September 25, 2008

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

Re: The Drug Enforcement Administration proposed rule on *the Electronic Prescriptions for Controlled Substances*, 21 CFR Parts 1300, 1304, et al. (June 27, 2008). Docket No. DEA—218.

Dear Acting Administrator Leonhart:

The American Medical Association (AMA) along with the undersigned organizations appreciate the opportunity to provide comments on the Drug Enforcement Administration's (DEA) proposed rule on electronic prescriptions for controlled substances. Under the rule, the DEA proposes a process for electronic prescribing (e-prescribing) of controlled substances that supplements, but does not replace, existing prescribing and dispensing requirements established by the Controlled Substances Act (CSA) and DEA regulations.

Currently, prescribers are prohibited from e-prescribing controlled substances. When properly implemented, an e-prescribing process and system for controlled substances will assist physicians with improving patients' quality of life in a safer, more secure, and efficient manner. Automating our current paper-based process is expected to create a safer prescribing environment by eliminating errors due to illegible handwritten prescriptions, providing physicians with drug interaction information at the point of care, and creating electronic audit trails of prescriptions for tracking purposes. In order to be successful, the e-prescribing process and system should be practical, functional, secure, as well as affordable for physicians.

Although we recognize the challenges associated with establishing a secure process and system for e-prescribing, we believe that the NPRM falls short of the goal of establishing a secure process for e-prescribing of controlled substances that is also effective and practical, and so we urge the DEA to revise language accordingly. Our initial concern is that the proposed rule would instead impose multiple stringent

security, authentication, and risk management requirements for users of e-prescribing. These additional requirements will force physicians to implement two different electronic workflows for e-prescribing: one for controlled substances and one for noncontrolled substances. Furthermore, the proposed standards go above and beyond many of the current requirements physicians must meet when prescribing non-electronic controlled substances. Given the complexity, costs, and liability concerns associated with the proposed rule, physicians may be reluctant to adopt e-prescribing for controlled substances. **We, therefore, strongly recommend that the DEA establish an advisory panel comprised of key stakeholders, including physicians, to develop a process for e-prescribing that properly balances efforts to minimize drug diversion and the nonmedical use of prescription drugs while maintaining a clinical practice environment conducive to safer, efficient, and high quality care.**

In-Person Identity Proofing

Under the DEA's proposed rule, a non-federal health care facility would be required to undergo in-person identity proofing and submit documentation to authenticate their identity. The identity proofing would be conducted by a DEA registered hospital, a State licensing board, or a State or local law enforcement agency. Although some states currently require physicians to register with their state board of pharmacy, prescribers are not required to undergo in-person identity proofing. We fail to see the rationale for requiring in-person identity proofing only for e-prescribing of controlled substances given that there are no assurances that this burdensome requirement will actually reduce prescription forgery, fraud, theft, and other-related crimes to drug diversion. Even the proposed rule acknowledges that, "most identity theft occurs not from people hacking into systems, but rather from insiders who know how to manipulate the system." Furthermore, if this stringent standard is adopted, physicians practicing in rural and remote areas, who would be required to travel significant distances for identity proofing, would likely be reluctant to engage in this process.

The imposition of additional fees for identity proofing is an additional barrier to e-prescribing adoption and use. The proposed fees associated with identity proofing—costs estimated by the DEA at $62 per physician—would add to an already costly DEA registration process that includes a $551 license fee for renewals; which is disproportionately high as compared to other registrants' fees. The DEA's costly registration / renewal process is made further unaffordable by the fact that the fees apply to all the states in which the prescriber needs to be registered. **We urge the DEA to remove in the final rule any fees on prescribers for identity proofing or increases in DEA prescriber registration fees.**

We also believe that the DEA should reconsider the current requirement that physicians, who prescribe in multiple states, as well as locum tenens physicians, obtain a separate DEA number per state. If the DEA were to make DEA numbers less accessible to non-DEA registrants and the public, such stringent controls would not be necessary, including the proposed in-person identity proofing. **We, therefore, strongly urge the DEA not to require in-person identity proofing and**

recommend the issuance of one federal DEA number that would be physician-specific and not site-specific in order to reduce the unnecessary burdens and costs on physicians for maintaining multiple DEA numbers.

Digitally Signed Records

The DEA explored, but chose not to require, practitioners to digitally sign electronic controlled substances. Digital signatures are created as part of a public key infrastructure (PKI)—a method for ensuring the integrity of an electronic message. This system uses asymmetric cryptography where an algorithmic function is used to create two mathematically related or complimentary public and private keys. Under an e-prescribing scenario, a prescriber would send an encrypted prescription to a pharmacy. With PKI, a trusted party conducts identity proofing and provides a subscriber (prescriber) with a pair of keys; a private key just for the subscriber and a separate public key which can be made available to anyone. The advantage of PKI is that it allows the confidential transmission of information in open networks when parties do not know one another in advance and eliminates the need to share secret key information.

