September 25, 2008

Michele M. Leonhart
Acting Administrator
Drug Enforcement Administration
DEA Federal Register Representative/ODL
8701 Morrissette Drive
Springfield, Virginia 22152


Dear Administrator Leonhart:

The Medical Group Management Association (MGMA) is very supportive of health information technology (HIT) solutions for medical groups as a method of improving clinical performance and streamlining administrative functions. As a critical component of HIT, electronic prescribing (e-prescribing) offers many potential benefits to both patients and providers. Despite the promise of e-prescribing, however, several significant challenges remain before this technology can be utilized fully by physicians and pharmacies nationwide. One of these challenges is the current prohibition against the e-prescribing of controlled substances. We are pleased that the Drug Enforcement Administration (DEA) has recognized the need to permit the e-prescribing of controlled substances and we offer the following comments in the hope that the DEA, in concert with the industry, can develop a workable regulation to allow practices to fully utilize this important technology.

MGMA, founded in 1926, is the nation’s principal voice for medical group practice. MGMA’s more than 21,500 members manage and lead 13,500 organizations, in which more than 270,000 physicians provide more than 40 percent of the health care services delivered in the United States. MGMA’s core purpose is to improve the effectiveness of medical group practices and the knowledge and skills of the individuals who manage and lead them.

As evidence of our strong commitment to the use of technology to improve clinical care and administrative functions, MGMA and several leading provider organizations have founded the Center for Improving Medication Management and recently collaborated with a number of leading professional medical societies to develop the www.GETRXConnected.com website and educational campaign. MGMA is also a co-sponsor of the Centers for Medicare & Medicaid Services E-Prescribing National Summit.
MGMA is strongly supportive of health information technology and we believe that moving the nation’s medical practices to e-prescribing, including the e-prescribing of controlled substances, will greatly improve patient care and significantly streamline administrative processes.

**E-prescribing: the Value Proposition**

E-prescribing offers a number of important opportunities to prescribers and pharmacists. From the clinical perspective, e-prescribing can permit the clinician and pharmacist to review allergies, drug-drug interactions and contraindications that, if not identified, could have an adverse impact on the patient. E-prescribing can also facilitate enhanced administrative functions including access to information related to formulary and benefit management. As well, fully integrated e-prescribing systems have the potential to limit the time prescribers and pharmacists spend on formulary management issues, create efficiencies in the delivery of health care, and provide enhanced access to electronic patient health information.

**Current Paper Environment**

Paper prescriptions are still the most widely used method of prescribing and most typically the method for prescribing controlled substances. Many clinicians rely on paper prescriptions because they are a simple and fast method. However, issues with deciphering illegible handwriting continue to plague the medical profession.

In most care settings today, preventing prescribing errors is dependent on a system of downstream inspection, usually by the dispensing pharmacist. While pharmacists are remarkably good at catching prescribing errors—they make more than 150 million calls to physicians each year to discuss possible errors or otherwise clarify prescriptions—many errors still slip through this safety net.

In their landmark 2003 study, “The Value of Computerized Provider Order Entry in Ambulatory Settings,” the Center for Information Technology Leadership (CITL) suggests that more than 8.8 million Adverse Drug Events (ADEs) occur each year in ambulatory care, of which over 3 million are preventable. CITL also estimates that nationwide adoption of e-prescribing will eliminate nearly 2.1 million ADEs per year in the U.S. This would prevent nearly 1.3 million provider visits, more than 190,000 hospitalizations and more than 136,000 life-threatening ADEs, or about 14 preventable ADEs per ambulatory care provider per year.

**E-prescribing Benefits: Clinical**

Of the many significant benefits associated with e-prescribing, the most important of these is enhanced patient safety. In an e-prescribing environment, safety is increased due to the legibility and accuracy of the prescription. Additional safety benefits accrue when e-prescribing incorporates drug formularies and facilitates the automatic screening of drug-drug interactions and contraindications at the time the medication is prescribed. With e-prescribing, there are no more lost paper scripts that are never filled, as the prescription is sent directly to the pharmacy or as an electronic transaction.
Medication information conveyed via a paper prescription is not automatically stored; it must be re-entered by hand in the pharmacy system, and is not recorded efficiently in the clinician’s office. Paper itself is expensive to move and store. Use of hand written prescriptions also raises security issues, as paper prescriptions are relatively easy to forge. Of particular concern for controlled substances is altering of the prescription sig. It is all too easy to change “1” refill to “10” refills, with almost no way for the clinician or pharmacist to know. In addition, physical security of the prescription pads is a constant concern for practices. Unfortunately, many break-ins at practices and clinics, especially in urban areas, are done specifically to acquire prescription pads.

