ACP
American College of Physicians
INTERNAL MEDICINE | *Doctors for Adults*

September 22, 2008

Michele Leonhart
Acting Administrator
Drug Enforcement Administration
Attention: DEA Federal Register Representative/ODL
8701 Morrisette Drive
Springfield, VA 22152

Re: (DEA-218P)

Dear Administrator Leonhart:

The American College of Physicians (ACP), representing more than 126,000 physicians specializing in internal medicine and medical students, is pleased to offer comments on the Drug Enforcement Administration's (DEA) *Electronic Prescriptions for Controlled Substances; Proposed Rule (DEA-218P).* The College applauds the DEA's efforts to bring into our healthcare system the many benefits that can be gained from expanding electronic prescribing to controlled substances, while ensuring that there are adequate regulatory protections against the diversion of these same substances into illicit markets and their abusive use. The College, through this letter, has attempted to provide comments from our unique perspective as prescribers that will facilitate the Agency reaching this commendable goal. We believe the issues and suggestions provided will assist the DEA in finalizing and implementing a regulatory framework that will be more congruent with the workflow of most healthcare settings—thus, ensuring greater acceptance, compliance and effectiveness. .

The College offers the following comments:

General

- **Definitions – Important terms are not defined and are not used consistently. For example, "service provider" sometimes refers to the vendor of the software that the prescriber uses to create the prescription. Other times "service provider" refers to a third party that receives the original prescription message from the prescriber and passes it to the pharmacy. Given that these two functions are assigned completely different requirements, it is crucial that they are given entirely different names that**

- **Technical Security Requirements - DEA requirements should recognize and be compatible with other agencies that establish security requirements that apply to prescribers and pharmacies. Toward this end, the DEA should ensure that it allows for as much flexibility as possible in the methods by which highly trusted authentication is achieved, including examples in all three major authentication categories, including "what you know" (a strong password), "what you have" (a hard token) and "who you are" (a biometric identifier). This will maximize the likelihood that DEA security requirements will be compatible with current and future authentication standards, specifications and requirements of other entities, agencies, regulations and laws. Rather than specifying a single approach (a hard token, which could be shared or stolen), DEA should recognize all existing effective approaches. In particular, biometric authentication using fingerprint pattern recognition is well established in the industry, is commonly available as an integrated authentication solution in commercially available computing devices in the consumer market, and some EHR vendors have already incorporated second factor authentication using a fingerprint biometric strategy to meet the Ohio Board of Pharmacy regulations for e-prescribing. Fingerprint biometric authentication also has the advantages of convenience, efficiency, virtually complete assurance against sharing or stealing, and lack of concerns about device failure or loss. Prescribers can not be expected to meet the idiosyncratic and sometimes conflicting technical requirements imposed by every conceivable authority.**

- **Testing – DEA is specifying a unique collection of complex technologies and new, currently non-existent, business processes. These specifications have never been tested in any setting, let alone in the real world. Thorough real-world testing of DEA specifications is required. In 2007 the Department of Health and Human Services issued a report titled, "Pilot Testing of Initial Electronic Prescribing Standards." (See:** http://healthit.ahrq.gov/portal/server.pt/gateway/PTARGS_0_1248_227312_0_0_18/eRxReport_041607.pdf**). These pilot tests examined the capabilities of several leading e-prescribing standards to support a range of e-prescribing functions in both laboratory and 'real-world" settings. Analysis of the results found that some standards are capable of effectively supporting some functions, while support for other functions is not yet ready. The scope of DEA-proposed rules should be limited to functions that have been determined by a recognized authority to be ready for use, using methods similar to this pilot study. If DEA orders the use of untested technologies and workflows, the agency risks enormous backlash from all stakeholders, as well as severely negative publicity which could harm its abilities to achieve its**

objectives. We believe that a smooth roll-out is worth some significant investments of time and resources.

DEA welcomes comments on:

Whether in-person identity proofing requirements consistent with, but not equivalent to, Level 3, are sufficient to address DEA's concerns, or whether (a) more stringent requirements, such as those required under Level 4, are necessary, or (b) DEA's concerns could be addressed with Level 2 requirements combined with risk-mitigating controls.