We support the use of PKI systems or other signature technologies designed to accommodate electronic prescriptions for sending Schedule II prescriptions. We believe these technologies should be adaptable to current computer systems, and satisfy the criteria of privacy and confidentiality, authentication, incorruptibility, and nonrepudiation. The DEA however, proposes not to use the PKI because the "intermediaries" in the existing e-prescribing system frequently reformat prescriptions during transmission, and in essence, alter what was originally sent by the prescriber making it impossible to validate a physician's digital signature. Physicians must be assured that the prescriptions they issue will be transmitted to the pharmacy as intended.

While we believe that the standards should accommodate the use of PKI for those prescribers who would like to use PKI, we do not support instituting separate prescribing requirements for the electronic transmission of Schedule II prescriptions vs. Schedules III-V, as this would impose an unnecessary level of complexity for prescribers and would result in a burdensome process that is likely to impede the e-prescribing adoption and use rates for controlled substances. **We urge the DEA to reconsider the use of PKI or other signature technologies, should a physician elect to use them.**

Authentication

Authentication is information (e.g., PINs, passwords, biometrics) that is used to verify a person's identity for security purposes. The authentication methods could be one-factor, two-factor, or multi-factor, and can be described as something you know, something you have, or something you are. The DEA has proposed a two-factor authentication requirement that calls for something you know and something you

have. The DEA further proposes the use of two factors with one of them to be stored on a "hard token" or the use of a multi-factor one time password token (e.g., hardware device like a PDA that generates one time passwords for use in authentication). The known item could be a password, while a hard token could be a PDA, cell phone, thumb drive, smart card, etc. According to the DEA's proposed rule, hard tokens would need to meet certain standards and the password could not be used without the hard token.

We are very concerned about the DEA's authentication proposal and believe that the requirement to use a hard token is unworkable in most practice settings. A recent AMA e-prescribing survey indicated that primary care physicians wrote up to 100 prescriptions per day. Specialists usually write an average of 10 to 25 prescriptions per day. Given the sheer volume of prescription activity, requiring a physician, especially a high volume prescriber, to comply with two-factor authentication with 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. For example, a small group practice that serves patients from a tri-state area would be required to manage multiple tokens for each physician, a situation that would be confusing and ultimately unmanageable. 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 Certification Commission for Healthcare Information Technology (CCHIT), an electronic health records (EHRs) certification body funded by the Department of Health and Human Services (HHS), 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. Should the DEA adopt a two-factor authentication standard, we strongly urge the DEA to remove the requirement that one factor be a hard token.**

Access Limitations and Signing

The proposed rule requires that the prescriber authenticate to the system using the two-factor authentication immediately prior to signing and transmitting the electronic prescription. This is not practical given that there may be a significant time lapse

between writing and transmitting a prescription. Physician practices often prepare information ahead of time (i.e., during patient visit) but must submit the prescription within a specified time period (i.e., time periods identified in the patient's certificate of coverage). In addition, under the current system, physicians are able to write prescriptions with future fill dates and thus the DEA's proposed rule would not allow for the transmission of predated prescriptions.

The DEA also proposes that after authenticating to the system but prior to the transmission of the electronic prescription, the system must present the following statement that the prescriber is required to positively attest to and "sign" (electronic signature):

> ''I, the prescribing practitioner whose name and DEA registration number appear on the controlled substance prescription(s) being transmitted, have reviewed all of the prescription information listed above and have confirmed that the information for each prescription is accurate. I further declare that by transmitting the prescription(s) information, I am indicating my intent to sign and legally authorize the prescription(s).''

Today, under paper-based systems, prescribers are not required to positively attest to the above-mentioned statement. The DEA indicates that the purpose of agreeing to this statement would be to "help positively bind the practitioner to the prescription" and provide nonrepudiation. We do not agree. Physicians will already be required to authenticate to the system in order to gain access. Requiring a physician to electronically sign or attest to such a statement provides no further assurance of the identity of the prescriber. Therefore, we believe that this attestation is unwarranted and 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 urge the DEA to remove the attestation requirement.**

However, we do agree that after authenticating to the system but prior to transmitting the controlled substance prescription, a limited summary of the controlled substance prescription being transmitted should be displayed (i.e., full name and address of the prescribing practitioner, the DEA registration number of the prescribing practitioner, full patient's name and address, the name of the drug prescribed, the dosage strength and form, quantity prescribed, and directions for use); a process that could further help avert medication errors. The medication list should also be available prior to the authentication and transmission of a single prescription.