E-prescribing Benefits: Administrative

From an administrative perspective, e-prescribing allows practices to take advantage of several streamlined processes. Most systems are small and portable, allowing many practices their first foray into health information technology. Automated prescription renewals can reduce clinical and administrative time for prescription renewals and pharmacy call-ins and eliminate pharmacy call-backs due to illegible writing, generic checking or formulary problems.

The following are examples of how inefficient the current paper-based system is and how the adoption of e-prescribing can produce significant administrative savings for each industry stakeholder.

- **Expedited Refill Process.** E-prescribing allows practices to handle refill requests faster, with MGMA estimating reductions of 12 minutes per refill (from 15 minutes using paper to 3 minutes using e-prescribing) and reduced time when e-prescriptions are faxed instead of using the phone-- from 6 minutes per call to less than one minute per fax.

- **Pharmacy Callbacks Prescription Reworking.** Callbacks from pharmacies and the reworking of prescriptions in a paper environment add considerable cost to the system. By some estimates, pharmacies make more than 150 million calls to physician practices each year to discuss possible errors or otherwise clarify prescriptions. In a study conducted by MGMA, the time spent returning phone calls and following up on faxes costs a ten-physician practice, on average, $19,444 a year. This figure is based on time and cost associated with manually processing refills and resolving issues related to formulary as well as issues related to dosage and legibility. These figures do not include the additional costs associated with managing fax communications with pharmacies.

In an ideal situation, a physician who is fully e-prescribing will have information available up front on pharmacy eligibility, formulary, benefits, and patient medication history, making it much more likely that the pharmacist will receive a prescription that does not require a follow-up call. The prescription renewals authorization process can be streamlined with electronic prescribing, and e-prescribing can also significantly reduce the need for pharmacy staff to manually enter prescription information into their computer systems.
E-prescribing can dramatically reduce the burden of returning phone calls and tracking down faxes to clarify prescription information and authorize prescription renewals. A Brown University study on the prescription renewals process found that when an electronic system was used, the average prescriber time spent per day was cut in half, from 35 to 17 minutes, and the average staff time spent per day was cut in half from 87 to 43 minutes for the prescription renewals authorization process.

- Medication Adherence. The National Community Pharmacists Association reported that in 2007 nearly one third of new prescriptions were never filled. Designing a more efficient process of refilling prescriptions makes it easier for patients to adhere to their medications. In a recent study, SureScripts, Walgreens, and IMS Health reported an 11.21 percent increase in patients picking up a new medication when prescribers used e-prescribing versus relying on hand-delivered scripts. Medication adherence can also be enhanced by the decreased costs for patients as a result of the prescriber having access to real-time formulary information.

- Real-Time Information Availability. From a patient safety perspective, e-prescribing allows prescribers and practice staff to have the potential of accessing clinical decision support information such as patient medication history, formulary, benefits and pharmacy eligibility information, drug-drug interaction alerts and drug-allergy interaction alerts. This can result in a safer prescribing decision for the patient. E-prescribing also facilitates real-time availability of information on formulary, benefits, and medication history. Health plans, health systems, and ultimately employers save money when prescribers stay on formulary and prescribe lower-cost medications.

- E-prescribing Integration with EHRs. One of most exciting benefits of e-prescribing comes from its integration with a practice electronic health record (EHR). Robust systems allow physicians to check the medication against other medications that the patient is taking, along with other allergies that the patient may have. In addition, an integrated system will document and store all prescriptions in the system for access by all authorized clinicians. One problem with the current system is that controlled substance prescriptions must be hand written, and then reentered in the EHR.

- Pharmacy Data Efficiencies. With an e-prescribing system in place, prescriptions arrive directly in the pharmacy’s computer system so pharmacy staff spends less time interpreting handwriting or manually re-keying information into their computer systems. An automated prescription renewals process is a tremendous time saver in the pharmacy, since the communication process is streamlined and electronic.

- Prescription Drug Spending. An actuarial analysis sponsored by RxHub indicated substantial savings potential when decision support information (i.e., patient specific interactive formularies) is presented to a physician at the point of prescribing. Drug spending by health plans may be reduced by as much as 8-15 percent and drug spending inflation could be reduced by as much as 1 percent per year.
• Health Plan Savings. For the health plan, e-prescribing can reduce costs due to accurate prescribing and decreased chance of medical errors, reduced costs due to increased adherence to preferred drug lists, reduced internal administrative costs, and may serve as marketing advantage to both subscribers and employers.

