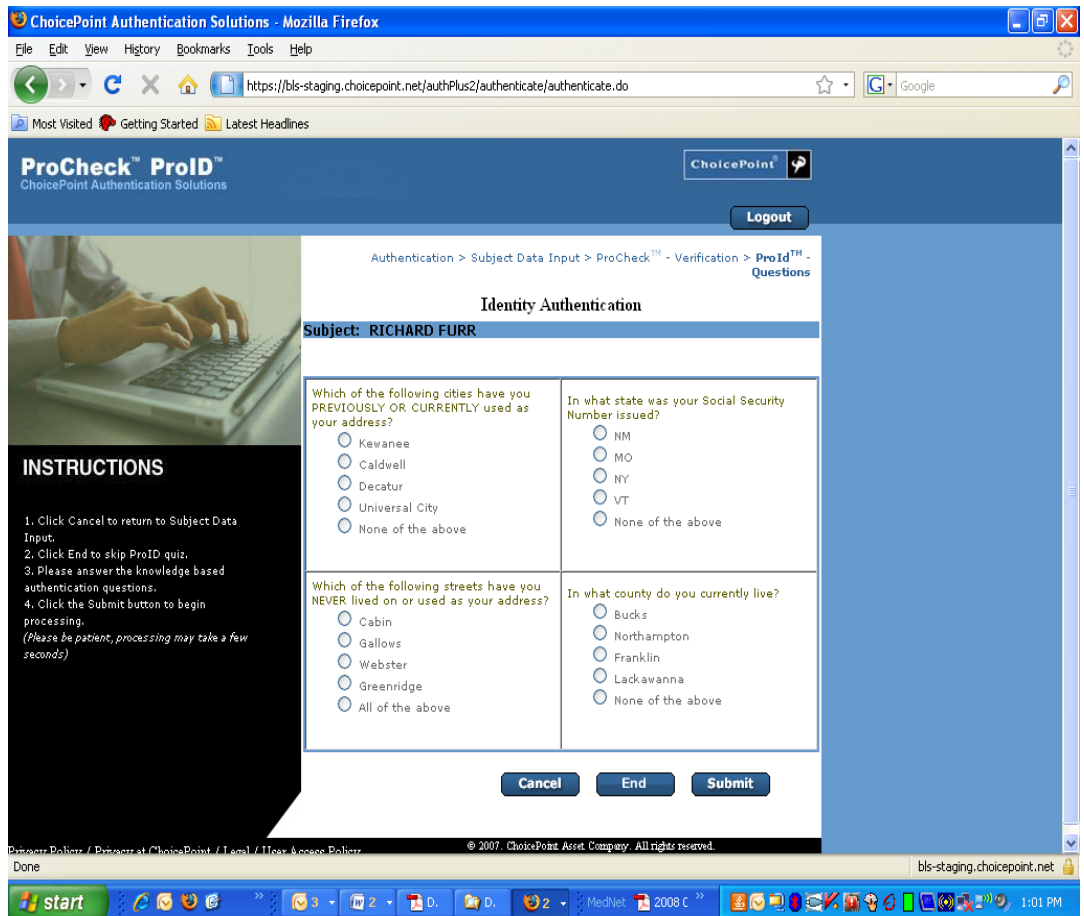
Risk Reduction: The invitation e-mail must go to an e-mail address that is entered by the sponsoring Requestor. This e-mail address must be in the business domain of the Applicant (in the case of medical professionals, the hospital, clinic or practice.) Only the Applicant can access the RAS and verify/modify the data entered by the Requestor to create their profile.

Depending on the process selected by the Requestor, the Applicant proceeds through one of the I&A processes. The possible choices are:

