Testimony on E-Prescribing

Overview of Electronic Prescribing

Submitted to the National Committee on Vital and Health Statistics

Subcommittee on Privacy and Confidentiality

Presented by

G. F. Brown

Mayer, Brown, Rowe & Maw LLP

November 18, 2004

Good morning and thank you for the opportunity to testify before the subcommittee on electronic prescribing.

My name is G. F. Brown, and I am an attorney with Mayer, Brown, Rowe & Maw LLP in Chicago. I specialize in technology law. In the early nineties, I was a computer programmer and worked on the first version of Microsoft Outlook. Clients to whom I have provided advice include the Secure Access For Everyone (SAFE) Initiative, which is giving testimony here today, and RxHub LLC, which provided testimony to the Subcommittee on Standards and Security earlier this year. On behalf of RxHub, I attended several of the Subcommittee on Standards and Security hearings, which culminated in recommendations that are part of NCVHS's initial recommendations to Secretary Thompson dated September 2, 2004. However, I do not today testify as attorney for the SAFE Initiative, RxHub or any other client.

Since most of the members of this subcommittee have not been actively involved in the review of electronic prescribing that the Subcommittee on Standards and Security has undertaken, I will first say a few words about the present state of electronic prescribing. I will then offer some observations about privacy and confidentiality issues raised by electronic prescribing.

Background on Electronic Prescribing

NCVHS's September 2 letter to Secretary Thompson provides an excellent brief introduction to electronic prescribing.[1] In its summary, NCVHS cites an estimate that "e-prescribing systems can avoid more than 2 million [adverse drug events] annually, of which 130,000 are life threatening".[2] Not only does electronic prescribing have the potential to save lives, but electronic prescribing also has the potential to save money. According to NCVHS's letter, some estimates put the number of dispenser calls to prescribing physicians at 900 million annually[3] – which results in a huge cost for both pharmacies and physicians' offices. The benefits of electronic prescribing appear substantial, and conversely the costs of delaying implementation of electronic prescribing are high.

Electronic prescribing achieves its benefits in two broad ways. First, it makes the current process of writing and transmitting scripts from the physician's office to the patient's pharmacy of choice more efficient. Electronic transmission can reduce or eliminate handwriting issues at the physician's office, key punch errors at the pharmacy, and the need to keep paper records of prescriptions that have been filled and refilled. However, a second benefit is that electronic prescribing, at least as envisaged by the Medicare Prescription Drug, Improvement, and Modernization Act of 2003 (MMA), also encompasses systems that provide the prescribing physician at the point of care with electronic access to information such as patient medication history, drug information, formulary and other coverage status. This additional "front-end" information can help physicians screen for adverse drug interactions, prescribe on-formulary, and thus write safer, more cost-effective, prescriptions.

Stakeholders in Electronic Prescribing

The health care community has taken several strong steps towards implementing electronic prescribing. One key organization has been the National Council for Prescription Drug Programs (NCPDP). NCPDP will be known to many here as the ANSI-accredited standards development organization that is responsible for several transaction standards under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). NCPDP is the also the source of the SCRIPT standard (not one of the HIPAA-mandated transaction standards). NCPDP SCRIPT is used by most electronic prescription providers to format prescriptions electronically to be sent from a prescribing physician's office to the patient's pharmacy of choice. There are, however, other formats for electronic prescription messages, including those developed by Health Level Seven (HL7), which are commonly used in hospital and clinical pharmacy environments.

---

[1] See http://www.ncvhs.hhs.gov/040902lt2.htm.

[2] NCVHS Letter to Secretary Tommy G. Thompson (Sept. 2, 2004), page 2 citing Center for Information Technology Leadership. The value of computerized order entry in ambulatory settings. 2003.

[3] *Ibid*., page 1.

Although NCPDP SCRIPT standardizes only the electronic encoding of a prescription, NCPDP has begun considering other standards for the request and delivery of "front-end" information to the prescribing physician such as medication history and formulary information. NCPDP's procedures for extending its existing standards and developing new standards for electronic prescribing are open, and participating in NCPDP task groups does not require membership in NCPDP. NCPDP serves an important role in the future of electronic prescribing by providing a forum for discussing and improving standards, which is especially needed in electronic prescribing because of the large and growing number of stakeholders in the electronic prescribing arena.