**General Comments on the Proposed Rule**

• Applicability of the HIPAA Security Regulation to the E-prescribing of Controlled Substances

Since the paper prescription pad and the clinician’s signature must be kept secure, the access to the e-prescribing part of the electronic computer must also be kept secure. We contend that the combination of the existing HIPAA security and privacy regulations augmented with several additional provisions, could ensure that controlled substances are e-prescribed safely and securely.

Section 164.306 of the Security Rule is quite explicit in its demands. It requires covered entities to:

1. Ensure the confidentiality, integrity, and availability of all electronic protected health information (E PHI) the covered entity creates, receives, maintains, or transmits;

2. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

3. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required by the Privacy Rule; and

4. Ensure compliance by its workforce.

In terms of technical safeguards under HIPAA Security, covered entities must implement policies and procedures for access control on systems that maintain EPHI. These systems must allow for unique user identification and include an emergency access procedure for obtaining necessary EPHI during an emergency.

To ensure transmission security of controlled substance e-prescriptions, we recommend examining whether two currently addressable specifications should be required: Integrity controls - security measures to ensure that PHI transmitted electronically is not improperly modified without detection until disposed of, and encryption of e-prescribing data.

Data integrity can be ensured through appropriate policies and procedures to protect EPHI from improper alteration or destruction. This integrity standard is currently coupled with an addressable implementation specification for a mechanism to corroborate that EPHI has not been altered or destroyed in an unauthorized manner. In addition, data integrity also must contain person or entity authentication, which requires the covered entity to implement procedures that verify that a person or entity seeking access to EPHI is the one claimed to be doing so.
Encryption as a method of converting an original message of regular text into encoded text is an excellent way of e-prescribing controlled substances. When the text is encrypted by means of an algorithm there would be a low probability that anyone other than the receiving party who has the key to the code or access to another confidential process would be able to decrypt, or translate, the prescription and convert it into plain, comprehensible text.

Digital signatures are also a key implementation feature for e-prescribing controlled substances. When digital signatures are employed, the following three implementation features should be implemented: message integrity, non-repudiation, and user authentication. Additional features include:

- Continuity of signature capability (electronic signature is maintained with electronic document.)
- Ability to accept electronic countersignatures.
- Independent verifiability of electronic signature.
- Message integrity.
- Ability to accept multiple electronic signatures on a document.

Obtaining a digital signature certification using public key infrastructure (PKI) may prove to be a good approach. PKI can certify encrypted data that contains prescription information. Clinicians would be required to guard access to this private key. Once the data is decrypted, the pharmacy would be assured that the prescription has come from a legitimate source. The use of PKI establishes a high level of trust among users.

Digital certificates were developed to be keepers of the public key, as well as other information related to the owner of the certificate. This information might include what systems a user can access—such as a prescription system for controlled substances.

Like a hand signature, a digital certificate provides proof that an originator of a message is who the person claims to be (authentication). A digital signature is a summary of the message along with the signer’s private key. This summary is unique for every message, just as a fingerprint is unique for every person. Techniques are available to show that the message was sent from that person (non-repudiation) and provide proof that it has not been altered (integrity).

Any e-prescribing system must have, at its core, control over access rights. A strong argument can be made that once the prescription leaves the practice, security can be maintained quite easily. The critical issue for practices employing e-prescribing systems for controlled substances will be to secure access to their system. The e-prescribing application must have the ability to access the patient’s record, handle secondary access roles and privileges, limit independent prescribing privileges, or contain prescribe-with-cosign privileges. Access to the e-prescribing system in a practice would only be granted to those who have permission to electronically prescribe. Access controls, such as expiration dates on passwords, and storing passwords securely, would also be in place.
• Alternatives to Meet Technical Security Requirements

The DEA should recognize that its technical security requirements must co-exist with those imposed by other federal agencies and state governments upon prescribers and pharmacies. Therefore, rather than specifying a single approach, the DEA should be open to recognizing all existing and potential future approaches that effectively meet the DEA statutory enforcement responsibilities. For example, biometric authentication using fingerprint pattern recognition is already well established and commonly used in the industry with commercially available computing devices.

