Security and the Health Care Provider
George Harrington

Traditionally health care has lagged behind other businesses in the move toward computerized records and communications. This is primarily due to the one on one relationship between Physician and Patient. However, within the past several years there has been a drive to move from a paper based system of record keeping and communications to paperless data collection and transfer. In this paper, I plan to explore some of the security concerns faced by the Physician's Office now and in the future. I plan to address three areas, Physician/Patient communication, Electronic Medical Records, and Use of Portable Devices.

Physician/Patient Communication

With the increasing use of E-mail as a means of communication, there is an increasing desire by patients to communicate with their physicians via E-mail to ask questions, make appointments, renew prescriptions, etc.

In a white paper, the *Journal of the American Medical Informatics Association* addresses the issue of physician/patient communication via e-mail. They layout some basic guidelines to maintain the security and confidentiality of e-mail between the physician and patient. These include:

- Consider obtaining patient's informed consent for the use of e-mail.
- Use password protection for all workstations involved in physician/patient e-mail.
- Never forward patient-identifiable information to a third party without the patients written consent.
- Never use patient's e-mail for marketing purposes.
- Do not share professional e-mail accounts with family members.
- Use encryption.
- On unencrypted messages never include patient identifiable information.
- Double check address fields.
- Perform routine backups of mail systems for long term storage.
- Commit policy decisions to written and electronic form.

The Health Insurance Portability and Accountability Act (HIPPA) and the associated rules being developed by the Department of Health and Human Services (DHHS) specifically address three of the guidelines above.
First, the physician must ensure that all workstations that participate in e-mail must be physically and technically secured.

- Workstations should not be placed in areas where unauthorized persons could gain physical access.
- All workstations/e-mail systems should require some form of access control, which should include unique user identification, and one of the following additional identifiers. Biometrics, a password system based on good password practice, a personal identification number (PIN), telephone callback for off site systems, or use of a physical device for user identification.
- All workstations provide for automatic user logoff.

- All workstations and e-mail systems should maintain audit controls to record and examine system usage.
- All workstations and e-mail systems should be routinely scanned for viruses.

Second, the white paper and HIPPA both address the need for routine backup of e-mail. The standard recommendation is that if e-mail is to be used in physician/patient communications the backups should be held in a secure location for the same period of time that paper records with the same information should be kept. HIPPA also includes the addition that backups should also be routinely stored in an off-site location. Also, HIPPA defines a secure location as a locked room or closet with limited access by unauthorized persons or staff.

Finally, the white paper discussed the use of encryption schemes and recommends that physician/patient communication be encrypted. HIPPA on the other hand will mandate the use of encryption where patient data is communicated in electronic form. Also, HIPPA mandates the DHHS work with the Department of Commerce in development and implementing a digital signature standard. For the physician this means, that any e-mail between physician and patient that contains patient information must be encrypted and should be digitally signed if there is a need for a signature. However, both the encryption and digital signature standard have yet to be defined. Most of the comments to the DHHS on the proposed Security and Electronic Signature Standards rules seem to favor the use of PGP or similar PKI systems.

Electronic Medical Records (EMR)
The use of EMR systems has traditionally been by hospitals or other large medical facilities where there was a staff devoted to information technology. However, as the cost of these systems comes down may smaller physicians groups are beginning to use EMR systems and it is necessary to examine the security ramification of having such systems.

Since EMR systems contain patient data of the most sensitive nature, the highest level of security needs to be maintained on them. The Security and Electronic Signature Standards being developed by the DHHS as part of HIPPA clearly cover the security requirements for EMR systems. These security requirements can be broken up into two areas: Organizational Practices and Technical Practices.

Organization Practices include:

- Development of written security policies and procedures. These procedures should address data integrity, confidentiality, and availability of data.
- All offices must have someone appointed as an Information Security Officer. This person is responsible for the information security for that office and needs to be familiar with all security policies and procedures. The Information Security Officer will control access to all systems, maintains records of system access, and maintain security of the system from inside and outside attack.
- All physicians’ office must have in place training and education programs for all staff members concerning data security and patient confidentiality.

- Finally, the physician's office must have in place a procedure for sanctioning individuals who violate security policies.

