California HealthCare Foundation

June 2014

Issue Brief

Proceed with Care: Tips for Providers Starting E-Prescribing of Controlled Substances

Introduction

Electronic prescribing (e-prescribing) has high potential for improving the efficiency and cost effectiveness of prescription transactions while improving the quality of patient care. However, its adoption and use in California has lagged other states. In 2013, California ranked 48th among the states and the District of Columbia on Surescripts Safe-Rx Ranking.[1]

In 2012, the California HealthCare Foundation (CHCF) identified several opportunities for advancing e-prescribing in California. Among them are pilot projects aimed at the adoption of new standards including e-prescribing for controlled substances (EPCS).[2]

Prescriptions for controlled substances account for approximately 11% of total prescriptions and until recently were not permitted to be transmitted electronically. In March 2010, the US Drug Enforcement Administration (DEA) issued an Interim Final Rule (the Rule) permitting electronic prescribing of controlled substances, subject to stringent security and audit requirements.[3] The basis for DEA authority is the Comprehensive Drug Abuse Prevention and Control Act of 1970, also known as the Controlled Substances Act (CSA). The Act "…mandates that DEA establish a closed system of control for manufacturing, distributing, and dispensing controlled substances."[4] In practice, this means that anyone involved in any of these activities must "register" with the DEA.

What Is E-Prescribing?

E-prescribing is generally comprised of these functions:

- Computer-based generation of a prescription
- Electronic transmission to a pharmacy
- Exchange of any renewal requests and responses between the prescriber and pharmacist
- Communication of pharmacy eligibility, benefit, formulary, and medication history from payers to prescribers

DEA registrants, such as physicians, dentists, nurse practitioners, and hospitals, have the primary responsibility for complying with the Act. They must use e-prescribing application providers (EHR/eRx software vendors) that satisfy the Act's requirements. In addition, registrants must undergo formal identity-proofing and must use a two-factor authentication protocol to sign each prescription. Pharmacies, health information networks (such as Surescripts), and health IT vendors must also comply with these requirements.

The DEA Rule for the e-prescribing of controlled substances is designed to insure that:

- Only DEA registrants or their permitted designees may be granted the authority to sign controlled substance e-prescriptions.
- The method used to authenticate a practitioner to the e-prescribing system must ensure that the practitioner cannot repudiate the prescription.
- The e-prescribing records must be reliable enough to be used in legal actions.
- The security systems used by any e-prescribing application must prevent the possibility of unauthorized creation or alteration of controlled substance prescriptions.[5]

The following requirements in the Rule require particular attention from provider organizations:

- Individual practitioners must meet specific requirements related to identity proofing, the issuance of two-factor authentication credentials, and the setting of logical (computer) access controls to EPCS applications.
- E-prescribing application providers (such as EHR vendors whose products support EPCS) must submit their EPCS functionality to a "third-party audit" to ensure compliance with the Rule.
- The EPCS functionality must include a "two-factor authentication" protocol that the practitioner must complete to electronically sign each controlled substance prescription.

In 2012 and 2013, CHCF awarded grants to three provider organizations to implement EPCS in compliance with the Rule.[6] These pilots produced a number of findings. It was learned, for example, that the required two-factor authentication protocol could be successfully integrated with e-prescribing functionality. However, issues were raised around ensuring that identity proofing and the integration of two-factor authentication applications and devices meet the Rule. These issues are discussed below, along with recommendations for provider organizations and practitioners to address them.[7]

Identity Proofing, Issuance of Two-Factor Authentication Credentials, and Setting Logical Access Controls

Prior to implementing EPCS functionality, practitioners must demonstrate that they are who they say they are (identity proofing). The individual is then issued two-factor authentication credentials and is explicitly granted access to the EHR/eRx EPCS functionality (called logical access controls).

The Rule describes two approaches to doing this: (1) for individual practitioners being authorized to use the EPCS functionality of an institutional practitioner, such as a hospital or clinic that is, itself, a DEA registrant; (2) for individual practitioners who are independent of an institutional practitioner, such as a physician in a solo or small group practice.

Figure 1 summarizes the processes defined by the Rule for identity proofing and issuance of authentication credentials in both of these cases. Figure 2 displays the processes defined by the Rule for granting logical access controls for EPCS in both of these cases. (See pages 3 and 4 respectively.)