• Cost on Practices Adopting E-Prescribing of Controlled Substances

Implementing e-prescribing for controlled substances will increase prescriber costs, necessitate changes in practice workflow, and initially impact productivity. The DEA is proposing requiring registration, hard token hardware and software, software upgrades, and annual system audits. It should be recognized that all these requirements will impose a significant financial burden on practices.

• Pilot Testing

Considering the complex untested technologies and new business processes that e-prescribing of controlled substances would require, we would urge DEA to conduct real world pilot testing of its specifications in advance of any national rollout. A good model for this is provided in the 2007 Department of Health and Human Services report entitled, “Pilot Testing of Initial E-prescribing Standards.” The time and resources spent on careful pilot testing will identify problems and challenges that can be addressed in the final regulation and/or by implementing entities. Successful piloting is also instrumental to encourage wider industry acceptance.

• Certification of Stand-Alone E-prescribing Software

There is currently no entity that certifies stand-alone e-prescribing software products. This makes the purchasing decision extremely tenuous for practices and increases the likelihood that practices could select inappropriate software. With no national certification program in place for stand-alone e-prescribing software, physicians have no guarantee that the product they purchase will meet their needs, and any applicable federal requirements. Certification could address the growing concern among practices and patients that the health information they send electronically is kept private and secure. The federal government should encourage and financially support the Certification Commission for Health Information Technology (CCHIT) to institute the certification of stand-alone e-prescribing software that includes criteria in the areas of functionality, security, interoperability, and usability.

In addition to developing the standard set of testable criteria similar to their certification program for electronic health records, functionality, security, and interoperability, we encourage CCHIT to include usability criteria. If e-prescribing systems are not easy and convenient for physicians to use, it is far less likely that they will adopt them.
Creation of a National E-prescribing Advisory Body

To quickly accelerate national adoption of this important technology, we recommend the creation of a national advisory body focused solely on e-prescribing that would be a public-private collaboration, including representatives from each segment of the industry impacted by e-prescribing. This advisory body, which could be a subgroup of an existing entity (i.e., National Committee on Vital and Health Statistics, Office of the National Coordinator for Health Information Technology, American Health Information Community), would be responsible for e-prescribing research, the development and dissemination of a set of standardized technical and administrative policies and procedures, and a national communications strategy.

Specific Comments of the Proposed Rule

(All italicized language is drawn directly from the DEA’s June 27, 2008 Federal Register Notice of Proposed Rulemaking)

In-Person Identity Proofing Requirements

Proposal to permit the conducting of in-person identity proofing of prescribing practitioners within:

(36739)

- A DEA-registered hospital that has previously granted the practitioner privileges at the hospital (e.g., a hospital credentialing office);
- The State professional or licensing board, or State controlled substances authority, that has authorized the practitioner to prescribe controlled substances;
- A State or local law enforcement agency.

Comments:

Identity-proofing should be streamlined and simplified. As described by the DEA, it will be difficult for many prescribers to find the time to undergo this, and will be very time consuming for system vendors and state licensing boards to accomplish the necessary credential checking. Also, the proposed fees associated with identity proofing, estimated by the DEA at $62 per prescriber, added to the already costly DEA registration process that includes a $551 license fee for renewals, represent additional barriers to the adoption of e-prescribing of controlled substances.

Many public key infrastructure (PKI) certifying authorities (CA) offer both in-person and on-line antecedent data-based identity verification procedures. Current digital identity vetting technology offers prescribers a completely on-line process, based on antecedent data including verification of medical license and DEA registry status that can be completed in less than 10 minutes. This process is used by the pharmaceutical industry to provide digital identity credentials to clinical investigators and by healthcare information exchanges to provide credentials to medical professionals and first responders.

We therefore recommend that the DEA permit identity-proofing without an in-person requirement.

If the DEA does choose to go forward with the in-person requirement, it should consider whether the above agencies are equipped or willing to perform identity-
proofing. We would recommend that the list of performing agencies be expanded to include those approved by an authorized PKI CA. Suggested agencies would include the Secretary of State’s office, passport application processing agencies, and the American Association of Medical Colleges (AAMC). The AAMC has been doing in-person identity proofing of MCAT examinees for several years, including collecting fingerprint biometric data and storing it in perpetuity, so that only the individual carrying that same fingerprint can take a subsequent examination later in training.

