Presentation By Cerner Corporation
To the
National Committee on Vital and Health Statistics (NCVHS)
Hearing by the Subcommittee on Standards and Security
On
The Impact of the HIPAA Security Rule on Healthcare Information Systems

Presented by: John Travis
Director
Solution Management
Information Security and Privacy
January 27, 2004

I want to thank you for the opportunity to come before the subcommittee to share Cerner's observations on the state of the market for healthcare information systems with regard to compliance with the HIPAA Security Rule. Cerner is a leading healthcare information systems company with over 5000 associates and over 1000 provider clients both in the United States and internationally. We are exclusively focused on automating the clinical processes for the delivery of healthcare for health systems, hospitals, clinics and individual providers. Personally, I have overseen Cerner's development efforts to assist our clients with matters of security and privacy compliance. I want to start out by sharing some observations of the current state of the market, and then discuss key challenges for the industry for compliance. I will conclude with recommendations to the subcommittee on areas we believe are significant for the subcommittee's attention.

The Current State

Most provider organizations are faced with making do with a significant inventory of existing systems, Providers are also attempting to take a more strategic view of security at an enterprise level. Several observations can be made about the way security has traditionally been approached in healthcare information systems:

- Each system vendor has tended to solve security in its own way
- Few vendors have prepared their systems to support dealing with security strategically at an enterprise level
- There has been a lack of security standards development, guidance or adoption within healthcare information systems until very recently.
- Few organizations have to treated security strategically although it is becoming an important function to perform at an enterprise level

Provider organizations have a choice to make in their compliance programs.

- To try to work with existing systems as they are, and hope vendors will provide upgrades where needed
- To try to improve security capabilities through investment in new technologies and system replacements so as to reduce costs to administer systems and to standardize security practices at an enterprise level

Providers that attempt to take the latter course as their compliance strategy may have to plan for a long term compliance horizon for getting individual vendor solutions replaced or upgraded to support an enterprise approach while dealing with the mandatory requirements of the rule in the short run as best they can.

Administratively, providers often are formally defining clear policies for access rights of users for the first time. It is very probable that system security was left to the imagination of individual system managers or department managers responsible for individual systems with little thought of standardizing access controls across the organization.

Challenges for Implementation and Compliance

As providers look to comply and improve current security practices, what are the challenges?

Policy Definition

First, providers have to have clearly defined security policies and procedures to guide how security is set up in systems. Providers should have well defined roles for users that guide the assessment and the definition of what clinicians and staff can see and do in systems that store patient data. For most organizations, the definition of roles within systems likely was done inconsistently over a long period of time between different vendor systems. There is no guarantee that a role in one system holds any meaning for another system. There has only recently been standards based work to propose standard roles for healthcare that would give providers guidance to normalize meanings.

Most providers linked the development of such security policies to their Privacy rule compliance efforts. This was done to deal with patient information privacy policies at the same time as defining what staff members could see or do with patient information. As a result, many providers are well down the line in terms of defining security policies, and in assessing their systems for support of these policies. The remaining task is to make sure that the systems support these policies in a consistent way without undue administrative costs to achieve that support.

Single Sign On and Single Point of Administration

Second, for those providers who see the Security rule compliance effort as a chance to reduce administrative costs for security and to standardize within their organization, we are seeing them focus on two key strategies. First, providers are trying to implement so called single sign-on (SSO) solutions. These allow a user to sign on once and be able to access systems they have rights to without having to sign on again and again. Second, providers are trying to use tools that allow users to be set up once and have all systems share user information in common. There are available technologies to do both. However, many older existing systems require both of these processes to happen within each system. So if each system vendor offers a different level of support or set of options for these problems, providers are left with a security infrastructure that is difficult to administer. To support single sign on, providers require individual vendor systems to be able to accept that sign on.

A great deal of administrative cost for security management could be reduced if providers could manage user information centrally. Again, the technologies are largely available. These technologies allow for user information, roles and role based access rights to be established once, and then the information can be shared between systems. However, providers are faced with the limitations of existing systems to be able to share such information because such systems often require this information to be manually set up within each system. Standards work has been underway for years within HL7 to promote exchange of personnel information and security information between systems so as to make this process easier.