The list of stakeholders in electronic prescribing begins with the same list of stakeholders in the non-electronic prescribing environment: prescribing physicians, pharmacists and patients. To these stakeholders, electronic prescribing adds: 1) point-of-care (POC) technology vendors, including hardware manufacturers and software providers; 2) "front-end" information sources, including formulary providers, medication history providers, drug information sources, etc.; and 3) information routers, including entities such as SureScripts and RxHub, which link together physicians, pharmacists and "front-end" information providers.

Today, there are several POC vendors, most of which are relatively small companies, and none of which is dominant in the marketplace. POC vendors market a diverse set of user interfaces, deployed on a number of platforms including wireless handhelds, desktop systems, etc. There is less diversity in methods of back-end processing, however, because POC vendors must interoperate with multiple counterparty systems and certify with information routers (both RxHub and SureScripts have a certification process).

There are several electronic prescribing "front-end" information sources. Providers of formulary and coverage information currently include health plans, pharmacy benefit managers (PBMs), and third-party aggregators. Health plans and PBMs can also provide medication history information on patients they cover by using their claims records. Providers of drug information include FDB, Medispan and Multum. Pharmaceutical companies can also provide information on the drugs they manufacture.

Information routers such as SureScripts and RxHub serve to tie the many other electronic prescribing stakeholders together. They provide links to and from the prescribing physicians' offices, pharmacies and data sources. Both SureScripts and RxHub are largely invisible to the prescribing physician and patient at the point of care – the POC vendor incorporates the SureScripts or RxHub functionality (or both) into the POC's service offering, permitting the prescribing physician easy access to the pharmacies and data sources in the information router's functionality.

Privacy and Confidentiality Issues

Privacy and confidentiality are key concerns throughout the electronic prescribing community. On a federal level, both prescribing physicians and pharmacists are covered entities under the HIPAA privacy regulations. All of the electronic prescriptions

described above and much of the "front-end" information (i.e., all information that is identifiable to a patient, but not information only about a drug or formulary) are protected health information (PHI) as defined by HIPAA's privacy regulations. However, the information, including the "front-end" information, is used and disclosed for treatment purposes – as part of the prescription-writing process – and thus benefits from the special provisions available under the HIPAA privacy regulations (e.g., the exceptions from the accounting of disclosures requirements). Of course, all of the electronic prescribing information that is PHI under the HIPAA privacy regulations is also covered by the requirements of the HIPAA security rule, which governs use of electronic PHI. Covered entities such as physicians and pharmacists must comply with (and document their compliance with) the provisions of the HIPAA privacy and security regulations.

The HIPAA privacy and security regulations require prescribing physicians and pharmacists to impose privacy and security requirements on other electronic prescribing stakeholders (whether or not those other stakeholders are themselves covered entities) through business associate agreements as defined in, and required by, the HIPAA regulations. A key requirement in all business associate agreements is that such agreements, with few exceptions, must prohibit the business associate from using or disclosing PHI "in a manner that would violate the requirements of [the privacy regulations], if done by the covered entity".[4] For example, if a certain use of PHI would qualify as "marketing" by the prescribing physician, the physician's POC vendor, as his or her business associate, must not make that use of the PHI.

Electronic Signatures

In light of the workplan published with NCVHS's September 2, 2004, letter to Secretary Thompson, which contains plans for several upcoming sessions of subcommittee testimony on electronic signatures in general and public key infrastructure (PKI) digital signatures in particular, and the testimony this morning of the SAFE Initiative, I will say a few words about the use of digital signatures in electronic prescribing.

Neither the HIPAA privacy regulations nor the HIPAA security regulations mandate the use of electronic signatures (whether or not PKI-based). Under the security regulations, covered entities must assess electronic mechanisms to corroborate that electronic PHI has not been altered or destroyed in an unauthorized manner and to track the identity of the person transmitting the PHI,[5] but here is no specific guidance on the use of electronic signatures. This is true even though draft regulations issued by the Department of Health and Human Services (HHS) did address electronic signatures. According to the preamble to the final HIPAA security regulations, HHS decided to delete electronic signature standards from the final security regulations and to issue a separate regulation on electronic signatures.[6] As of today, no separate HIPAA electronic signature regulation has been published.

---

4 45 CFR 164.504(e)(2)(i) and 164.504(e)(2)(ii)(A).

5 45 CFR 164.312. See also, explanation of the term "addressable" in 45 CFR 164.306(d)(3).

6 68 Fed. Reg. 8334, 8335 (Feb. 20, 2003).