Authentication Protocol Requirements

Whether authentication protocol requirements, use of a hard token and two-factor authentication, meeting the requirements of Level 4 are sufficient to address DEA’s concerns, or whether (a) more stringent requirements, such as those imposed in a public key infrastructure system, are necessary, or (b) DEA’s concerns could be addressed with Level 3 requirements combined with risk-mitigating controls. (36738)

Access to the e-prescribing system for the purposes of signing prescriptions must meet the standards for Level 4 authentication in NIST SP 800-63. That is, the system must require at least two-factor authentication to access the system; one factor must be a cryptographic key stored on a hard token that meets the requirements for Level 4 authentication in NIST SP 800-63 or a multi-factor one time password token. The hard token must be a hardware device that meets the following criteria: (36739)

- The token must require entry of a password or biometric to activate the authentication key.
- The token is not able to export the authentication key.
- The token must be validated under Federal Information Processing Standard (FIPS) 140-2 as follows:
  - Overall validation at Level 2 or higher.
  - Physical security at Level 3 or higher.

Comment:

We are concerned about the DEA’s authentication proposal and believe that the requirement to use a hard token is unworkable in most practice settings. Given the sheer volume of prescription activity, requiring a physician, especially a high volume prescriber, to comply with two-factor authentication using a hard token combined with a separate authentication process is onerous and will significantly affect practice workflows.

This proposed requirement is even more challenging for physicians who prescribe controlled substances for patients in multiple states, as they would need multiple tokens. Adding just a few minutes a day for each controlled substance prescription would substantially affect physician practice workflows and take time away from patient care. The efficiencies intended under an electronic system would be lost if the hard token approach is adopted. In order for hard tokens to work, the computer to which it is authenticating must be properly configured. The technological complexities and costs associated with these adjustments, especially for smaller practices, have not been thoroughly assessed by the DEA.

Moreover, hospitals and other settings outside the physicians’ practice must also be configured to accept hard tokens and most of these settings prohibit the connection of
foreign devices to their systems due to security concerns. We believe the DEA’s proposed authentication requirement will detract significantly from the workability of an e-prescribing system for controlled substances and would deter physicians from using the system. The CCHIT does not recommend the requirement of a hard token. A two-factor authentication is not unreasonable, however, the requirement that one factor be a hard token is not adequately flexible, given the alternative technologies, such as biometric identification. Should the DEA adopt a two-factor authentication standard, we strongly urge the DEA to remove the requirement that one factor must be a hard token.

The DEA should permit biometric authentication as a preferred alternative to a hard token. We contend that biometrics are more secure than hard tokens. They can not be stolen, borrowed, or left behind. Biometric authorization has been successfully implemented at many healthcare institutions. It would not be reasonable for the DEA to insist that facilities invest in new, less secure technology for this one purpose.

Proposed Standards for Electronic Prescription Systems

The security of the system must be audited annually using a third-party audit that meets the requirements of a SysTrust or WebTrust audit for security and processing integrity. (36739)

Comments:

- These audits will be costly, and the bills will ultimately be paid by the prescribers in the form of higher software and subscription fees. The DEA has not explained why it believes a yearly audit is necessary. By comparison, the CCHIT certifies EHR systems for three years. The DEA has not indicated how often it would expect to modify system requirements.

- Prescribers are not likely to be technically competent to review these audits. Rather than make prescribers responsible for reviewing audits, the DEA should simply publish a list of qualifying systems.

- How will prescribers be informed about the qualification status of systems available for use? It appears that a prescriber will have to ask each system vendor for a copy of the most recent audit. Will the DEA maintain an authoritative list? If so, why would prescribers be required to do anything more than pick a system from the list?

The system must have an automatic lockout if the system is unused for more than 2 minutes. (36739)

Comments:

- We recommend that the DEA define and explain this further. What does “lock out” mean? Out of the specific prescription being prescribed? Out of the second authentication workflow? Out of the prescribing module, requiring authentication to re-enter? Out of the EHR being used at the time? Also, what does “unused” mean? Failure to transmit the prescription? No interaction with the computer at all? Does this mean if a prescriber starts but does no transmit the prescription because he or she pauses to examine the patient, and then comes back to the screen...
3 minutes later, they are locked out of the e-prescribing module? The EHR? The computer? Does the prescription vanish and does the prescriber have to start over?

- We contend that the 2 minute “lock out” rule does not take into account the realities of a fast-paced prescribing environment where physicians are constantly multi-tasking. For example, if a physician began to enter a prescription into the system and had to take an urgent call, the physician would be logged out of the system within 2 minutes. We, therefore, recommend that the physician be provided with the flexibility to set an automatic timeout according to their practice workflow.

