Testimony of

David C. Miller

December 4, 2007

Congressional Testimony
December 4, 2007
Written Statement of
David C Miller
Chief Security Officer
Compuware Covisint

Introduction

Chairman Leahy, Ranking Member Specter, and distinguished Members of the Judiciary Committee, I want to thank you for the opportunity to discuss electronic prescribing of controlled substances. Given the fact that all types of communication in our country are shifting away from face-to-face in favor of electronic media, it is vital that we consider the advantages of electronic commerce in all areas of the economy. This holds particularly true in the healthcare industry where controlling costs, protecting privacy and sharing information effectively will have an impact on every United States citizen.

In the years that I have been working as a security expert at EDS, IBM, General Motors, and now with Compuware Covisint, I have become very familiar with the challenges related to securing transactions on the public internet, considered by some to be an inherently insecure network. Covisint was created to leverage the internet in a secure way, such that automotive companies could take advantage of the technology without being exposed to this risk. As a result, Covisint's solution evolved as a unique information sharing hub providing a service for communities of interest to collaborate and securely exchange information.

The concerns of the automotive industry parallel those of the DEA in e-prescribing controlled substances, albeit for different reasons. In building a secure information sharing hub, the Covisint solution had to manage these electronic communications; it was our responsibility to create a system that could support the secure communication issues of a diverse community while keeping cost and implementation time to a minimum.

As Covisint expanded its business landscape and grew into other industries (healthcare, law enforcement, financial services), we saw the same sort of challenges. Healthcare systems need to interact with each other, sending highly personal data back and forth, while maintaining compliance to HIPAA regulations. In law enforcement, Covisint helped create an information-sharing pilot for the Department of Justice to use in sharing sensitive terrorist-related information between law enforcement agencies. In each case, the challenge was to balance security with implementation cost and complexity. In a nutshell, a security solution that cannot be implemented or is only partially implemented may be worse than no security at all. What we have done for these institutions is to find that balance.

Electronic Communications Offer Security Advantages
Although some believe that paper-based transactions such as medical prescriptions are inherently secure, I believe that this is often not the case. Paper transactions are hard to track and manage. Paper transactions involve manual processes that are particularly vulnerable to human error. Paper transactions are difficult to store and retrieve without redundant processes to enter the transaction into an electronic format. Paper transactions are subject to a declining adherence and a declining attention to process as the people involved are asked to simultaneously support both the paper-based process and an electronic-based process. Although paper transactions can include a physical signature, this method of authenticating is based solely on the assumption that the recipient can successfully distinguish one signature from another.

In days past, we always went to the same doctor and always visited the same pharmacy. Doctors had relationships with pharmacists such that a voice and signature were readily recognized. Even doctor's prescribing habits were recognizable by pharmacists. Pharmacists often picked up the phone to verify or inquire about the validity of a prescription. The days of tight relationships between doctors and pharmacists are quickly disappearing. And the weakening of these relationships weakens the ability of pharmacists to validate signatures, recognize prescription patterns and otherwise ensure security associated with the paper process.

So what is the solution? Electronic transactions, whether on the internet or over a private network, offer us the best alternative today. With a set of electronic transactions, the prescribing activity of physicians can be tracked and monitored. Electronic transactions minimize human error and detect irregularities in activity. Electronic transactions are easy to store and allow extensive search capabilities. Processes in the electronic system can be highly controlled via predefined workflow. Electronic systems offer a variety of methods for authenticating the user and ensuring the user's authority to perform the transaction.

In terms of checks and balances, electronic transactions:

- can be supplemented with physical signatures, which can be faxed and appended to the transaction.

- can incorporate alerts and triggers in the workflow, for example alerting doctors of certain physician activities, such as prescribing a controlled substance. This is known as a closed loop transaction.

- can monitor pharmacies and warehouses to ensure their accuracy and honesty in filling and shipping prescriptions.

As demonstrated by these examples, it is important to remember that information security looks at both "bad guys" who are intruding on the system and "good guys" who have legitimate access but may abuse their access.
In general the advantages to e-prescribing are:

1. An audit trail

With an electronic log of what is sent, when it is sent and who received it, you can provide true audit capability. This is important when you need to understand the patters of prescribing for physicians.

2. Real-time tracking

Electronic methodologies happen in real time. With paper-based systems it can take weeks for a trend or abuse to surface. In the electronic world, these activities are visible as they happen.

3. Transparency

In the electronic world, there is always an audit trail; a physician or pharmacist cannot hide their activities. This generic visibility creates transparency. Transparency is also a deterrent, as users are aware that they are constantly being monitored. The paper world offers opportunities for people to mask their activities.

4. Event alerts

As a result of the electronic nature of e-prescribing, monitoring for abusive behavior takes place real-time and provides alerts that can be acted on prior to dispensing the medication. With paper transactions, people need to be involved, and they become the bottleneck.

