



Summary of DEA's Interim Final Rule on Controlled Substance E-Prescribing

On March 31, 2010, the Drug Enforcement Administration (DEA) issued an interim final rule (IFR) that would permit hospitals, health care providers, and pharmacies to use electronic prescriptions in the dispensing of controlled drugs (Schedules II, III, IV, V). Comments on the DEA's IFR are due by June 1, 2010. The IFR will become effective on June 1, 2010, unless the effective date is modified following Congressional review.

The IFR permits all DEA registrants (e.g., DEA authorized prescribers) to transmit electronic prescriptions to pharmacies for schedules II through V controlled substances using a compliant e-prescribing application. The IFR is similar to the DEA's June 2008 proposed e-prescribing regulation to a certain extent (e.g., requires stringent controls over the e-prescribing of controlled substances, including a two-factor authentication). The IFR includes many recommendations made by the American Medical Association (AMA) in response to the DEA's 2008 proposed rule, including: the need for more flexibility for identity proofing; allowing the use of digital certificates and signatures; and not mandating physician reviews of prescription logs.

It is important to note that the e-prescribing of controlled substances is an option—physicians may still dispense controlled substances through the use of written prescriptions, regardless of whether they choose to write controlled substance prescriptions electronically.

The following highlights the IFR's key requirements for controlled substance e-prescribing (which are described in more detail below):

- **Physicians have the option of e-prescribing controlled substances as of June 1, 2010, if they comply with specific requirements, as described below.**
- **Physicians must first undergo a verification process (either in person or remotely) in order to receive authorization to e-prescribe controlled substances.**
- **Physicians must set access controls in their office practice prior to e-prescribing controlled substances.**
- **Physicians must use a two-factor credential to e-prescribe controlled substances.**
- **Physicians can use their own digital certificate to sign e-prescriptions for controlled substances.**
- **Physicians are not required to review their prescription logs.**
- **Physicians must comply with notification requirements if they lose their hard token or if they discover that their security controls have been compromised.**
- **Physicians must use a compliant e-prescribing application in order to e-prescribe controlled substances.**

Identity Proofing and Access Controls

Individual Physicians—for individual physicians in private practice, identity proofing (verifying that the authenticated user is who he/she claims to be) must occur by an authorized third party that will, after verifying the physician's identity, issue the authentication credential to the authorized prescriber. The DEA is requiring physicians to apply to certain federally approved credential service providers (CSPs) or certification authorities (CAs) to obtain their authentication credentials or digital certificates. These CSPs

or CAs will be required to conduct identity proofing at National Institute of Standards and Technology (NIST) SP 800-63-1 Assurance Level 3, which allows either in-person or remote identity proofing. Once a federally approved CSP or CA has verified the identity of the prescribing physician, the CSP or CA will issue the necessary authentication credential. Once the authentication credential is issued to the physician, logical access controls must be set (verifying that the authenticated user has the authority to perform the requested operation).

Logical access controls may be by user or role-based; that is, the e-prescribing application may allow permissions to be assigned to individual users or it may associate permissions with particular roles (e.g., physician, nurse), then assign each individual to the appropriate role. Access control must be handled by at least two people within a practice, one of whom must be registered with the DEA (e.g., DEA authorized prescriber). In other words, the validation process needs to be a two person step—someone other than the prescriber needs to authenticate the prescriber.

Institutional practitioner (e.g., hospital)—the DEA is allowing, but not requiring, institutional practitioners to conduct identity proofing in-house as part of their credentialing process (e.g., a hospital credentialing office). At least two people within the credentialing office must put together a list of individuals to be granted access control. This list must be sent to a separate department (e.g., the information technology department), which will use it to issue authentication credentials and enter the logical access control data. As with private practices, two individuals will be required to enter and approve the logical access control information. Institutional practitioners may require registrants and those exempted from registration to obtain identity proofing and authentication credentials from the same CSPs or CAs that individual physicians use. The institutional practitioner may also conduct the identity proofing in-house, and then provide the information to these CSPs or CAs to obtain the authentication credentials. An institutional practitioner that elects to conduct identity proofing must retain a record of the identity-proofing and issuance of the credential.

Two-Factor Authentication

Authentication is information (e.g., PINs, passwords, biometrics) that is used to verify a person's identity for security purposes. For example, ATMs use two-factor authentication—something you know (a personal identification number (PIN)) and something you have (bank card). According to the IFR, e-prescribers for controlled substances would have to prove their identities by using two out of three factors: something you know (e.g., passwords), something you have (e.g., hard token stored separately from the computer being accessed), or something you are (e.g., biometrics such as a fingerprint or iris scan). The DEA is allowing the use of a biometric as a substitute for a hard token or a password. If a biometric is used it may be stored on a computer, a hard token, or a biometric reader. The government lists certain biometric technologies it has tested and rated at: Biometric <http://fingerprint.nist.gov>, <http://face.nist.gov>, and <http://iris.nist.gov>. If a hard token is used, it must be a cryptographic device or a one-time-password device that meets Federal Information Processing Standard 140-2 Security Level 1, and it must be stored on a device that is separate from the computer in use (e.g., smart card).

Public Key Infrastructure (PKI) and Digital Certificates

PKI is a set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates. A digital certificate is an authorized digital identity that contains certain information used to verify that the owner sending a message is who he/she claims to be, and to provide the receiver with the means to encode a reply. The IFR allows a physician to use his/her own digital certificate to sign e-prescriptions for controlled substances. If the physician and his/her e-

prescribing application provider wish to do so, the two-factor authentication credential can be a digital certificate specific to the physician that the physician obtains from a Certification Authority that is cross-certified with the Federal Bridge Certification Authority at the basic assurance level.