The prescription must contain all of the required data (date of issuance of the prescription; patient name and address; registrant full name, address, DEA registration number; drug name, dosage form, quantity prescribed, and directions for use; and any other information specific to certain controlled substances prescriptions mandated by law or DEA regulations). Prior to signing the controlled substance prescription, the system must show the prescribing practitioner at least the patient name and address, drug name, dosage unit and strength, quantity, directions for use, and the DEA number of the prescriber whose identity is being used to sign the prescription. (36739)

Comments:
- To support this, EHR vendors may have to move quickly to structured, codified SIG, but this is an area where the e-prescribing standard has not yet been approved/accepted.

Where more than one prescription has been prepared for signing, prior to authenticating to the system the practitioner must positively indicate which prescription(s) are to be signed. (36739)

Comments:
- What does this mean in practice? For example, prior to performing the separate e-prescribing authentication, the prescriber could be presented with a list of the controlled prescriptions, which have been drafted by the prescriber or others, and which are ready to be signed. Must the prescriber check a box next to each waiting prescription, or is it satisfactory to click an “all” button? If the latter is not acceptable, please explain why this is so.

- This may be a good thing if it means a prescriber can prepare a future prescription, but not yet sign/transmit it. We hope that the DEA does not intend to control the “how” of this but rather leave it to prescribers and e-prescribing / EHR vendors to work out the strategy.

The practitioner must authenticate himself to the system immediately before signing a prescription; (36739) and,

After authenticating to the system but prior to transmitting the prescription, the system must present the practitioner with a statement indicating that the practitioner understands that he is signing the prescription being transmitted. If the practitioner does not so indicate, by performing the signature function, the prescription cannot be transmitted. (36739)
Comments:

- Although the DEA indicates that the purpose of agreeing to this statement would be to “help positively bind the practitioner to the prescription,” we believe that this attestation is unwarranted and therefore should not be required. Furthermore, prescribers must currently adhere to CSA and DEA requirements and e-prescribing controlled substances does not alter this responsibility. The sheer volume of information proposed by the DEA, which the prescriber needs to review prior to the transmission of the prescription, is not workable in existing practice settings. We thus urge the DEA to remove the attestation requirement.

- A better approach would be to present a simple dialog box with a clear and short warning that a prescription for a controlled substance is about to be signed. This dialog could have three buttons: Agree, Cancel, and Check Record. When prescribers get prescription renewal requests in their EMRs now they have to minimize or temporarily ‘cancel’ the request - check the chart for appropriateness - and then click yes or no. The DEA proposed rule does not appear to include this necessary capability.

The system must transmit the electronic prescription immediately upon signature. The system must not transmit a controlled substance prescription unless it is signed by a practitioner authorized to sign such prescriptions. (36739)

Comments:

- “Immediately” makes sense, but prescribers will worry if they have done something wrong or be in trouble if/when the inevitable glitch arises that delays transmission. The DEA should word this so the intent is clear that the e-prescribing application is to be configured to electronically transmit the prescription as soon as it has been signed by the prescriber, and describe how transmission errors are to be handled.

The electronic data file must include an indication that the prescription was signed; and, (36739) The system must not allow printing of prescriptions that have been transmitted; if a prescription is printed, it must not be transmitted. (36739)

Comments:

- The key to this rule is the definition of “transmitted.” The DEA must make it clear that an e-prescription is not considered to be “transmitted” unless it has been successfully received by the pharmacist who will fills the prescription, and an acknowledgment has been returned to the prescriber’s system.

- This is not workable as written, given that many prescribers prepare prescriptions in advance. Under the current system prescribers are permitted to write scripts with future fill dates and this should not be jeopardized. Patients should not be required to make otherwise unnecessary trips to their prescribers’ offices just because the date coincides with the expiration of a prescription. Prescribers should not be required to revert to paper as the only solution to common prescribing events.
• We suggest the following alternative language: “If electronic transmission is prevented by weather, power loss, or equipment failure, or other similar system failure, prescriptions may be faxed to the pharmacy or printed.”

• Prescribers may want to print a copy of the prescription and place it in the patient’s record. The DEA should allow the printing of copies that clearly indicate that they are printed copies of e-prescriptions.

• Another version of that prescription may need to be faxed/printed – as depending on the market – the certainty of e-prescriptions going thru to the pharmacist can vary, with a great degree of uncertainty in some circumstances.