While single sign-on and centralizing and standardizing security information may not be literal compliance requirements, they are initiatives many providers wish to consider investing in as they deal with compliance efforts.

Digital Signatures

Although an electronic signature requirement was scoped out of the final Security rule, the need for secure and reliable electronic signature methodologies in healthcare grows. At a recent meeting of HL7, the committee chair responsible for medical records stated that the lack of standards or regulatory requirement for electronic signature federally would dampen the use of the web for sharing patient information. Historically, this has not been a significant issue because many vendor systems were "closed". Systems only sent information to each other within the same organization. As areas of e-commerce emerge for sharing patient information between organizations such as e-prescribing, the importance of trusting the web becomes more significant. One key to that trust is to have reliability in electronic signatures. We encourage the Secretary and the committee to promote proposed rule making and standards development in this area.

Accountability and Audit Systems

The most challenging and costly aspect of Security rule compliance may be implementing audit systems for how patient information is used or disclosed. This will be a leading cause of system replacement or upgrade. There are several contributing factors to this.

First, many existing systems do not provide for an adequate level of auditing. This is particularly true if patient information is only inquired or printed. Many systems only offer auditing when patient data is created or changed. Enabling audit of inquiry or printing often is a major system enhancement. So the availability of auditing may prove problematic to older systems still in use. Most vendors have addressed this issue in newer versions of systems. That is why this particular matter may lead to system upgrades more often than system replacements.

Second, good security practice requires audit information to be stored securely and separately from the systems that store patient information. For patient care systems that do provide capability to audit how patient information is used; many of them do not provide secure audit logs or store the audit data as part of the patient record. As a result, a security auditor has to access many logs to get a complete picture. This problem is most easily solved by having an organization level audit log. The log can draw from each patient care system and present one whole audit trail. This is not the current state of the market, but it needs to become that.

Third, only draft standards are available for healthcare providers to try to share audit data between patient care systems and an audit system. HL7, ASTM and DICOM have come together to propose a common audit standard that should help solve the problem, but it is a ways from adoption. Some vendors have designed auditing around this standard prospectively, but mostly for newer versions of systems. Providers are usually left with incomplete ways to get audit data for whatever they can find. Audit data gathering can be tedious, requires knowledge of how systems are designed and custom programming to get at the data. There are no guarantees that a very complete picture of accountability emerges in such a state.

Importance of Standards

I have highlighted the importance of standards and guidance to the healthcare information systems industry in the areas of auditing, personnel/user management and other areas. Our main point is that healthcare IT has suffered from a lack or lateness of standards adoption or availability. Unlike HIPAA EDI where standards were strongly supported by regulation and industry consensus, that has not been the case for security under HIPAA. The more that can be done to promote the adoption of standards within healthcare IT relative to security, the better.

Treating Security as an Organization Level Problem to be Solved

We feel that providers need to try to solve security strategically. Vendors also should back the use of standards that enable consistent definition of security policies at an enterprise level, and provide

support for using security tools that reduce costs of administration and provide user convenience for accessing systems.

There are good examples in the provider community of organizations attempting this. The VA is taking a leadership role to standardize user roles, and is suggesting such a model for healthcare information systems. Many organizations are implementing the kinds of security tools discussed earlier to ease the burden of security administration. The need to treat auditing as problem to be solved once for an organization lags behind these other areas, but it too needs to be dealt with in that manner.

While it may not be the government's role to encourage particular tools or techniques, it may be appropriate for best practice development to be encouraged. Interpreting and providing working examples of what organizations have used successfully (such as was done with WEDI SNIP for HIPAA EDI) needs to be encouraged.

Balancing Access with Privacy

Now that the Privacy rule has been in effect for 9 months, the industry has had ample opportunity to take measure of its impact.

Many of our clients have taken advantage of our systems to improve the protection of patient information without our having to undertake any coding changes. We see that as our clients implement our systems, security and privacy are becoming standard focuses for new electronic medical record projects. Our clients have provided valuable feedback to our offerings we have incorporated to improve our capabilities.