Technical Practices include:

- The individual authentication of users. This is done by unique user identifiers and the use of another means of identification such as passwords, biometrics, or tokens.
- The implementation of access controls. Access controls include physical access to systems such as maintaining servers in a secure location. Access by individual staff members to data must be based on job function and need.
- If the system is connected to an outside system (the Internet) controls must be in place to prevent outside intrusion or attacks.
- Any remote access points must be protected from unauthorized use.
- There must be a chain of trust, which means that data entry must be tied back to an individual. Audit trails need to be kept which show when, where, how, and by whom data was entered or accessed on the ERM system.
- A third party to ensure compliance to the new rules must perform a routine system assessment.
- Finally, software discipline must be maintained. This means that routine hardware and software changes to the EMR system must be reviewed and tested to ensure they do not impact security or cause weaknesses.

Also, when patient data is transmitted electronically, HIPPA requires that the data is sent securely using either a private-wire arrangement or if transmitted over open system such as the Internet or POTS requires use of an encryption system. Whatever system is used it will include the following features:

- Integrity controls
- Message authentication
- Access controls in the case of private-wire arrangements or encryption

If the system is using a network for communication, these additional features need to be implemented:

- Network monitoring and alarm functions to warn of a possible security breach.
- Audit trails of all transactions on the network
- Entity Authentication
- Event reporting

Use of Portable Devices

The use of portable devices (laptops and PDA) in the medical profession has increased dramatically. Nearly all medical schools now recommend or require incoming medical students to own a laptop computer. Many physicians use PDA's as part of their daily practice to keep patient appointment records and other information. The health care software and hardware vendors have seen this trend and are moving toward making more information available to these portable devices.

New software is being introduced on the market to make patient data available via laptop and PDA. There are systems to allow doctors to track a patient prescription history on

PDA. Several companies have introduced systems to allow physicians to perform billing functions on a PDA or laptop in real time.

The security concerns primarily have to do with data held on the portable device and the mode of data transmission. All data that is held on the device should be encrypted, this is a fairly straight forward process on a laptop. However, on a PDA because of the limited resources available little has been done beyond password protection and there appears to be little incentive by vendors to make applications that will encrypt data on a PDA. With the current system therefore, the primary focus needs to be on educating the user on the confidentiality of the data stored on such a system and the potential for harm if the device is lost or stolen.

The other security concern is with data transmission, especially for devices that work from real time data. If the devices use a docking station or cradle to upload or download information to a medical system, the primary need is to have that data encrypted on transmission. A review of a number of vendors found almost no mention of data encryption to remote systems. However, HIPPA rules will require that any patient data transmitted over a network must be encrypted.

Newer devices are being developed which allow wireless transmission of patient information. However, currently there are only a few security protocols for wireless transmission of data. The most common is Wireless Application Protocol (WAP) which has a known security hole. This hole is supposed to be fixed with the WAP 2.0 but this protocol will not be out until November 2000. Also, in most cases the security is based on a 56-bit key, which is easily hackable. Therefore, physicians need to be aware that there are potential problems with these technology and question vendors on their implementation of security for these devices.

Conclusion

While there are exciting new resources available to physicians to assist with patient care, physicians are going to find that they have a lot of work to do implementing these technologies. The regulations coming out of HIPPA are going to mandate that good security practices are used. Health care is now finding itself I the same position as many other businesses as they struggle with computer and network security.

Sources

Kane, Beverley MD and Sands, Daniel Z. MD, MPH. "Guidelines for the Clinical Use of Electronic Mail with Patients." Journal of the American Medical Infomatics Association. 5:104-111 (1998) URL: http://www.jamia.org/cgi/content/full/5/1/104 (25 July 2000)

Department of Health and Human Services. Notice of Proposed Rule Making for Security and Electronic Signature Standards.
URL: http://erm.aspe.hhs.gov/ora_web/plsql/erm_rule.rule?user_id=&rule_id=62
(23 July 2000).

Nobel, Carmen and Berinato, Scott. “Wireless: Unplugged and insecure.” ZDNet News. July 6, 2000. URL: http://www.zdnet.com/zdnn/stories/news/0,4586,2597657-1,00.html (29 July 2000)