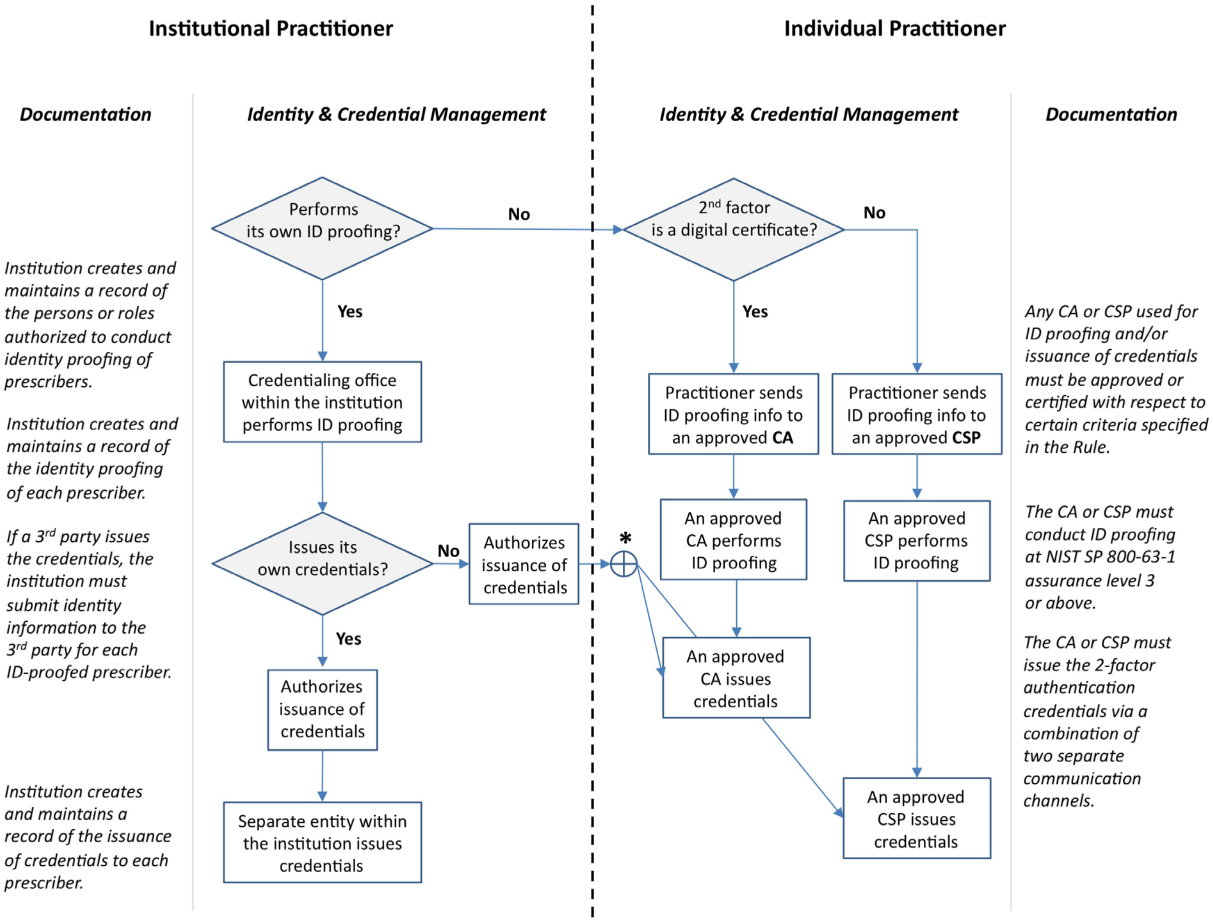
These processes are complex, and they also vary depending on the approach pursued. Therefore, it is important for provider organizations and individual practitioners to determine which approach is applicable to them and to carefully plan their processes, workflows, and resources accordingly.

For example, individual practitioners granted access to an institutional practitioner's EPCS application must be identity proofed in person. Identity proofing may be conducted by the institution's credentialing office and the institution may issue the two-factor authentication credential directly. In contrast, for individual practitioners, "remote" identity proofing is permitted and the granting of two-factor authentication credentials is conducted by federally recognized credential service providers (CSPs) or certification authorities (CAs).