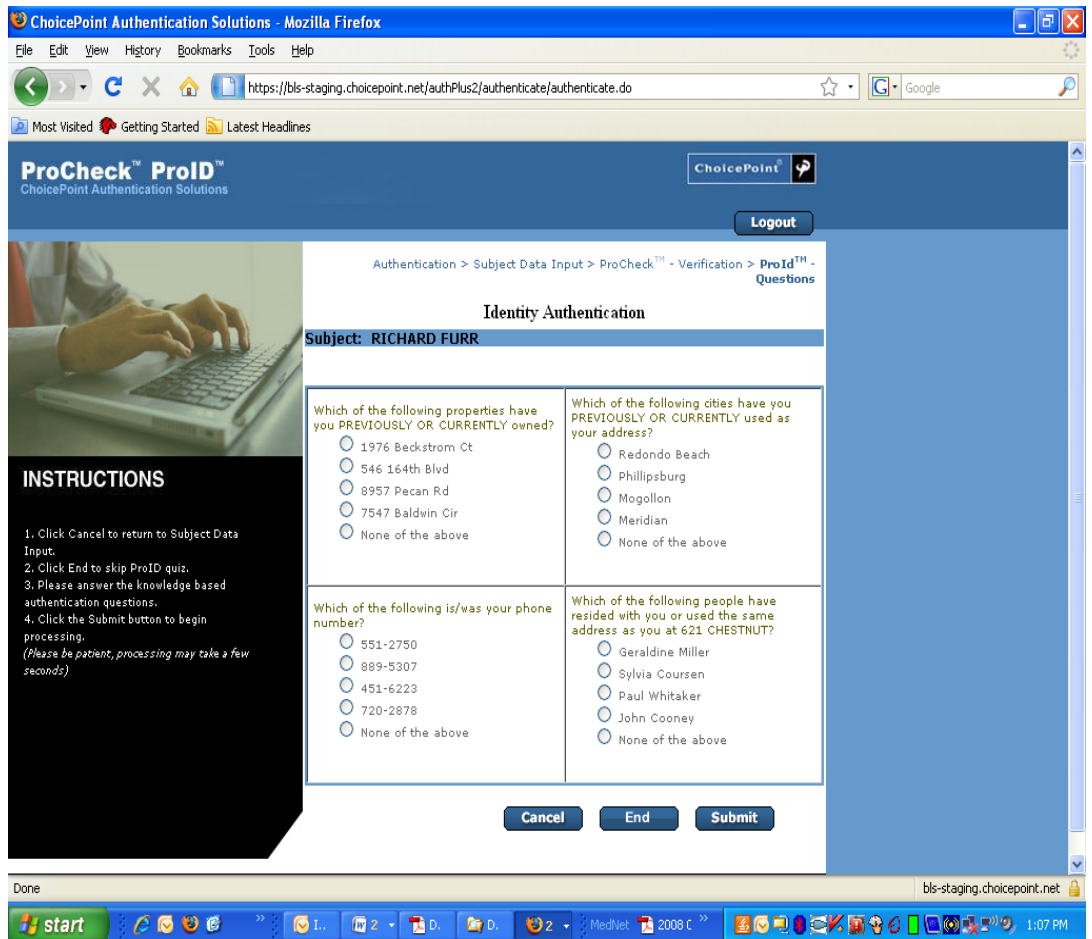
1. Trusted Agent face to face – The Trusted Agent (TA) is an employee of a Member Company, or other trusted third party, delegated and trained by SAFE-BioPharma to perform the processes required to verify Applicants’ identity according to the SAFE-BioPharma standard. The TA must also possess a valid SAFE-BioPharma digital certificate for accessing the RAS and also to apply their digital signature to the completed on-line I&A form. Acceptable forms of identity for this process include those that are required to be presented as part of the Federal Government Employment Eligibility (I9) process. Requirement includes at least one picture ID. If this ID is issued by a national Government Agency, one ID is all that is required. If the picture ID is issued by a State Government Agency, one additional form of ID from the I9 list is required. The TA enters pertinent information, e.g., document unique number, issuing agency, validity period in an on-line RAS form which is then maintained in the system for a period of 10.5 years. The TA digitally signs this form.
2. Notary face to face – This process is very similar to the Trusted Agent process except that the Applicant appears before a Notary and the I&A form is notarized. Either the Applicant or the Notary sends the completed, notarized form to the RA for review, scan and upload and maintenance. **If this process were approved by the DEA, we would require the notary to forward the form to reduce risk of any alteration or fraudulent activity post notarization.**
3. Bulk Load Antecedent – In the process a Member company approver creates an Excel .csv file with pertinent data for Member company employees which is uploaded to the RAS to begin the process. Identity data is based on I9 or other in person-based data that was developed and is maintained by the Member company HR or Security Departments. A key requirement of the ability to use such data is an additional requirement that the in-person identity verification upon which the data is based must include a presentation and verification of a picture ID. In all cases, the identity verification must also meet the requirements of the SAFE-BioPharma Certificate Policy and the data must be maintained by the company for the requisite 10.5 years. The process must also be controlled by a Standard Operating Procedure which has been reviewed and approved by SAFE-BioPharma. This process is subject to audit by SAFE-BioPharma.
4. Individual Antecedent - We anticipate this process would be the most frequently used by Practitioners. The process begins when a Member company Requestor nominates a Medical Professional for a certificate. The process was developed to support clinical trial investigators and their supporting sub-investigators and staff, as well as, medical professionals affiliated with National Health Information Networked Healthcare information Exchanges (HIE). Many of these doctors are either affiliated with DEA registered hospitals or clinics, or they may be affiliated with large individual practices. Not all are DEA registered, but many will be. As noted, SAFE-BioPharma was created by the biopharmaceutical industry with multiple goals. One primary goal is to reduce the number of “tokens” that medical professionals are required to manage. As noted by the DEA, many of these “tokens” are based on user name and password. A typical clinical trial investigator who works with multiple pharmas will have a token issued by each Pharma with which they work. Past audits have revealed that it is not unusual for an investigator to have from four to ten “tokens”, and when these are user name and password based, it is further not unusual