DEA is proposing to permit the conducting of in-person identity proofing of prescribing practitioners within:

- 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.

DEA also proposes that the service provider must check both the practitioner's State license and DEA registration to determine that both are current and in good standing. Although DEA believes that many service providers would be on site at practitioners' offices routinely due to the complexity of the EHR systems of which electronic prescribing is often a part, DEA recognizes that conducting enrollment activities at that time may be inconvenient.
ACP encourages consideration of the following concerns and suggestions related to the proposed in-person proofing and service provider requirements:

- **The defined agencies and service providers are generally not equipped to handle this additional responsibility. Private agencies will not be willing to accept the potential liability in case of fraud.**

- **Will entities that conduct identity proofing be permitted to charge physicians for this service? Will DEA fees be increased to pay for this?**

- **It is likely that many rural prescribers will be required to travel for hours to perform in-person enrollment.**

- **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. Paul Jolly from AAMC has lead this effort and gave testimony at an AHIC meeting. (See:** http://www.hhs.gov/healthit/ahic/materials/meeting09/cps/P3-EHR-Jolly.pdf**; his testimony has a number of good ideas on identity proofing that could be used.)**

- **The two other most qualified/experienced entities in identity proofing today are 1) the local Secretary of State's office, and 2) any passport application processing agency (e.g., USPS). These entities should seriously be considered as in-person proofing sites. With some training and the right tools for all (e.g., collecting fingerprints, voice prints, handwriting samples, retinal scans would be the big 4 in 2009), one might also add to the list the credentialing offices of academic group practices in medical schools. The gold standard for a workable process currently in use might be the AAMC as mentioned above.**

- **The DEA assumption that service providers would be on site at practitioners' offices is faulty. This is not likely to happen in any but the largest of practices**

DEA welcomes comments on:

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.

Access to the electronic 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:

- 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.

ACP encourages consideration of the following concerns and suggestions related to the proposed authentication requirements:

- **A second authentication at the time of transmission is reasonable given the potential for unintentional or intentional failure to have only authorized prescribers actually transmit the Rx. The key is to view authentication as having many highly acceptable approaches and requiring that a certain strength of authentication be the outcome; not prescribe the exact method by which that authentication is generated. For example, a strong password would be one great way of getting one factor authentication, but it may not**

- **Two factor authentication with a hard token, however, is generally viewed by physicians as impractical and inconvenient. It is also cost-inefficient compared to alternative strategies, unnecessary as a means of second factor authentication, and may slow down the prescribing workflow for users required to read off and enter passwords generated by the hard token. Hard tokens can also be shared or stolen, resulting in unauthorized use.**

- **The hard tokens mentioned (cell phones, PDAs, and USB drives) are not considered secure enough for this purpose. DEA must provide more detailed examples of how acceptable objects can be made sufficiently secure.**

- **DEA should permit biometric authentication as a preferred alternative to a hard token. Biometrics are more secure than hard tokens. They can not be stolen, borrowed, or left behind. "Who you are" is clearly more secure than "what you have." Biometric authorization has been implemented successfully at many healthcare institutions. It is unjustifiable for DEA to insist that these facilities invest in new, less secure technology for this one purpose.**

- **DEA should also permit the use of "tap-and-go" proximity cards as a cost-effective, preferred alternative to the specified hard token.**

- **How will hard tokens be managed? Who will create them? How will they be distributed to prescribers? How will losses of tokens and passwords be handled? What will be the full costs to practices? What happens when they malfunction, are dropped, broken, immersed? What if the system supporting them goes down?**

- **For hard tokens to work, the computer to which it is linked for authentication must be adapted. First, this will be a significant expense that has not been identified by DEA. Second, hospitals and other facilities in which prescribers practice do not allow connection of foreign devices to their systems because of obvious security concerns. Adapting all clinical computers in a medical center for hard token authentication presents a significant security, engineering and financial challenge.**

- **Small practices do not have the information technology (IT) service resources to install and manage hard token connections.**

DEA welcomes comments on:

Whether no requirements regarding the authentication process, as proposed in this rule, should cause DEA concern, such that imposing requirements is necessary.