Proposed Post-Transmission Requirements

A prescription created electronically for a controlled substance must remain in its electronic form throughout the transmission process to the pharmacy; electronic prescriptions may not be converted to other transmission methods, e.g., facsimile, at any time during transmission. (36740)

Comments:

• Given that there are circumstances, such as transmission failure, where printing or faxing are appropriate, could an electronically submitted prescription, upon printing or faxing, show a “Submitted electronically” imprint so that any viewers of a printed/faxed version would have an indication that it was previously e-prescribed? Also, for internal record keeping purposes, we believe that the DEA should permit a prescriber to generate a print-out of an electronic controlled substance prescription, as long as the print out clearly delineates that it is a “duplicate” or “copy”.

The registrant must retain sole possession of the hard token. If a token is lost or compromised and the registrant fails to notify the service provider within 12 hours of discovery, the registrant will be held responsible for any prescriptions written using the token. (36740)

Comments:

• What does “held responsible” for prescriptions mean? Could this include criminal charges? Could it include liability for abuse of fraudulently obtained prescriptions? What is the parallel in the current paper-based world? This introduces new liability concerns. We recommend that prescribers not be held responsible for actions resulting from a lost or stolen hard token.

• The timeframe is too short. It is unclear whether service providers would be open on weekends to accept these reports. The time limit should be extended to at least 48 hours.

• How would this be accomplished – electronically, call to e-prescribing service provider? Does the DEA also need to be notified?

• What does “compromised” mean, and how would someone know if a key was “compromised?”
• This may be unreasonable. We believe that an interpretation that the individual must guarantee physical possession at all times would be unreasonable. For example, if a prescriber goes on vacation or out for a walk, must the device travel with him/her. Clarity is needed on what this means and the implications for not keeping physical possession of this key.

• This is one of the most compelling reasons to make the biometric option available.

The practitioner and pharmacist must notify DEA and the service provider if they identify problems in the logs they review that indicate that prescriptions have been created without their knowledge or altered. (36740)

Comments:
• While it is not unreasonable to ask for notification of irregularities, being held responsible for failure to notify may deter most prescribers from e-prescribing of controlled substances.

Proposals for Audits

Specifically, DEA is proposing that any system that will be used to create controlled substance prescriptions must have a third-party audit prior to accepting controlled substances prescriptions for processing and annually thereafter that meets the criteria for a SysTrust or WebTrust audit for security and processing integrity; (36747) and,

The practitioner must determine initially and at least annually thereafter that the third-party audit report of the service provider indicates that the system and service provider meet DEA’s regulatory requirements regarding the e-prescribing of controlled substances. (36748)

Comments:
• Prescribers are not law enforcement experts, nor are they computer technicians. Yet, these requirements to review and accept third-party audits of independent vendors place an undue burden on prescribers to take on these roles.

• This proposed rule places a disproportionate share of legal responsibility on prescribers and pharmacies. There should be more responsibility accepted by the DEA to certify “service providers” (vendors) and “intermediaries.”

• As previously mentioned, CCHIT certification is good for three years therefore it’s unclear why an annual audit is needed.

• It is unclear whether DEA requirements are expected to change yearly.

• We anticipate that the costs of these audits would be shifted to prescribers.

• It is unclear how a prescriber would know they are purchasing a DEA compliant system if the system is an e-prescribing stand-alone system, since CCHIT only certifies EHRs.

• It is unclear how the names of these compliant systems would be made widely available to prescribers.
Proposals for Prescribing Logs

DEA is proposing that electronic prescription service providers generate and send practitioners a log of all controlled substance prescriptions the practitioner has written in the previous month. The practitioner would be required to review the log and indicate to the service provider that the practitioner has reviewed it. A record of the indication that the review has occurred must be retained for five years. (36748)

Comments:

- We are concerned that while the DEA phrases this almost as a casual review, ("they do not expect that prescribers will check each entry in this log against the medical record, but rather just scan it for names they don't recognize, or drugs they typically don't prescribe"), the implications for this review will dictate otherwise. We believe the effort required to review these logs will be much more rigorous and time-consuming, and one more reason prescribers may opt not to adopt e-prescribing of controlled substances.

- Electronic prescription service providers should be required to provide these logs in a standard, electronic format that will enable practitioners to perform this audit (or have it performed on their behalf) automatically.