However, we are finding an interesting situation emerging. It seems many organizations are treating compliance as primarily a legal problem and not an operational one. Many long-standing practices have had to change about how patient information is handled and disclosed. For example, we repeatedly have had clients ask for our advice about whether or not faxing should even be used, and that faxing is in itself a non-compliant practice with HIPAA. Some provider organizations have behaved as if protecting privacy is the primary role of information systems without due consideration given to the role of information systems to automate the business processes within healthcare.

This poses a challenge (and possibly a threat) to proper patient record access and use. We encourage the NCVHS to consider recommending to the Secretary that guidance and reasonable perspective be given on the Security rule, just as the Office of Civil Rights provided on the Privacy rule. Currently there is much speculation on what a "compliant" system is, and much is left in the eye of the beholder. For example, the limited amount of standards based guidance on healthcare roles leaves providers to determine this for themselves at a time when they are trying to reconcile roles across systems within their enterprises.

Enabling Community Information Sharing

Finally, there is one last issue that is much related to the previous issue. The issue is whether or not the Security rule works well with other regulations to promote proper sharing of electronic health information between healthcare providers. It seems desirable for the government to wish to promote examples of appropriate information sharing practices between community members, and a good example for this is embodied in the recently passed Medicare prescription drug legislation for e-prescribing. As we observed in the Privacy rule amendment process, and in the guidance given to covered entities regarding eligibility practices, processing prescriptions and the like, sometimes the literal interpretation of regulation goes too far and retards the very thing it was to assure happens properly. We see many provider organizations that make a determination to remain closed, and to only disclose information when there is absolute written proof of patient permission for disclosure, even related to care. We also see great desire on the parts of many provider organizations to share properly with each other and to promote such sharing within a community to better the care delivered to patients they all share in common. This is retarded by the fact some organizations interpret the Privacy and

Security regulations as making a presumption that electronic health information is held only within provider organizations, and somehow should not be at a community level or that community sharing is only possible with very burdensome administrative and technical conditions applied.

We encourage the committee to consider taking a position on proper information sharing practices that can encourage enabling electronic community level health records. We believe that the government has a strong interest in the promotion of electronic health record standards that include appropriate information sharing as an important goal. A personal and portable electronic health record is an important future objective for healthcare information systems. It is the vehicle by which real patient rights towards their record can begin to be realized. We believe the US healthcare system has an interest in promoting good model frameworks for how to reconcile the security and privacy requirements for the health record with the community level information sharing objectives important to such a health information structure.

Recommendations

To summarize our recommendations to the committee, we believe the following are important to consider:

1. The promotion of the use of standards in healthcare information systems security. We have identified several key areas of emphasis:

    a. Healthcare roles for users

    b. Audit

    c. Exchange of security information between systems to reduce administration costs

    d. Electronic (digital) signatures

    Standards work is available or nearly available in most every significant area. We do not necessarily suggest a formal DSMO process for their adoption, but we recommend that their adoption be given a strong backing by the NCVHS

2. The development of guidance or best practices around what constitutes proper and appropriate information sharing practices especially at a community level so as to promote an effective balance of privacy and availability of patient data

3. Consideration for best practice sharing through a process similar to WEDI SNIP

In conclusion, the Security rule compliance period catches the healthcare information systems industry between an era when it was OK for vendor solutions to worry only about their own systems, and an era when healthcare is moving rapidly towards enterprise solutions. However, there still is quite a bit of existing system inventory in place that serves to hinder the pace of that progress. Providers do not have the budget in many cases to both re-mediate systems and move to adopt enterprise solutions. The last comment I can leave you with is that much consideration should be given to the good faith efforts of providers and their vendors to enable compliance in the design of the enforcement regime for the Security rule as I am certain many providers will be in the process of implementing their plans come April, 2005 because of the choices they have to make between remediation and improvement.

On behalf of Cerner, I would like to thank the subcommittee for the opportunity to present Cerner's observations and recommendations on this critical matter.