to find the user name and password written on yellow Post Its and affixed to the particular machines that were provided by the supported Pharma. With the increasing move to IT-based healthcare systems, e.g., electronic health records, e-prescribing, and other IT-based care systems, it is likely that authentication tokens will proliferate, thereby creating a token management nightmare. SAFE-BioPharma was created by the biopharmaceutical industry with one of its primary goals being the provision of a single strongly bound digital identity token to medical professionals. We believe our identity proofing and credential provisioning capabilities and structure would provide the security required by the DEA to support e-prescribing of controlled substances. The antecedent process developed for use by SAFE-BioPharma uses the identity vetting capabilities of ChoicePoint, an organization that also provides support to agencies of the Federal Government. The process developed by SAFE-BioPharma for use with licensed medical professionals (LMP) follows:

- a. The LMP accesses the RAS using the invitation code provided in the invitation e-mail and verifies the information entered by the Requestor. The Applicant further completes data to include:
 - i. Home address
 - ii. Medical license number
 - iii. Last four digits of their SSN
 - iv. Partial birth date (dd/mm).
- b. ChoicePoint uses these data to perform full identity discovery as follows:
 - i. Build and verify full SSN exists in public records, that holder is not deceased, and that the name and address match.
 - ii. Verify that medical license listed is valid (state license agencies require face to face identity vetting with picture ID. This meets requirements for picture ID in face to face situation.)
 - iii. Determine, based on other identification data that LMP has valid registration with DEA;
 - iv. Parse DMV records to determine verify DMV license status;
 - v. Parse mortgage and financial records to determine record status.
- c. If the identity cannot be confirmed, the Applicant is advised to access the RAS and provide full SSN and date of birth. If identity cannot be confirmed using these data, the Applicant is kicked out and moved to the notary process for identity verification.
- d. If identity is confirmed, ChoicePoint generates a set of seven (7) questions based on data derived from the record check. The answers to the questions are ones that should only be known to the specific individual whose records were checked. The Applicant is presented a list of five (5) questions similar to the following screen shot:



For the SAFE-BioPharma process, the Applicant receives an initial list of five (5) questions and must answer four (4) correctly. If the Applicant fails the first set, they are presented one additional chance.



If they pass, ChoicePoint creates a file that includes all data references that were parsed to identify the Applicant and this is maintained for future audit for a period of ten and one-half years. ChoicePoint then creates a pass/fail notice and a transaction code that is linked to the identity data file for audit purposes. The pass/fail notice and the transaction code are forwarded to the RA who proceeds to initiate the certificate issuance from the CA.

- e. If the Applicant fails the test a second time, they are forced into the Notary process.
- f. The RA sends a blank hardware token to the Applicant via courier (FedEx, UPS, etc) at the listed business address. The Applicant must sign a receipt for the package.
- g. The RAS generates an activation code e-mail that is sent to the Applicant at the e-mail address listed. The e-mail includes a link to the RAS.
- h. The Applicant access the RAS using their previously developed profile password (which they have been advised to remember, BUT not write down.)
- i. The applicant is presented the SAFE-BioPharma Subscriber Agreement which binds them to the SAFE-BioPharma rules and policies concerning use of their credential and clicks thru to affirm acceptance. (Upon completion of the certificate generation and download to the token, the Applicant will use their

newly generated credential to digitally sign the Agreement which is maintained in the RAS.)