CHCF has published a set of how-to guidelines to assist practitioners to understand the Rule and to correctly implement either of these approaches.[8]

It is important to note that compliance is dependent on the actions taken by practitioners and/or

Figure 1. Summary of Processes for Identity Proofing and Issuance of Two-Factor Authentication Credentials for EPCS


Institutional Practitioner
Individual Practitioner
Documentation
Identity & Credential Management
Identity & Credential Management
Documentation
Performs its own ID proofing?
No
Yes
2nd factor is a digital certificate?
No
Yes
Institution creates and maintains a record of the persons or roles authorized to conduct identity proofing of prescribers.
Credentialing office within the institution performs ID proofing
Institution creates and maintains a record of the identity proofing of each prescriber.
Practitioner sends ID proofing info to an approved CA
Practitioner sends ID proofing info to an approved CSP
Any CA or CSP used for ID proofing and/or issuance of credentials must be approved or certified with respect to certain criteria specified in the Rule.
If a 3rd party issues the credentials, the institution must submit identity information to the 3rd party for each ID-proofed prescriber.
Issues its own credentials?
No
Authorizes issuance of credentials
*
An approved CA performs ID proofing
An approved CSP performs ID proofing
The CA or CSP must conduct ID proofing at NIST SP 800-63-1 assurance level 3 or above.
Yes
Authorizes issuance of credentials
An approved CA issues credentials
The CA or CSP must issue the 2-factor authentication credentials via a combination of two separate communication channels.
Institution creates and maintains a record of the issuance of credentials to each prescriber.
Separate entity within the institution issues credentials
An approved CSP issues credentials

*Depending on type of 2nd factor.

Note: CA = certification authority. CSP = credential service provider.

Source: Sujansky & Associates, LLC, "Guidelines for the Electronic Prescribing of Controlled Substances: Identity Proofing, Issuing Authentication Credentials, and Configuring Logical Access Controls," November, 2013, www.chcf.org. See also www.deadiversion.usdoj.gov.

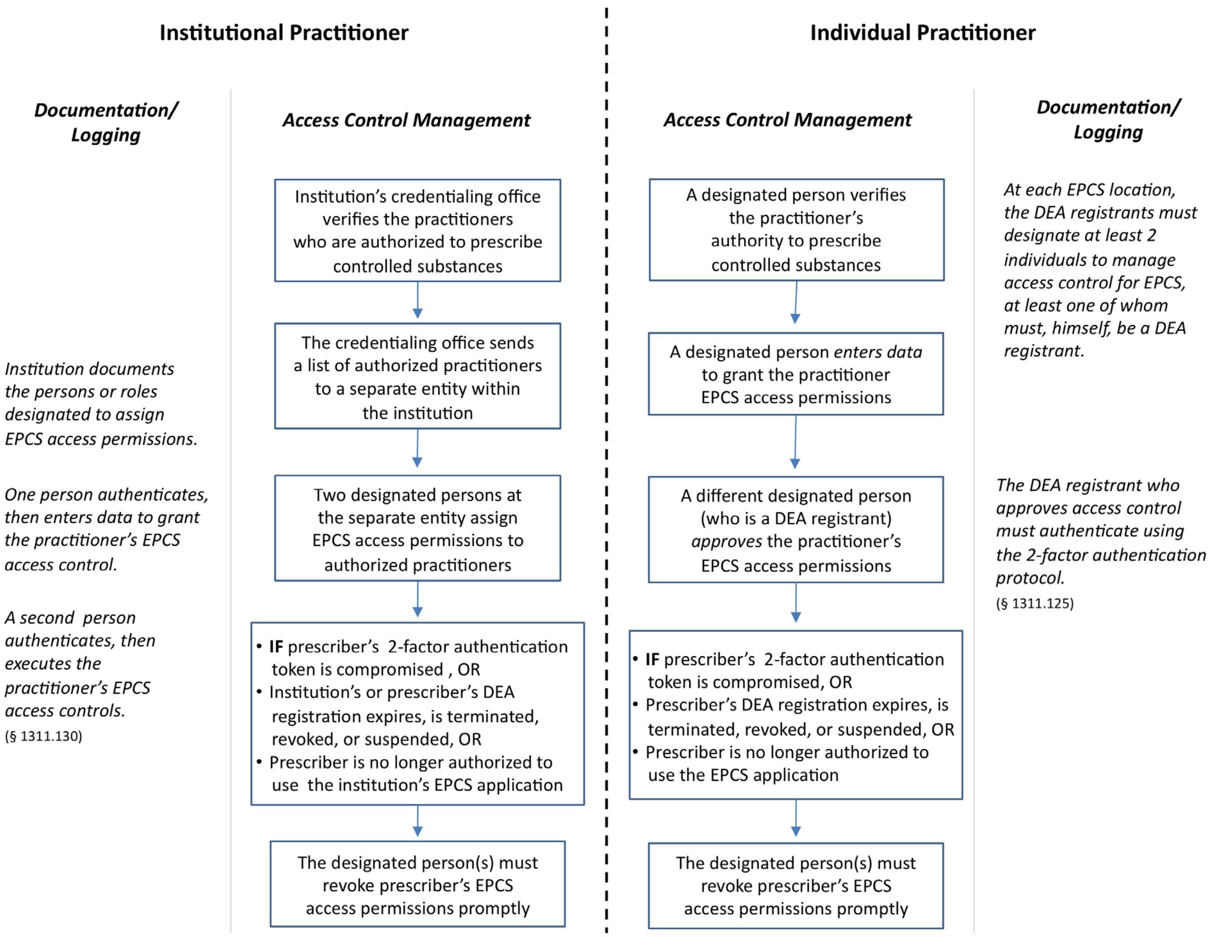
their institutions and the capabilities of the EPCS application software to document those actions. For example, the DEA notes that current procedures for setting logical access controls may need to be modified for individual practitioners. Absent EPCS, access to the EHR and its e-prescribing functionality may have been managed directly by the e-prescription application provider. However, the DEA requires that two individuals, one of whom is a DEA registrant, must authorize DEA registrants to use the EPCS functionality. This may require application providers to modify security controls and, more generally, to work closely with practitioners in implementing EPCS.

