

**Statement**  
**of the**  
**Medical Group Management Association**  
**to the**  
**Drug Enforcement Administration and the**  
**Department of Health and Human Services**

**Presented by**  
**Robert M. Tennant, MA**  
**Senior Policy Advisor**

**RE: Electronic Prescribing of Controlled Substances:**  
**Practitioner Perspective Panel**

**July 11, 2006**

The Medical Group Management Association (MGMA) is pleased to submit our testimony to the Drug Enforcement Administration and the Department of Health and Human Services on the issue of electronic prescribing of controlled substances. My name is Robert Tennant and I am a Senior Policy Advisor at MGMA where I lead the association's efforts in health information technology.

MGMA, founded in 1926, is the nation's principal voice for medical group practice. MGMA's 20,000 members manage and lead 12,000 organizations in which approximately 242,000 physicians practice.

MGMA is strongly supportive of health information technology and we believe that moving the nation's medical practices to electronic prescribing, one that includes controlled substances, will greatly improve patient care and significantly streamline administrative processes.

I would like to focus my discussion on four main areas this afternoon:

(1) The current use of paper prescriptions, (2) the clinical and administrative benefits to e-prescribing, (3) some of the security

issues of e-prescribing and (4) conclude with recommendations on moving ahead with e-prescribing controlled substances.

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. 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<sup>i</sup> – 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 ADEs occur each year in ambulatory care, of which over 3 million are preventable.

CITL also estimates that nationwide adoption of electronic prescribing will eliminate nearly 2.1 millions ADEs per year in the US. 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.

Of course, 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 brings up security issues, as paper prescriptions are relatively easy to forge and steal. Of particular concern for controlled substances is altering of the prescription sig. It is all too easy to change one refill to ten 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.

Let me turn to the benefits of electronic prescribing. Of the many significant benefits associated with e-prescribing, the most important of these is enhanced patient safety. Safety is increased due to the legibility and accuracy of the prescription, as compared to handwritten notes. Additional safety benefits when e-prescribing incorporates drug formularies, so that interactions and contraindications are automatically screened at the time of prescribing the medication. No more lost paper scripts that are never filled, as the prescription can be sent directly to the pharmacy or as an electronic transaction.

E-prescribing could also improve quality, efficiency and reduce costs by:

- Actively promoting appropriate drug usage
- Providing information about formulary based drug coverage including formulary alternatives and copay information
- Reduction of phone calls required
- Providing instant connectivity between health care providers, the pharmacy, health plans and PBMs.

From an administrative perspective, practices can take advantage for 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.

From a cost saving perspective, E-prescribing allows practices to handle refill requests faster, with estimated 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.

One of most exciting benefits of e-prescribing comes from its integration with a practice electronic health record. Robust systems allow the 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 electronic medical record.

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.

Thanks to the Medicare Modernization Act and the HHS final rule, we now have an excellent set of foundation standards for e-prescribing. The NCPDP SCRIPT standard for transactions between prescribers and dispensers include several critical transactions including new prescriptions, refill requests and response, prescription change request and response, prescription cancellation request and response, and ancillary messaging.

However, one transaction was not included in the first set of foundation standards that should prove to be a valuable security tool for the e-prescribing of controlled substances. The fill status notification transaction will permit pharmacies to send a message to the clinician when the prescription has been filled. This will allow clinicians to monitor the dispensing of controlled substances to guard against security breaches that led to unauthorized fills.

As the paper prescription pad and the clinician's signature must be kept secure, the access to the electronic prescribing part of the electronic computer must be kept secure. I contend that the combination of the existing HIPAA security and privacy regulations along 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:

- Ensure the confidentiality, integrity, and availability of all electronic protected health information (EPHI) the covered entity creates, receives, maintains, or transmits;
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;
- Protect against any reasonably anticipated uses or disclosures of such information that are not permitted or required by the Privacy Rule; and
- 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 electronically-transmitted PHI 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 signature is 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 prove 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

electronic prescribing application must have the ability to access the patient's record, handle secondary access roles and privileges, limit independent prescribing privileges, or prescribe-with-cosign privileges.

Access to the e-prescribing system in a practice is only granted to those who have permission to electronically prescribe. Access controls, such as expiration dates on passwords, and storing passwords securely, must also be in place.

The requirement to protect confidential information is clearly more critical than ever. Augmenting the HIPAA Security Rule appears to be the best approach to achieving what all stakeholders require—safe secure and streamlined electronic prescribing of controlled substances.

In conclusion, while MGMA is confident that electronic prescribing is improve clinical performance, easing administrative burdens and facilitating improved data interchange within the health care

community, roadblocks exist that must be addressed before electronic transmission of controlled substance prescriptions will be achieved. Revising the HIPAA Security Rule, developing the fill notification transaction standard, expanding provider education on appropriate security measures and harmonizing the myriad of state laws governing e-prescribing should be considered.

Having two systems in a medical practice to prescribe medications makes no sense 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.

Allowing considerable flexibility for covered entities in terms of how to comply, while ensuring the security, would appear to be the best approach.

We appreciate your interest in this important topic and thank the DEA and HHS for inviting us to present our views on this issue.

---