- j. The Applicant enters the provided authentication code, creates a six character token pass phrase which is used to authenticate the user to the token and the system downloads the credential to the token. The credential is ready for use.

5. Part: 1311.105(b)

Proposed: (b) The following entities are permitted to conduct in-person identity proofing as described in paragraph (a) of this section:

- (1) The entity within a DEA-registered hospital that has previously granted that practitioner privileges at the hospital (e.g., a hospital credentialing office). The practitioner's privileges must be active and in good standing;
- (2) The State professional or licensing board or State controlled substances authority that currently authorizes the practitioner to prescribe controlled substances;
- (3) A State or local law enforcement agency.

Suggested: b) The following entities are permitted to conduct identity proofing as described in paragraph (a) of this section:

- (1) The entity within a DEA-registered hospital that has previously granted that practitioner privileges at the hospital (e.g., a hospital credentialing office). The practitioner's privileges must be active and in good standing;
- (2) The State professional or licensing board or State controlled substances authority that currently authorizes the practitioner to prescribe controlled substances;
- (3) A State or local law enforcement agency.

(4) A Notary Public, or Trusted Agent trained and delegated by a Registration Agent, or Registration Agent (RA) trained and delegated to perform identity verification by a Certificate Authority (CA) that is in a network of trust that is, cross certified, with the US Federal Bridge to issue at least medium hardware assurance level certificates. The CA must be a part of a closed system of trust which includes specific liability requirements to prevent fraudulent activities and mitigate risk related to fraudulent I&A activities. The RA, and supporting system, would require approval from the DEA to perform these activities.

(5) An antecedent data-based process, that meets the requirements of a CP managed by a CA/RA approved by the DEA as noted in (4) above.

Rationale: Provides alternate sources of identity vetting which could markedly reduce the impact of the process on the practitioner. The RA is responsible for conducting I&A according to the specific policies, procedures and requirements of the Certificate Authority. This would allow SAFE-BioPharma to submit its system for approval to the DEA. SAFE-BioPharma is the non-profit association created by the pharmaceutical industry to manage digital identity certificates for members of the industry and the healthcare industry. Among other stated goals of the association and its members is the ability to provision medical professionals with one strongly bound digital identity credential based on a strongly authenticated identity verification process. Further, NIST SP 800-63 states "The Identity Proofing and Certificate Issuance

processes of Certification Authorities cross-certified with the Federal Bridge CA under policies mapped to the Medium, Medium-HW, or High Assurance Certificate policies in [FBCA1] or Common-Auth, Common-SW, Common-HW, and Common-High Certificate Policies in [FBCA3] are deemed to meet the identity proofing provisions of Level 4.

The SAFE-BioPharma Bridge CA is cross certified with the US Federal Bridge at the Medium and Medium Hardware Assurance levels.

Risk: Similar to those identified in discussion of 1311.105.a.

Risk Mitigation: Same as identified in previous discussion.

6. Part § 1311.135 Electronic prescription system requirements: Revocation of access authorization.

Proposed:

- (a) The service provider must revoke the authentication protocol used to sign controlled substance prescriptions immediately upon receiving notification from the practitioner that a password or token has been compromised, lost, or stolen.
- (b) The service provider must revoke the authentication protocol used to sign controlled substance prescriptions on the expiration date of the practitioner's DEA registration unless the service provider determines that the registration has been renewed.
- (c) The service provider must check the DEA CSA database at least once a week and revoke the authentication protocol used to sign controlled substance prescriptions for each practitioner using the system whose registration has been terminated, revoked, or suspended.