Since EPCS is just beginning to be adopted, it is not known how application providers will assist practitioners to conduct identity proofing, obtain two-factor authentication credentials, and set logical access controls.

Third-Party Audits for E-Prescribing Applications and the Integration of Two-Factor Authentication Applications and Devices

The DEA Rule addresses all aspects of creating and signing prescriptions for controlled substances, including requirements for internal audit trails, recordkeeping, the creation of monthly logs, and the reporting of auditable events to practitioners. The DEA recognizes that individual practitioners cannot be expected, on their own, to determine whether the e-prescribing software they are using complies with these requirements. Therefore the Rule requires that application providers must have a "third-party audit" of their EPCS application to insure compliance with

Figure 2. Summary of Processes Required for Setting Logical Access Controls for EPCS


Institutional Practitioner
Documentation/ Logging
Access Control Management
Institution's credentialing office verifies the practitioners who are authorized to prescribe controlled substances
The credentialing office sends a list of authorized practitioners to a separate entity within the institution
Institution documents the persons or roles designated to assign EPCS access permissions.
One person authenticates, then enters data to grant the practitioner's EPCS access control.
Two designated persons at the separate entity assign EPCS access permissions to authorized practitioners
A second person authenticates, then executes the practitioner's EPCS access controls.
(§ 1311.130)
• IF prescriber's 2-factor authentication token is compromised , OR
• Institution's or prescriber's DEA registration expires, is terminated, revoked, or suspended, OR
• Prescriber is no longer authorized to use the institution's EPCS application
The designated person(s) must revoke prescriber's EPCS access permissions promptly
Individual Practitioner
Access Control Management
Documentation/ Logging
A designated person verifies the practitioner's authority to prescribe controlled substances
At each EPCS location, the DEA registrants must designate at least 2 individuals to manage access control for EPCS, at least one of whom must, himself, be a DEA registrant.
A designated person enters data to grant the practitioner EPCS access permissions
A different designated person (who is a DEA registrant) approves the practitioner's EPCS access permissions
The DEA registrant who approves access control must authenticate using the 2-factor authentication protocol.
(§ 1311.125)
• IF prescriber's 2-factor authentication token is compromised, OR
• Prescriber's DEA registration expires, is terminated, revoked, or suspended, OR
• Prescriber is no longer authorized to use the EPCS application
The designated person(s) must revoke prescriber's EPCS access permissions promptly

Source: Sujansky & Associates, LLC, "Guidelines for the Electronic Prescribing of Controlled Substances: Identity Proofing, Issuing Authentication Credentials, and Configuring Logical Access Controls," November, 2013, www.chcf.org. See also www.deadiversion.usdoj.gov.

its requirements before it is used. As an alternative to the third-party audit, the EPCS application may be certified by an organization whose certification process has been approved by the DEA.[9]

The EPCS application must be re-audited or re-certified whenever a functionality related to controlled substances prescription requirements is altered, or every two years, whichever occurs first. The Rule also requires that the application provider make the audit or certification report available to any practitioner who is using or considering use of the application.[10]

In October, 2011, the DEA published a "clarification and notification" related to the Rule that stated that:

> "Any audit must include *all* of the applicable requirements for e-prescribing of controlled substances found in 21 CFR part 1311 *(Requirements for Electronic Orders and Prescriptions)* and not just section 1311.300 of part 1311….Thorough review and testing of all requirements is both required by the regulations and necessary to ensure secure and effective e-prescribing and dispensing of controlled substances in the interests of public health and safety."[11] (Emphasis added; section title added).