As others will testify in more detail, PKI digital signatures provide high levels of authentication, non-repudiation and integrity of transmissions. However, most electronic prescription programs do not include PKI digital signature capabilities. In part this is because NCPDP SCRIPT does not include a data element for electronic signatures (PKI-based or otherwise). NCPDP is currently sponsoring a task group to evaluate the use of electronic signatures in the SCRIPT standard. That task group is preparing recommendations that will be available later this year or early next year. However, it should be noted that most electronic prescribing systems require the prescribing physician to identify prescriptions as his or hers by using some electronic mark – and this identification likely qualifies as an electronic signature as defined by the Electronic Signatures in Global and National Commerce Act (ESIGN).

In addition to adding an electronic signature data element to the NCPDP SCRIPT standard, there are other technical challenges that will need to be overcome before digital signatures can be standardized in electronic prescribing. For example, the script digitally signed by the prescribing physician may not be identical to the script received by the dispensing pharmacy. Testimony before the Subcommittee on Standards and Security identified several places where the data that a prescribing physician submits for a script may be changed before it reaches the dispensing pharmacy. These changes do not alter the content of the prescription, but do invalidate the prescribing physician's PKI digital signature. For example, a prescribing physician likely enters the name of the prescribed drug, which the electronic prescribing system may translate to a code. The translation may occur at the POC vendor's server rather than at the physician's device because the translation databases are located there. Similarly, an electronic prescription submitted in NCPDP SCRIPT format may be translated to HL7 or vice versa. In each case, the prescribing physician's PKI digital signature will not be associated with the prescription as received by the dispensing pharmacy. The electronic prescribing and PKI communities will need to resolve these technical challenges in the context of electronic prescribing.

Although PKI digital signatures would provide higher levels of authentication, non-repudiation and integrity of electronic prescribing transmissions, current electronic prescribing systems do provide more protection than paper-based systems. Since prescription pads can be stolen or forged, there is no guarantee that prescriptions are secure in a paper-based system. Depending on a pharmacist's knowledge of the patient, prescribing physician, quantity of drug prescribed, other known medications of the patient, and other factors, the pharmacist may call the prescribing physician to verify a paper prescription. However, such verification is subject to the professional judgment of the pharmacist and cannot detect all forgery and tampering, without an undue burden to the current paper-based system.

Today's electronic prescribing systems, even without electronic signatures, implement user authentication procedures to guard against unauthorized access by prescribing physicians, pharmacies and others. Moreover, many electronic prescribing systems offer channel encryption capabilities, which protect the integrity of the script transmission.

These protections allow electronic prescribing to be more secure than the current paper-based prescribing system.

State Law Issues

In addition to federal regulation, electronic prescribing systems are subject to state privacy laws and regulations that are more stringent than the federal HIPAA requirements. In fact, some states make it very difficult to implement electronic prescribing, and at least a couple do not allow electronic prescribing at all.[7] There are several types of state laws and regulations that affect electronic prescribing, including some related to privacy and confidentiality of health information. For example, many states require that, prior to transferring information about certain drug treatments (e.g., HIV treatments), the source of the information must obtain the consent of the patient. This poses particular problems to physicians requesting medication history. In order to get a complete medication history on a patient, the physician must obtain the consent of the patient and find some way to transfer evidence of the patient's consent to the source of the patient's medication history. Today there is no standard for transmission and validation of such consent. Thus, some information sources remove information about a list of sensitive drug classes from all medication history – which reduces the value of the medication history to the prescribing physician.

Another example in several states is "anti-depot" provisions that prohibit parties other than the dispensing pharmacy from collecting prescriptions. These could be interpreted as prohibiting information routers from electronically receiving and routing electronic prescriptions. Even prohibitions on third parties opening prescriptions may be interpreted as prohibiting an information router from reading routing information on a prescription (even if the router never accesses the content of the prescription).

Conclusion

A comprehensive set of standards can promote the benefits of electronic prescribing by clarifying how existing privacy, confidentiality and security laws and regulations apply to electronic prescription systems. The challenge for the electronic prescribing standards is to promote the objectives of existing privacy, confidentiality and security regulations while at the same time promoting the early success of electronic prescribing envisaged by the MMA and the electronic prescribing community.

Thank you again for the opportunity to testify before you today.

[7] See written testimony of the National Association of Boards of Pharmacy to the NCVHS's Subcommittee on Standards and Security dated July 28, 2004, which identified South Carolina and South Dakota as not allowing electronic transmission of electronic prescriptions.