



Health Record Banking Alliance

May 7, 2010

Drug Enforcement Administration
Attention: DEA Federal Register Representative/OD
8701 Morrisette Drive
Springfield, VA 22152

Re: Docket No. DEA-218, Electronic Prescriptions for Controlled Substances
Electronically submitted at: dea.diversion.policy@usdoj.gov

To Whom It May Concern:

The Health Record Bank Alliance (HRBA) is pleased to have the opportunity to respond to the Request for Comments on the Interim Final Rule for Electronic Prescriptions for Controlled Substances. The HRBA is an alliance of various organizations and individuals with the goal of establishing accurate, secure and complete health records, which can be accessed and authenticated by the patient's health care providers under the control of the individual patient. Information about the HRBA and its principles can be found at: <http://www.healthbanking.org>.

The HRBA is in favor of identity proofing, strong (2-factor) authentication, and logical access control for providers entering patient-related information into electronic health information technology systems. This includes those systems that support electronic prescribing, and specifically the prescribing of drugs on the DEA controlled substances lists. Such trusted information is of benefit to not just the DEA, but to the other patient-authorized users of the information, such as the patient's healthcare providers.

Our primary concern with the Interim Final Rule is that trusted information is a more general requirement. Ideally, all information pertaining to a patient has a verifiable origin that cannot be repudiated. This includes information entered by healthcare providers and by others, such as pharmacies and laboratories. Such information overcomes many objections to the use of electronic health records under the control of patients, since neither the patient, nor anyone else, can undetectably change the information, and the trustworthiness of the source can be independently authenticated.

Since trusted health information is such a general requirement, it is important that the creation of such information be as straightforward and simple as possible. This implies

that common services be used to support trust in health information technology (IT) applications, rather than different services for different sets of information. The Interim Final Rule, while it proposes to use services based on NIST standards, does not clearly allow those services to be used efficiently to support the full range of requirements of the underlying health IT system. In particular, in a health IT system that includes a strong, two-factor authentication requirement for access to the system itself, it is not clear that there is any need to repeat the two-factor authentication protocol at the point of prescribing a controlled substance.

More generally, there are a growing number of proposed uses for Federal and state government and non-government identity proofing and strong authentication that may apply to providers. These include identification and authentication of emergency responders, including physicians, of private healthcare providers working in government facilities, and even of private providers working in private facilities. Use of common “hard” tokens across the full range of environments is desirable to minimize costs and to simplify management of these applications. While the Interim Final Rule mentions some of these potential applications, such as the biometric standards associated with the Personal Identity Verification (PIV) program, it does not address other aspects of the PIV program, including the GSA standard form factor for the hard token, which would assist in interoperability. It also does not mention the PIV-Interoperable (PIV-I) program, which is intended to allow interoperability between Federal government-issued PIV credentials and privately-issued credentials conforming to a specific set of requirements. We recommend that DEA, as a minimum, reference such associated programs, and permit the use of common services that meet the functional requirements of the Interim Final Rule.

Finally, the Interim Final Rule should essentially be a functional specification for a trusted electronic prescription system, including the provider application, the transmission subsystem, and the pharmacy subsystem. In addition, it must specify effective certification and auditing subsystems. Functional specifications for systems of this level of complexity are usually subject to significant modifications as the systems are developed, especially in the case of systems such as this one which are intended to allow interoperability between subsystems created by different developers. While DEA has attempted to simplify some important aspects of the system with digitally signed prescriptions both within the provider subsystem and the pharmacy subsystem, it is still likely that significant issues will arise during development (should the systems be developed by private industry at all, given the cost and limited applicability of the system as defined in the Interim Final Rule). We suggest that the DEA adopt some of the policies and approaches used for Internet for standards development in order to increase the likelihood that systems conforming to the Interim Final Rule are actually developed, and, when developed, successfully interoperate and meet the goals of the Rule. Specifically, DEA should:

- Fund the modification of at least three provider e-prescribing systems to conform to the Interim Final Rule, at least one of which is open source
- Fund the modification of at least two pharmacy e-prescribing systems to conform to the Interim Final Rule

- Fund the demonstration of the successful interoperation of the provider systems with the pharmacy systems
- Modify, as necessary, the Final Rule to incorporate the lessons learned

The HRBA supports the DEA's efforts to develop trusted systems that allow the e-prescribing of controlled substances. The Interim Final Rule addresses many of the problems associated with not only this application, but with trusted health IT systems and information in general. We hope that DEA, HHS, VA, DOD and other Federal agencies take full advantage of the DEA effort to incorporate appropriate identity proofing and strong authentication of providers and other health care entities such as pharmacies and laboratories into our developing interoperable health IT infrastructure.

Sincerely yours,

/s/ William A. Yasnoff

William A. Yasnoff, MD, PhD
President and CEO
william.yasnoff@healthbanking.org