In view of this clarification, practitioners should exercise due diligence in reviewing third-party audit or certification reports as part of their determination that the EPCS process complies with the Rule. There are a number of situations in which practitioners should exercise special caution in determining whether compliance has been achieved. These are discussed below.

Two-Factor Authentication for EPCS

A DEA registrant who has been granted access to EPCS functionality must present *two of three factors* to sign each EPCS:[12]

- Something s/he *knows* (e.g., a password)
- Something s/he *has* (a hard token, e.g., proximity card, USB drive, one-time password device, smart card)
- Something s/he *is* (a biometric pattern, e.g., fingerprint, facial, iris)[13]

The two-factor protocol that is selected could be a password and a hard token, or a password and a biometric, or a hard token and a biometric. If one factor is a hard token, it must be separate from the computer to which the practitioner is granted access and must satisfy specific security standards set by other authorities that are cited in the Rule. If one factor is a biometric, it must comply with additional standards as described in the Rule.

To demonstrate the potential complexity associated with ensuring compliance with the Rule, two examples, one related to the use of hard tokens and the other related to the use of a biometric device, are described below.

Example 1. A provider organization uses, as one factor, *a hard token that generates a "one time only" passcode on a smart phone.*[14] To ensure compliance with the Rule, the security token software used by the smart phone must use a "cryptographic module" that is validated at Federal Information Processing Standard (FIPS) 140-2 Level 1 or higher. It is important to verify that this standard is met because the DEA indicates that "out of band" tokens that send the user a message over a separate channel, e.g., to a cell phone, are not acceptable.[15]

Example 2. A provider organization uses, as one factor, *a fingerprint (biometric pattern),* using a fingerprint reader that matches the practitioner's fingerprint, entered when the prescription is signed, to a database containing the practitioner's fingerprint that was collected during the identity proofing process. In order for this protocol to comply with the Rule, requirements for the biometric device that is used include:

- It must perform at a "false match rate" of .001 or lower.
- It must be tested by National Institute of Standards and Technology (NIST) or another DEA-approved government or non-governmental laboratory.
- If applicable, it must conform to Personal Identity Verification authentication biometric acquisition specifications pursuant to NIST Special Publication 800-76-1.
- It must store device ID data at enrollment (i.e., biometric registration) with the biometric data and verify the device ID at the time of authentication.
- It must protect the biometric data, match results, and/or non-match results when authentication is not local.

The Rule states that in order to provide practitioners or e-prescribing application providers with an objective appraisal of the biometric application provider's compliance with DEA requirements, it is requiring independent testing of those applications. This testing, the results of which must be made publicly available, is similar to the third-party audits or certifications of the e-prescribing and pharmacy applications that the DEA is also requiring.[16]

E-prescribing application providers bear primary responsibility for assuring that their EPCS applications comply with the requirements set forth in the Rule. However, DEA registrants are also responsible for ensuring that the EPCS application they are using complies with the requirements — and that registrants not electronically prescribe controlled substances if they learn that any aspect of EPCS functionality is not in compliance.[17] Therefore, practitioners and provider organizations should conduct their own "audits" of the EPCS process they are implementing, and consider the following types of questions:

1. Have they fully complied with the DEA requirements for identity proofing, issuance of two-factor authentication credentials, and setting logical access controls?

   These requirements are summarized in the guidelines noted above.[18] However, practitioners, especially those in solo or small practices, should consult with their EHR/eRx vendors for assistance or for recommendations regarding possible sources of assistance. While large practices and hospitals may have the resources to comply with these requirements, it is nevertheless recommended that they coordinate this activity with their EHR/eRx application providers.

2. Have they requested, received, and reviewed the third-party audit or certification report for the

e-prescribing application they are using or are considering using?

3. Have they requested, received, and reviewed these reports for the re-audits or re-certifications that the Rule requires every two years or when the e-prescribing application has been modified, for example, to adopt a new e-prescribing standard?