- **The College believes that the DEA must recognize that it is not the only agency that imposes security requirements on prescribers and pharmacies. DEA must be careful not to over-specify details of authentication and other security functions, because these specifications will conflict with other established and future requirements. DEA requirements must coexist with those of many other agencies, regulations and laws. Rather than specifying a single approach, DEA should recognize all existing effective approaches.**

The College offers comments on the following 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.

- **These audits will be costly, and the bills will ultimately be paid by the prescribers in the form of higher software and subscription fees. DEA has not justified the need for a yearly audit. CCHIT certifies EHR systems for three years. DEA has not indicated how often it expects to modify system requirements.**

- **Prescribers are not technically competent to review these audits. Rather than make prescribers responsible for reviewing audits, 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 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 lock out if the system is unused for more than 2 minutes.

- **It is important to 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 EMR being used at the time? Also, what does "unused" mean? Failure to transmit the Rx? No interaction with the computer at all? Does this mean if a prescriber starts but does no transmit the Rx because he or she pauses to examine the patient, and then**

- **If the end point is to avoid prescribing by unauthorized users, the end point of this is the second factor authentication, and a clear indication of each of the controlled substance medications that will be prescribed at that time. It is not clear that anything is added by a lock out after 2 minutes. The most important point is the easy ability to inspect what you are about to e-prescribe and to strongly authenticate (e.g., fingerprint) that I am who I am and I approve transmission.**

 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.

- **To support this, EMR 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.

- **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 DEA does not intend to control the "how" of this but rather leave it to physicians and e-prescribing / EHR vendors to work out the strategy.**

 The practitioner must authenticate himself to the system immediately before signing a prescription.

 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.

- **Would this activity be similar to clicking a button to accept a vendor's license agreement prior to installing a piece of software? This has become a meaningless act that we all perform without thinking about it. This adds no value to the transaction.**

- **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. As we read the DEA proposed rule - it did not seem 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.

- **"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. DEA should word this so the intent is clear that 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.

 The system must not allow printing of prescriptions that have been transmitted; if a prescription is printed, it must not be transmitted.

- **The key to this rule is the definition of "transmitted." 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 fill the prescription, and an acknowledgment has been returned to the prescriber's system.**

- **This is not workable as written given many prescribers prepare prescriptions in advance. Under the current system physicians 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**

- **We suggest the following 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."**

- **Physicians may want to print a copy of the prescription and place in the patient's record. 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 ranges from 15-100%**

The College offers comments on the following proposed Post-transmission Requirements

 The first recipient of the prescription must digitally sign the prescription and archive the digitally signed version of the prescription as received.

 The contents of a controlled substance prescription must not be altered, other than by reformatting, during transmission.

- **Why must intermediaries have the capability to reformat prescription messages? The system would be more secure, and prescribers' liability would be reduced, if prescribers could digitally sign prescriptions. Allowing the intermediary to sign the message makes it impossible for the prescriber to validate its accuracy. Prescribers can not be held liable for inaccuracies in prescriptions if they do not have the capability to digitally sign them. Unless allowed to digitally sign, the prescriber's record of the transmitted prescription must be legally presumed to be accurate in cases of dispute or audit.**

 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.

- **Given that there are circumstances, such as transmission failure, where printing or faxing are appropriate, could an electronically submitted Rx, 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?**

 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.

- **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.**

- **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.**

- **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 physician goes on vacation, must the device travel with him/her. If the physician goes running, must the device go with him/her? We need clarity on what this means and the implications for not keeping physical possession of this key, in the same manner that we keep physical possession of other things.**

- **This is one of the most compelling reasons to make the biometric option available. We always take our fingers, voice, retina and handwriting patterns with us everywhere we go, they never get lost or stolen and we know if we lose one of them almost immediately, in most circumstances.**

 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.

- **The 12 hour 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.**

- **Liability concern - This is not unreasonable to ask for notification of irregularities – but being held responsible is a new level of criminalization of failure to notify that may make most physicians not use this program.**

The College offers comments on the followings proposals related to Audits and Logs

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.

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 electronic prescribing of controlled substances.