Signature and Transmission Requirements

The e-prescribing application may allow the prescribing physician or his/her agent to enter data for a controlled substance prescription, provided that only the physician may sign the prescription. The IFR does not require signing and transmission to occur at the same time. The e-prescribing application will apply a digital signature to and archive the controlled substance prescription information when the physician completes the two-factor authentication protocol. Alternatively, the physician may sign the controlled substance prescription with his/her own private key. The DEA expects that most prescriptions will be transmitted as soon as possible after signing, but recognizes that physicians may prefer to sign prescriptions before office staff add pharmacy or insurance information. In long-term care facilities, nurses may need to transfer information to their records before transmitting. By having the application digitally sign and archive at the point of two-factor authentication, physicians and electronic applications will have more flexibility in issuing and transmitting electronic prescriptions. Prior to transmitting the prescription, the system must present a statement that the physician understands he/she is signing the prescription (legal signature). If the physician does not then perform the signature function, the prescription cannot be transmitted.

Printed Copies of Prescriptions After Transmission and Faxed Prescriptions

The IFR allows printing of a copy of a transmitted prescription, receipt, or other record, provided that the copy is clearly labeled: "Copy only – not valid for dispensing." The copy should state that the original prescription was sent to [pharmacy name] on [date/time] and that the copy may not be used for dispensing. Printed copies of transmitted prescriptions may not be signed. A provision is also included in the IFR that the e-prescribing application may print a prescription for signing and dispensing if transmission fails. The DEA requires that these original prescriptions include a note to the pharmacy that the prescription was originally transmitted to a specific pharmacy, but that the electronic transmission failed. The IFR notes that a faxed prescription is considered a paper prescription and must be manually signed. It is not permissible to electronically generate and fax a controlled substance prescription without the physician manually signing it.

Notification Required to Avoid Liability

According to the IFR, the physician must retain sole possession of the hard token, where applicable, and must not share the password or other knowledge factor, or biometric information, with any other person. The physician must not allow any other person to use the token or enter the knowledge factor or other identification means to sign prescriptions for controlled substances.

The IFR also indicates that a physician must notify the individuals designated to set logical access controls and the DEA within one business day of discovery that his/her hard token has been lost, stolen, or compromised, or that the authentication protocol has been compromised. A physician must also notify individuals designated to set logical access controls and the DEA within one business day of discovery that one or more prescriptions that were issued under a DEA registration held by that physician were prescriptions the physician had not signed or were not consistent with the prescriptions he/she signed. A physician who fails to comply with these requirements may be held responsible for any controlled substance prescriptions written using his/her two-factor authentication credential. The IFR also indicates that a physician must cease immediately from using a malfunctioning and/or non-compliant e-prescribing application.

E-Prescribing Application and Audit Requirements

E-prescribing applications must be compliant with the IFR requirements and the e-prescribing application provider must undergo a third-party audit. The application provider must either hire a qualified third party to audit the application or have the application reviewed and certified by an approved certification body. The auditor or certification body will issue a report that states whether the application complies with the DEA's requirements. The application provider must provide a copy of the report to physicians to allow them to determine whether the application is compliant.

The IFR states that any person designated to set logical access controls is responsible for determining whether any identified auditable event represents a security incident that compromised or could have compromised the integrity of the prescription records (e.g., an unauthorized person attempting to sign or alter a prescription would be an auditable event; a pharmacist annotating a record to indicate a change to a generic version of a drug would not be). The applications must run the internal audit function daily to identify any auditable events. When one occurs, the application must generate a readable report for the physician or pharmacist. If a physician or pharmacy determines that there is a potential security problem, they must report it to the DEA within one business day. The IFR also indicates that although physicians are not expressly required under the DEA regulations to report suspected diversion of controlled substances to the DEA, all DEA registrants have a duty to provide effective controls and procedures to guard against theft and diversion of controlled substances. The DEA expects physicians to ensure that information regarding potential diversion is provided to law enforcement authorities, where circumstances so warrant.

Monthly E-Prescribing Logs

The IFR requires that the e-prescribing application automatically provide the physician with a monthly log of the physician's controlled substance e-prescriptions. The e-prescribing application is also required to provide physicians a log upon request. The IFR also requires the application to allow the physician to specify the time period for log review, and to allow the physician to request and obtain a display of up to a minimum of two years of prior e-prescribing of controlled substances and to request a display for particular patients or drugs. The IFR does not require the physician to review the logs or indicate his/her review of the logs. Rather, the logs are intended to serve as a tool to help physicians monitor and detect fraud or inappropriate activity.

Two Year Recordkeeping Requirement

The IFR requires records related to controlled substance e-prescriptions to be retained electronically for two years from the date of their creation or receipt. This record retention requirement does not preempt any longer period of retention which may be required now or in the future, by any other Federal or State law or regulation, applicable to physicians.

E-prescribing Controlled Substances is an Option

The IFR emphasizes that the e-prescribing of controlled substances is in addition to, not a replacement of, existing requirements for written and oral prescriptions for controlled substances. The IFR provides a new option to prescribing physicians and pharmacies. It does not change existing regulatory requirements for written and oral prescriptions for controlled substances.

Prescribing physicians will still be able to write, and manually sign, prescriptions for Schedule II, III, IV, and V controlled substances, and pharmacies will still be able to dispense controlled substances based on those written prescriptions and archive those records. A physician or his/her agent can still use an

existing e-prescribing application that does not comply with the IFR to prepare a controlled substance prescription, so that an electronic health record (EHR) and other e-prescribing functionality may be used, and print the prescription for manual signature by the physician. Such prescriptions are considered paper prescriptions and subject to the existing requirements for paper prescriptions.