4. Are the two-factor authentication technology software and devices, which either they or the e-prescribing application provider has chosen, in compliance with the Rule?

   - Was this technology reviewed as part of the electronic application provider's third-party audit or certification? If not, has the security technology provider documented compliance with the Rule?

   - If one factor is a hard token, is it separate from the computer to which it is gaining access and does it meet at least the criteria of FIPS 140-2 Security Level 1 for cryptographic modules or one-time password devices?[19]

   - If one factor is a biometric (e.g., fingerprint), does the associated hardware and software comply with the requirements of the Rule?[20]

Conclusion

Implementation of e-prescribing for controlled substances is just beginning. Over time, the issues that have been identified, as well as other issues that may emerge, will likely be addressed and clarified by e-prescribing application providers, technology vendors, and the DEA. In the meantime, provider organizations, in partnership with their e-prescribing application providers, should exercise special care to ensure that all requirements of the DEA Rule are fully met.

Author

Ronald C. Wacker, independent consultant
ronwacker@yahoo.com

About the Foundation

The **California HealthCare Foundation** works as a catalyst to fulfill the promise of better health care for all Californians. We support ideas and innovations that improve quality, increase efficiency, and lower the costs of care. For more information, visit www.chcf.org.

Endnotes

1. Surescripts is the health information network that transmits the vast majority of electronic prescriptions. The Safe Rx Ranking reflects adoption use for all key aspects of e-prescribing including requests for patient eligibility information, responses to requests for patient medication history and the total number of prescriptions routed electronically; Surescripts, State Progress Reports, California at www.surescripts.com. Surescripts 2013 report available at www.surescripts.com (see p. 8).
2. "E-Prescribing in California: Why Aren't We There Yet?" CHCF Issue Brief, March 2012.
3. Department of Justice, Drug Enforcement Administration, "21 CFR Parts 1300, 1304, 1306, and 1311. Electronic Prescriptions for Controlled Substances; Final Rule," March 31, 2010 (see www.gpo.gov) For "Questions and Answers," see also www.deadiversion.usdoj.gov and www.deadiversion.usdoj.gov.
4. Electronic Prescriptions for Controlled Substances, see endnote 3, p. 16,237.
5. Electronic Prescriptions for Controlled Substances, p. 16,241.
6. "Pilot of the Electronic Prescribing of Controlled Substances," CHCF, February 2013, www.chcf.org.
7. "Private sector" provider organizations; different requirements apply to federal provider organizations.
8. Sujansky & Associates, LLC, "Guidelines for the Electronic Prescribing of Controlled Substances: Identity Proofing, Issuing Authentication Credentials, and Configuring Logical Access Controls," November, 2013, www.chcf.org. See also www.deadiversion.usdoj.gov.
9. See www.deadiversion.usdoj.gov for a listing of Approved Certification Processes.
10. Electronic Prescriptions for Controlled Substances, section 1311.300, Application Provider Requirements — Third Party Audits or Certifications, p. 16,318.
11. Federal Register, Volume 76, Number 202, pp. 64,813–8, October 19, 2011.
12. The DEA requires compliance with NIST 800-63-1, Level 3, which requires two authentication factors (Electronic Prescriptions for Controlled Substances, p. 16,253); See also, Electronic Authentication Guideline, Recommendations of the National Institute of Standards & Technology, NIST Special Publication 800-63-1, December 2011 for a discussion of security assurance levels, tokens, risks, and risk mitigation factors.
13. The DEA notes that, based on a 2009 HIMSS security survey, 18% of 196 health care systems surveyed used biometrics as a tool to provide security for electronic patient data and that 36% intended to do so. Also, the DEA notes that the HIMSS survey also found that 33% of those surveyed already use two-factor authentication for security. (Electronic Prescriptions for Controlled Substances, p. 16,250).
14. See, for example, Symantec's "VIP Access for Mobile," at www.symantec.com.
15. Electronic Prescriptions for Controlled Substances, pp. 16,252–3. FIPS 140-2 can be found at www.nist.gov.
16. Electronic Prescriptions for Controlled Substances, p. 16,251.
17. Electronic Prescriptions for Controlled Substances, section 1311.102, Practitioner Responsibilities, p. 16,311.
18. See endnote 8.
19. Electronic Prescriptions for Controlled Substances, section 1311.115, Additional Requirements for Two Factor Authentication, p. 16,312.
20. Electronic Prescriptions for Controlled Substances, section 1311.116, Additional Requirements for Biometrics, pp. 16,312–3.