As the DEA notes, electronic signatures are considerably different from digital signatures. Signing an electronic prescription is merely an attestation by the prescriber to the validity of the prescription which would legally bind them to that prescription. Because it does not provide any further assurance against

nonrepudiation, we oppose such a requirement. Digital signatures on the other hand, as discussed earlier, are used to maintain the integrity of the prescription and are thus preferable. The advantage of using digital signatures is that "they provide, in a single step, what other systems do not: a straightforward means of determining record integrity. If the first recipient of an electronic prescription signs it digitally, (the) DEA will be able to prove what the practitioners signed."

Automatic "Timeout"

The DEA proposes a two-minute "timeout," which would lock a prescriber out of an electronic system if the system is not used within the two-minute time frame. The two-minute timeout rule is just not practical and 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 his/her practice workflow.**

Prescribing Logs

The DEA's proposal requires service providers to generate a monthly log of prescriptions for controlled substances to prescribers. Requiring physicians to review a monthly log of all of their electronic controlled substance prescriptions, affirmatively indicate having done so, and retain such records for at least 5 years, is overly burdensome. Given the sheer volume of prescribing activity, it is too onerous and time-consuming for physicians, especially high volume prescribers, to review a log of their prescriptions on a monthly basis and attest to this review. It is entirely unclear why this is being required when paper-based prescriptions could be altered and yet there is no requirement for reviewing lists of non-electronic controlled substances prescriptions. However, we agree that logs should be made available for review but requiring physicians to review every single electronic prescription and attest to the log's accuracy is excessive. **We, therefore, recommend that the DEA remove the requirement for physicians to confirm monthly reviews of prescription logs generated by service providers.**

Third-Party Audits

The proposed rule also calls for prescribers to only use systems that meet DEA's security and prescribing requirements. The DEA proposes that vendors and pharmacies pursue third-party audits performed by qualified certified public accounting firms in order to confirm that their systems meet DEA standards. In turn, prescribers would be required to initially and annually thereafter review the third-party audit report provided by their service vendor and affirm that their system complies with DEA requirements. If the system is non-compliant the prescriber

would be required to immediately cease use. Physicians do not have the technical or law enforcement expertise to make such determinations.

Furthermore, the CCHIT does not certify stand alone e-prescribing systems so physicians would be unable to determine whether their e-prescribing systems are compliant with widely-recognized technical and security standards. Moreover, the requirement that a physician immediately cease using a system that is determined not to meet DEA's requirements could significantly affect patient access to needed prescriptions. **We urge the DEA to remove the requirement for physicians to attest that their EHRs or e-prescribing systems are compliant with the DEA requirements.**

Service Provider and Intermediary Accountability

The term, service provider, which is not defined in the proposed rule, refers to a software vendor that a prescriber uses to create a prescription and to parties involved with transmission of the prescription. We recommend that terms and definitions for both of these described parties be clearly defined because their functions differ.

We also are concerned that in order for prescribers and pharmacies to comply with DEA requirements they must rely upon the services of other parties, the "service providers" and "intermediaries," which are not required to comply with the CSA or DEA regulations. The lack of accountability of non-regulated parties could adversely effect requirements intended to ensure the integrity and security of controlled substance prescriptions. This lack of accountability is already being experienced with the enforcement of the Health Insurance Portability and Accountability Act (HIPAA). Under HIPAA, health care providers, payers, and clearinghouses are considered "covered entities" and are required to comply with privacy and security standards when using or disclosing protected health information. Although third party billers, employers, personal health record vendors, marketing firms, as well as other non-HIPAA covered entities may handle protected health information, they are not held directly accountable under HIPAA. This creates a gap in federal privacy protection coverage that leaves large volumes of identifiable health information vulnerable to improper access and disclosure without meaningful enforcement mechanisms or remedies. The DEA's lack of jurisdiction over service providers and intermediaries also creates a gap in ensuring the integrity and security of e-prescribing of controlled prescriptions. **We, therefore, urge the DEA to pursue legislation that extends legal responsibilities to non-DEA covered parties involved with the electronic transmission and processing of prescriptions for controlled substances.**

Cost Impact of Security Measures and Requirements

One of the most significant and widely-recognized barriers for physician adoption of e-prescribing and health information technology (HIT) is cost. The proposed rule indicates that the average cost of an EHR ranges from approximately $20,000 to $50,000 per physician, not including an annual maintenance charge of