Suggested:

- (a) The **credential or protocol** service provider must revoke the authentication protocol used to authenticate to the e-Prescription system used to sign controlled substance prescriptions immediately upon receiving notification from the practitioner that a password or token has been compromised, lost, or stolen.
- (b) **The e-Prescription service provider must update the e-Prescription system access control list (or similar mechanism) to prevent authorization of a Practitioner whose DEA registration has expired, been suspended or revoked unless the provider determines that the registration has been renewed.**
- (c) **The e-Prescription service provider must check the DEA CSA database at least once a week and must update the e-Prescription system access control list (or similar mechanism) to prevent authorization of a Practitioner whose DEA registration has expired, been suspended or revoked unless the provider determines that the registration has been renewed.**

Rationale: The protocol provided to the Practitioner may be used for other healthcare purposes. If the "protocol" is a digital identity certificate, as we propose, that is provided by a third party, such as SAFE-BioPharma, that certificate could be used for other legitimate healthcare purposes, including authentication to other systems and infrastructures across the healthcare space. It

could also be used to apply digital signatures to clinical and other documents. The digital identities provided by SAFE-BioPharma, as noted, provide the capability to serve as the single identity for medical professionals and to replace the multiple weaker identity forms currently in use. The requirement to revoke as proposed would defeat the purpose of these strongly authenticated identity credentials.

Placing the burden to control access to systems is not an undue hardship on the e-Prescription system providers. Requiring these providers to control access to their systems via the access control mechanism is something they already must do, regardless of the authentication protocol.

As defined in various studies and whitepapers, digital identity management is built upon “the Three A’s,” two of which are defined as:

Authentication

The confirmation that a user who is requesting services is a valid user of the network services requested. Authentication is accomplished via the presentation of an identity and credentials. Examples of types of credentials are [passwords](#), [one-time tokens](#), [digital certificates](#), and phone numbers.⁴

“Electronic authentication (E-authentication) is the process of establishing confidence in user identities electronically presented to an information system.”⁵ There are a number of methods that may be used for authentication; however the use of Security Assertion Markup Language (SAML) assertions is growing in application. SAML is an XML standard for exchanging authentication and authorization data between security domains, that is, between an identity provider (a producer of assertions) and a service provider (a consumer of assertions). SAML is a product of the OASIS Security Services Technical Committee. The National Institute of Standards and Technology (NIST) identifies four levels of authentication assurance based on the level of identity authentication, types of identity tokens recommended and the number of factors used in the authentication scheme, each increasingly more secure than the previous.

Just as there are multiple levels of assurance, there are two types of authentication schemes: single-factor and two-factor. Single-factor schemes, characterized by the use of user names and passwords, i.e. something you know, are notoriously simple for hackers and identity thieves to break and compromise. This vulnerability prompted the Federal Financial Institutions Examination Council to issue guidance to the American banking system to strengthen the security of their website authentication schemes by the end of 2006. While this guidance fell short of mandating a move away from single-factor authentication, it strongly suggested they move to two-factor authentication.

⁴ The Minnesota Privacy and Security Project. Minnesota Department of Health, *A Framework of Principles and Resources for Addressing the Four A's*. April 2007.

⁵ NIST SP 800-63, *Electronic Authentication Guideline*, September 2004

In order to understand two-factor authentication, it is important to understand the three methods by which people authenticate themselves to digital systems. There are three universally recognized factors for authenticating individuals:

- 'Something you know', such as a [password](#), [PIN](#), an [out of wallet](#) response, shared secret, questions that require a specific user's knowledge to answer or user-selected images identified from a pool of images.
- 'Something you have', such as a [mobile phone](#), [credit card](#), USB, [security token](#) or password-generating token.
- 'Something you are', such as a fingerprint, voice, keystroke, a [retinal scan](#) or other [biometric](#).

Authorization

Authorization is the granting of specific types of [service](#) (including "no service") to a user, based on their authentication, the services they are requesting and the current system state.

Authorization may be based on restrictions; for example, time-of-day restrictions, physical location restrictions or restrictions against multiple [logins](#) by the same user. Authorization determines the nature of the service which is granted to a user.⁶

We suggest that these are two separate functional processes and that the intent of the DEA, management of authorization to electronically sign the prescription, can be managed via the authorization process mechanisms inherent in e-Prescription systems. This suggested change will not require revocation of the authentication protocol, but will provide the needed strength to prevent access to such systems at the point it should be exercised.

Risk: Rogue Practitioners could collude with systems administrators of e-Prescription system service providers to circumvent the requirement to revoke access rights to the system.

Risk Mitigation: The requirement for e-prescription service providers to verify the DEA registration as cited in subparagraph (c) and the security audit requirements of Section 1311.145 should be sufficient to discover any such incidents.

⁶ http://en.wikipedia.org/wiki/AAA_protocol