- In cases of failed transmissions, we recommend that the DEA specify exactly how prescribing activities will be logged. Assume that, for whatever reason, an e-prescription is not presented to a pharmacist for filling. The prescriber may then choose to write a new, paper prescription for the patient. The patient's medical record will now show that two prescriptions have been written for the same drug and for the same time period. How will the prescriber demonstrate that the e-prescription was never filled? It is likely that the log of the e-prescribing software will show that the prescription was sent. Likewise, the log from the intermediary may show that the prescription was transferred. The DEA should mandate that prescription logs are fail-safe from the point of view of the prescriber. Unless every system in the chain receives a clear acknowledgment that the prescription was both filled and picked up by the patient, the log should show that the attempted e-prescription failed.

Other Comments/Issues

1. The standards for electronic health records system security developed by the Certification Commission for Healthcare Information Technology (CCHIT) require systems to support two-factor identification (36741)

Comments:

It appears clear that the CCHIT does not currently certify systems to support two-factor identification. CCHIT has established this as a goal (see below) for its 2010 Roadmap, in response to issuance of the DEA’s proposed rule:

\[ SC \ 03.13 \text{ The system shall support two-factor authentication in alignment with NIST 800-63 Level 3 Authentication. Note: This is to support the 21 CFR Parts} \]

We believe that the DEA's assumption that CCHIT certified systems already have this two-factor identification capability is incorrect; adding this capability to existing systems would represent an added cost to their users, and another barrier to adoption of e-prescribing of controlled substances.

2. Interaction with Medicare's New E-prescribing Incentive/Disincentive Program

Comments:

Shortly after the DEA published the proposed regulation for electronic prescriptions of controlled substances, the President signed the “Medicare Improvements for Patients and Providers Act of 2008” (MIPPA) (P.L. 110-275) into law on July 15, 2008. In order to encourage the adoption and use of e-prescribing, this new law includes both incentives and the imposition of penalties to encourage e-prescribing, and among many other things, creates incentives for physicians to electronically prescribe prescriptions written for Medicare patients under Part D of the Medicare program. Based upon allowed Medicare charges, physicians who e-prescribe in 2009 and 2010 will be eligible for a 2 percent Medicare payment bonus, which will be phased down to 1 percent in 2011 and 2012 and 0.5 percent in 2013. Physicians, who do not e-prescribe, will be penalized by 1 percent in 2012, by 1.5 percent in 2013, and by 2 percent in 2014 and beyond.

At this time, the Secretary has not published conforming regulations stipulating how the e-prescribing program in MIPPA will operate. For example, it is unclear whether controlled substances will be excluded from determining whether a physician will be exempt from receiving incentives and/or facing penalties. Given the complexity, costs, and liability concerns associated with the DEA's proposed rule, physicians may be reluctant to adopt e-prescribing for controlled substances. We urge the DEA to recommend that CMS use discretionary authority as provided under MIPPA to exempt the e-prescribing of controlled substances from any assessment of penalties against physicians who choose not to e-prescribe controlled substances. In order to enhance e-prescribing adoption and usage rates, the DEA should also recommend to CMS that physicians be entitled to receive incentive payments, regardless of whether they choose to e-prescribe controlled substances in accordance with the DEA's final rule and requirements.

Conclusion

Having two systems in a medical practice to prescribe medications is inefficient and may in fact slow the movement to health information technology. Banking and other industries have successfully transitioned away from paper and into a secure electronic environment; it's time for health care to make that same move.
It is important to remember, however, that health information technology is costly and the majority of this cost is borne by physician practices. We encourage the federal government to take into account the cost and burden of e-prescribing when developing rules relating to controlled substances. The HIPAA Security Final Rule itself is an excellent model for how additional regulations could be crafted. We believe that allowing considerable flexibility for covered entities in terms of how to comply, while ensuring the security of the prescribing process, is the best approach.

It is critical that the final rule for the e-prescribing of controlled substances be made straightforward and appealing to prescribers and ensure it is a smoothly integrated component of a single, uniform workflow for all prescriptions. If it is not, and significant additional cost and workflow changes are asked of prescribers, there is really no incentive to move from paper-based to e-prescribing of controlled substances. Absent such incentive, we are concerned the potential for tremendous societal benefits from e-prescribing may be lost if a balance point between the DEA’s enforcement responsibilities and industry adoption feasibility cannot be reached.

We look forward to working with you to accomplish the challenging and important goal of improving the delivery and administration of health care with the use of e-prescribing.

Sincerely,

William F. Jessee, MD, FACMPE
President and Chief Executive Officer