- **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 physicians 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 DEA to certify "service providers" (vendors) and "intermediaries."**

- **EHR systems certified by CCHIT are only certified every three years therefore it's unclear why an annual audit is needed.**

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

- **Costs of audits could easily be shifted to prescribers.**

- **It is unclear how a prescriber would know they are purchasing a DEA compliant system that is standalone system since CCHIT only certifies EHRs.**

- **It is unclear how the names of these systems be made widely available to physicians.**

The College offers comments on the followings proposals related to 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.

- **Controlled substance abuse and associated deaths are a huge problem and spending a little time each month to inspect the list for patient and drug**

- **We are concerned that while the DEA phrases this almost as a casual review, ("they do not expect that physicians 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. There must be more clarity around the implications of this review. If a physician is prosecuted for drug diversion, what will this review mean in court?**

- **Electronic-prescription service providers must 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, DEA must 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. DEA must 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 must show that the attempted e-prescription failed.**

    - **Example:**
        - **John Doe, Percocet #30, Sent electronically - transmission failed; fill history - zero**
        - **John Doe, Percocet #30, Printed and given to patient; fill history - filled 8-15-08 by CVS #12345**

The College offers comments on the followings proposals related to Costs

DEA is not aware of any comprehensive data on controlled substance prescription diversion in general, and forgeries in particular. DEA does not track information on prescription forgeries and alterations because enforcement is generally handled by State and local authorities.

The costs to DEA registrants are relatively small. As noted above, the initial costs to the practitioner would range from about $62 to $266 for identity proofing, mostly for the time to have the identification checked. The main ongoing costs for the proposed rule would be the monthly log review by practitioners (about $89 a year) plus any incremental cost of the software or service. The initial and ongoing costs for the basic rule elements represent less than 0.2 percent of the annual income of the lowest paid practitioner.

- **DEA has underestimated the costs for registration, hard token hardware and software, software upgrades, annual system audits, and, especially, for separate prescribing workflows for controlled drugs.**

- **Single Workflow – The cost-benefit analysis presented does not acknowledge the primary motivation for the development of the proposed rules. Congress, the administration, and many public and private institutions have identified e-prescribing as possibly the most beneficial near term HIT function available. One of the major factors inhibiting e-prescribing acceptance among prescribers is the fact that they must use a different workflow for controlled substances. Nothing short of a single, consistent workflow for all e-prescribing activities will supply the anticipated benefits and provide the motivation needed to move prescribers to accept the challenge of e-prescribing. The analysis does not include the added costs for each prescriber every time a controlled substance prescription is written. The comparison should not be with the current system where controlled substance prescriptions require a separate workflow. The comparison should be with a preferred system where all prescribing takes place in a single workflow.**

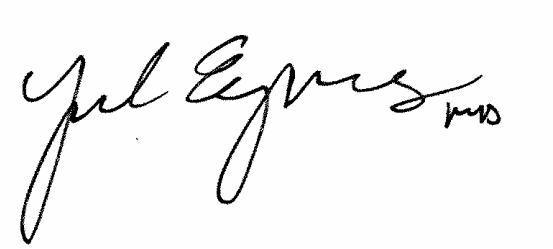
- **While DEA is motivated to minimize the costs of prosecutions, those costs are dwarfed by the potential benefits offered by a single, manageable e-prescribing system. The potential for tremendous societal benefits may be lost in a misguided focus on prosecution costs.**

- **DEA admits that they do not have valid data on the costs to society from diversion. Without valid estimates of the cost of the problem, it is impossible to justify the expense of the proposed solution.**

The ACP believes that the basic regulatory structures outlined in this proposed rule represent a well-intended, positive first step towards achieving the goal of electronic prescribing for controlled substances. The many comments and suggestions supplied above are made as colleagues with DEA in moving towards this goal, and we hope they are accepted as such. We are committed to work with DEA staff to improve on this initial proposed structure and bring the electronic prescribing of controlled substances to realization.

Please contact Thomson Kuhn @ tkuhn@acponline.org or 202 261-4550 if you have any questions regarding these above comments.

Respectfully,



Yul D. Ejnes, MD, FACP, Chair
Medical Service Committee