5. Trend and historical pattern analysis

Often the only way to see abuse is to discern patterns in historical data. This historical data could be millions of records over many months. In the paper world, managing this amount of data is difficult at best, impossible at worst. With electronic transactions you can do trend analysis in seconds instead of months.

Complexity of Securing Electronic Transactions

When considering the approach to secure these electronic transactions, the temptation is to implement the most sophisticated and secure technologies that are available to the industry. This can often be the death of an implementation. I have seen many cases of the security of the implementation being so complex that the users of the system have either found ways around the system, thus defeating the security implementation, or have made up excuses as to why "it won't work," and thus abandoning the system altogether.

In information security today, Public Key Infrastructure, or PKI, is that "sophisticated and secure technology." Although PKI- based authentication methods provide some superior functionality, the current state of the technology brings with it major implementation and usage challenges:

- The heart of the system relies on a very long numeric key. This key would be impossible for a user to memorize, so it is stored on a device called a container. This container can be a PC, or a card that understands PKI (e.g. a smart card). The key requirement is that the container if physically available to the prescribing physician. Thus, if the physician forgot his card or his PC is broken, no authentication can occur and no prescribing can occur. The physician is unable to perform a key task until the container is recovered. In addition, many PCs cannot handle the PKI container requirements and would need to be upgraded.

- Because the container or device holds the key, it too must be secured. In most cases, this requires some sort of pass phrase or password to use the key which unlocks the container. So in the end, a password is the true security method. Anyone who shares that password and allows others access to the container can circumvent the security.

- Access to the container is paramount. If you are out of the office without your PC, then you would not be able to access the system. At face value this may seem like a good thing, but experience tells us that in today's world you cannot guarantee where a person is located when working. Many times physicians need to access their e-prescribing system while on call after hours, but without their work computer present at home, or wherever they may be, they cannot utilize the system. Or imagine if after Hurricane Katrina no physicians in New Orleans could provide healthcare because their computers were all underwater.

Proven Alternatives

So if solutions such as PKI won't work, what alternatives do we have? I believe that by combining technology, process and oversight a solution can be provided that allows for appropriate levels of security for controlled substances while providing all of the advantages of e-prescription. This technique will allow for the authentication, integrity and non-repudiation, which we all want.

The components of this solution include:

- A robust authentication capability
Authentication is very important to the implementation of a secure, transaction-based system. We all know the problems with passwords, such as:

a. Users write down good passwords (difficult to guess)
b. Users can memorize bad passwords (easily guessed)
c. Passwords are prone to hacker attacks

In my experience there are additional technologies that can mitigate this. Multi-factor technologies allow an added degree of protection while still allowing for reasonable implementations.
For example one time passwords are a method whereby the user is required to enter the code that is presented on a

device that he carries all the time - such as a cell phone or keychain fob. Additionally, the user must enter a password that only he knows. The advantage of these "token" based technologies is in order for another user to access as the original user they need to both have the device and know the password. The advantage over PKI is that the device in this case requires no computer interface such as the PKI container and thus can be used on any PC.

Another type of authentication is knowledge based. In this model the user is asked a set of random questions that only he would know. This along with the password provides a two-factor system. This is exactly what is being used in many web banking systems in direct response to guidance from the FDIC.

- A group of trusted identity providers
Another mitigating control is to identify a group of trusted identity providers or credential providers. The identity providers would need to be vetted as capable of providing highly secure authentication technology. The benefit of these organizations is that they allow users to leverage existing identities and thus reduces the number of passwords for a given user. Audit and logging capabilities would still be managed at the user level. Examples of possible identity providers would be large health systems, universities or major payer organizations or any trusted, technology-capable organization in the supply chain. This exact method is being utilized as part of both the e-authentication initiative and the Federal Law Enforcement Information Sharing Program (LEISP).

- Third party "trusted broker"
Organizations often have a need to share transactions with each other where the organizations may not have complete trust with each other, or there is concern that organizations could collude to circumvent the process. In these cases, a third party trusted broker that has visibility to all of the transactions can facilitate an implied trust relationship while monitoring the community for non-compliance or collusion.

- A consistent policy
Regardless of the technical approach, a consistent policy needs to oversee each of these possible implementations. This policy then can be implemented and enforced by the third-party trusted broker.

- An oversight organization
As with any community it is imperative that an oversight organization be in place (e.g. DEA). This organization can draft and own the policy, manage and monitor the hub, and determine which technology is best suited for each implementation. It can also be the coordination point for the migration activities that will have to occur.
Conclusion

Ultimately, the success of any system is all about adoption. Getting the constituents to adopt a new methodology will require selection of a cost-effective, simple and secure solution. I believe that there are simple-to-use authentication technologies, which--when partnered with policy and oversight--can achieve adoption within the whole healthcare community. This approach can also overcome the security concerns associated with enabling the e-prescribing of controlled substances. I have seen this approach work successfully in many industries over the past seven years and believe it has real merit and deserves further consideration.
Chairman Leahy, and members of the Committee, I thank you
for the opportunity to discuss this vital issue and welcome any questions you may have.