$6,000 per doctor. Additionally, the extensive technical, security, and other standards requirements (i.e., costs for registration, hard token hardware, software, indirect costs, reprogramming, and audit requirements) for e-prescribing controlled substances will undoubtedly be significant and ultimately be passed on to physicians and others. For example, the proposed rule indicates that the initial programming costs in order to comply with the DEA requirements will be $36,700 for an EHR. Moreover, the DEA projects a 4 percent per year adoption rate and 15 years for implementation which clearly indicates that the DEA requirements are too costly and burdensome. **Given that the costs of acquiring and maintaining EHRs and the additional costs associated with adoption of the DEA proposed standards, we strongly recommend that the DEA work with an advisory panel comprised of key stakeholders, including physicians, in order to come up with an affordable, functional, practical, and secure mechanism for e-prescribing controlled substances.**

Other Standards

Converting Electronic Prescriptions to Fax or Paper

Under the proposed DEA rule, once a controlled substances prescription has been sent electronically, it can not be printed or faxed, otherwise the prescription would be rendered invalid. In the case of the use of "hard copy" facsimile transmissions, as with the original written prescription for Schedule II controlled substances, we agree that faxes should not be permitted, except as currently authorized in accordance with Section 1306 of Title 21 of the Code of Federal Regulations.

We are concerned however about precluding prescribers from printing documentation of copies of their controlled substance prescriptions. There may be situations which call for the printing of a controlled substance prescription after it has been electronically transmitted to a pharmacy. For example, a physician may be audited by a health care payer and contractually required to furnish medical records, including prescriptions for controlled substances. Moreover, HIPAA requires physicians to furnish patients with a copy of their medical record, including prescription information, upon request. It is also unclear what protocol a physician would have to follow for network transmission failures. The resubmission of a prescription due to a network transmission failure could be erroneously deemed as a duplicate. **We, therefore, urge the DEA to permit physicians to print documentation of controlled substance prescriptions so long as the print out clearly delineates the copy as a "duplicate" or a "copy." We also urge the DEA to define the term "transmission" and explain how transmission errors would be identified and handled.**

Reporting Lost or Stolen Tokens

We are concerned with a provision in the proposed rule that would hold physicians responsible for any controlled substance prescriptions written using the hard token if

the hard token is lost, missing, or compromised, and not reported within 12 hours of discovery. We strongly believe that this additional legal burden imposed on physicians will act as a disincentive for physicians to e-prescribe controlled substances given that they can be held liable for unforeseeable actions resulting from a lost or stolen smart card, cell-phone, or PDA. We also believe that the 12 hour time frame for reporting purposes is not practical. For instance, if a prescriber's cell phone is lost or stolen on a Friday evening, and the service provider is not available until Monday morning, the 12 hour time limit would not be met. We also recommend defining the vague term "compromised" or removing it altogether. **We strongly recommend that the time frame for reporting a lost or stolen token be extended to 48 hours and that physicians not be held responsible for actions resulting from a lost or stolen hard token.**

The "Medicare Improvements for Patients and Providers Act of 2008" (MIPPA)

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 for 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, therefore, 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 use 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

We appreciate the opportunity to comment on this proposed rule and look forward to providing ongoing input to the DEA to ensure the development of an e-prescribing

process and system for controlled substances that is practical, functional, affordable, and secure for physicians. Should you have questions about these comments, they can be directed to Mari Savickis at mari.savickis@ama-assn.org or 202-789-7414.

Sincerely,

American Academy of Dermatology Association
American Academy of Family Physicians
American Academy of Home Care Physicians
American Academy of Hospice and Palliative Medicine
American Academy of Otolaryngology-Head and Neck Surgery
American Academy of Pain Medicine
American Association of Clinical Endocrinologists
American Association of Neurological Surgeons
American College of Cardiology
American College of Emergency Physicians
American College of Obstetricians and Gynecologists
American College of Osteopathic Internists
American College of Osteopathic Surgeons
American College of Physicians
American College of Radiology
American College of Surgeons
American Gastroenterological Association
American Geriatrics Society
American Medical Association
American Osteopathic Academy of Orthopedics
American Osteopathic Association
American Psychiatric Association
American Society of Addiction Medicine
American Society of Anesthesiologists
American Society of Clinical Oncology
American Society of Hematology
American Society of Plastic Surgeons
American Thoracic Society
American Urological Association
Congress of Neurological Surgeons
Infectious Diseases Society of America
Medical Group Management Association
Society of Hospital Medicine
Society of Interventional Radiology