American Hospital Association

Liberty Place, Suite 700
325 Seventh Street, NW
Washington, DC 20004-2802
(202) 638-1100 Phone
www.aha.org

September 24, 2008

Michele M. Leonhart
Acting Administrator
Drug Enforcement Administration
8701 Morrissette Drive
Springfield, VA 22152

***RE: DEA-218, Drug Enforcement Administration, Electronic Prescriptions for Controlled Substances; Proposed Rule (Vol. 73, No. 125), June 27, 2008***

On behalf of our more than 5,000 member hospitals, health systems and other health care organizations, and our 38,000 individual members, the American Hospital Association (AHA) appreciates this opportunity to comment on the Drug Enforcement Administration's (DEA) proposed rule for electronic prescriptions for controlled substances. The use of information technology (IT) in health care can improve the efficiency, safety and quality of care in hospitals, and we appreciate the DEA's effort to remove barriers to further IT adoption by allowing electronic prescriptions for controlled substances.

The AHA supports the voluntary participation aspect of the DEA's proposal. To increase participation, we urge the DEA to ensure that implementation of this rule is aligned with other efforts within the federal government and the private health care sector to avoid conflicts and redundancy. For example, the recently passed *Medicare Improvements for Patients and Providers Act* provides incentives beginning in 2009 for physicians who adopt e-prescribing for their Medicare patients.

The DEA's proposal highlights the complexity of finding a practical solution to the controlled substances issue. If introduced correctly, e-prescribing of controlled substances can be adopted cost effectively and with reduced risk to all stakeholders. Our comments on the proposed rule address three areas of concern: inadequate technologies at the present time and the associated costs, new legal risks and the need for pilot testing. Left unresolved, these issues will have a negative impact on the adoption of e-prescribing of controlled substances.

### CURRENT TECHNOLOGY IS INADEQUATE

We recommend that the DEA recognize all existing security approaches that effectively meet or exceed the agency's objectives. The DEA's proposed approach of two-factor authentication, which requires two means of identification – a password and a token, is burdensome and costly.

The DEA makes incorrect assumptions in the proposed rule about the security-related functionality of current electronic health record (EHR) systems and their adoption rates. In the proposed rule, DEA states on page 36741:

> 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. Consequently, all of the EHR systems certified by CCHIT (approximately 85 systems) already support two-factor authentication.

This is not correct. CCHIT does not certify for this functionality at this time; however, it has made two-factor authentication part of its 2010 roadmap, which reads as follows:

> SC 03.13 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 1300, 1304, et. al. Electronic Prescriptions for Controlled Substances; Proposed Rule published on Friday, June 27, 2008, Federal Register / Vol. 73, No. 125F11.

Therefore, as a direct result of this proposed rule, CCHIT has targeted 2010 to begin certifying for two-factor authentication functionality. Most EHR systems in use today do not have this functionality. For hospitals that have already implemented EHR systems, there will be significant costs associated with adding this functionality. Costs will be even higher for hospitals that have developed their own EHR systems or significantly modified a vendor's EHR system.

There are alternatives to two-factor authentication that would be more cost-effective and more secure. Two-factor authentication with a hard token (such as, a memory stick or personal digital assistant), as described in the rule, is viewed by prescribers as impractical and inconvenient, and will slow the prescribing workflow. Hard tokens can be shared or stolen, resulting in unauthorized use. Furthermore, the hard tokens mentioned are not considered secure enough for this purpose. Adapting all clinical computers in a hospital for hard token authentication presents significant security, engineering and financial challenges. Further work must be done to demonstrate how hospitals would integrate these objects into a secure system for this purpose.

If the DEA insists on the two-factor authentication, the AHA recommends that the DEA consider the use of biometric authentication as a preferred alternative to a hard token.

Biometrics are more secure than hard tokens. They cannot be stolen, borrowed or lost. "Who you are" is clearly more secure than "what you have." Biometric authentication has been piloted or implemented in a growing number of technically advanced hospitals as a way to increase system security without a significant impact on workflow. Regardless of the method selected, smaller or rural hospitals, for example, will incur additional costs whether they implement for the first time or modify existing systems to meet the DEA's requirements described in this rule.

## NEW LEGAL RISKS COULD IMPEDE ADOPTION OF E-PRESCRIBING

As written, the proposed rule introduces unnecessary legal risk to hospitals and prescribers that will impede the adoption rate of e-prescribing for controlled substances. The DEA's proposal to allow DEA-registered hospitals to perform identity proofing for community prescribers potentially exposes hospitals to liability if a mistake is made. We urge the agency to clarify whether or not the DEA will provide immunity from such liability.

The proposed rule also introduces further areas of liability in its requirements related to lost tokens, audits and prescriber logs:

- The DEA says a registrant (a presciber registered with the DEA) will be held responsible for any prescriptions written using a lost or compromised token [page 36740]. It is unclear if this includes criminal charges, or whether the liability is restricted to the individual who lost the token, or if liability extends to the hospital where the token was compromised.

- The DEA says a 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 electronic prescribing of controlled substances" [page 36748]. These requirements to review and accept third-party audits of independent service providers and vendors place an undue burden on prescribers to take on the roles of law enforcement and computer forensics. The proposed rule places a disproportionate share of legal responsibility on prescribers and pharmacies.

- The DEA proposes on page 36748 that "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 that the review has occurred must be retained for five years." The DEA further notes that "they [DEA] 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." It is unclear what legal weight this review of the log will hold in court if a prescriber is prosecuted for drug diversion.

Again, these review requirements and the legal uncertainties will keep adoption rates of e-prescribing lower than anticipated.

### PILOT TESTING MUST BE CONDUCTED

Given these additional costs and risks, we urge the DEA to conduct real world pilot testing prior to a national rollout of this rule. Pilot testing will help identify any technology or process issues, and provide the DEA with additional information to refine rules and increase the adoption rate of electronic prescribing of controlled substances. With information based on actual implementation, strategies can be shared and risks lowered for all stakeholders. Testing could either be performed in conjunction with other e-prescribing pilots already in place, or by volunteer health care communities. In either case, both rural and urban communities should be represented in the pilot.

### CONCLUSION

Historically, the health care field has been slow to adopt IT. To increase participation, we urge that the DEA gain a better understanding of the security-related functionality of current EHR systems, clearly define financial and legal risks associated with e-prescribing of controlled substances, and conduct careful pilot testing. In addition, the AHA recommends that the DEA ensure its efforts are aligned with those of other federal agencies and private entities.

If you have any questions about these remarks, please contact me or Rod Piechowski, senior associate director for policy, at (202) 626-2319 or rpiechowski@aha.org.

Sincerely,

Rick Pollack
Executive Vice President