

EMR CONFIDENTIALITY AND INFORMATION SECURITY

ABSTRACT

Healthcare is no longer one patient and one physician. Many people and services are involved, and they all need access to the same accurate, complete data to provide excellent care. The onus is on healthcare providers to come up with information security solutions that don't hinder patient care while still providing the confidentiality of patient information.

GARY KURTZ, FHIMSS



Since the time of Hippocrates the need to maintain the confidentiality of medical information has been recognized. A tenet of information practices is that one cannot have confidentiality without information security. In the case of medical information, a balancing act is always present between ease of access for prompt medical care and that of information security to maintain confidentiality.

There is no doubt that information security measures could be used to lock information up so tightly that no one could access it. What purpose would that serve? Physicians and caregivers need to be able to easily access patient information to provide care. What is the right mix to be able to do both? Information security must be proportionate to the risk and the value of the asset to be protected. It seems that the magic formula is elusive.

The solution will probably be different for each healthcare organization depending in large part on specific policies and the culture. Some pieces will be the same, howev-

er the techniques might be different. The onus is on healthcare providers to come up with information security solutions that don't hinder patient care while still providing the confidentiality of patient information.

The correct solution will probably be determined in your organization by who defines service and how information security is implemented.

Definitions

There are distinctions between the terms privacy, confidentiality, and information security, and it is appropriate to establish those definitions.

1. Privacy is the right of an individual to control disclosure of his or her medical information.
2. Confidentiality is the understanding that medical information will only be disclosed to authorized users at specific times of need. It entails holding sensitive data in a secure environment limited to an appropriate set of authorized individuals or organizations.

KEYWORDS

Electronic medical record (EMR) Confidentiality Information security Privacy

- Information security includes the processes and mechanisms used to control the disclosure of information. It is the protection of computer-based information from unauthorized destruction, modification, or disclosure.¹

Electronic Medical Record Project

Attention to information security and confidentiality started early in the electronic medical record project with the formation of an Information Security Work Group. The workgroup knew that the patient/physician relationship is based on trust. Patients will share information only if they have this trust. It was important to be able to maintain this trust with the introduction of electronic records.

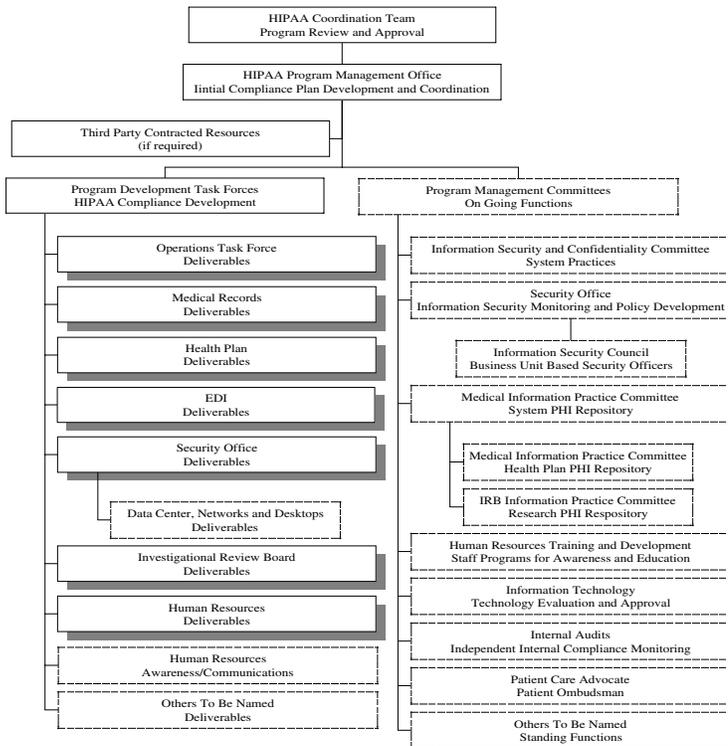
Many people are involved in the care of a patient and we have an acute responsibility to protect that information and make sure it only gets into the hands of those authorized to see it. It is a trust issue with our patients. The members of the workgroup were laying the foundation for policies and procedures aimed at ensuring the confidentiality of patient-identifiable medical information and thus maintaining trust.

Members of the workgroup included professionals from health information management, medical informatics, physician ranks, internal audits, legal services, human resources, and information technology. Their charge was to identify issues and propose policy solutions in the areas of information security, system security, and patient confidentiality. They did so, keeping in mind that some patients would not be entirely comfortable having their records in electronic form, which is Geisinger's strategy.

As a result of the workgroup's efforts, the following policy recommendations were derived:

- The establishment of an ongoing oversight group with responsibilities for managing information security, confidentiality, and access; overseeing the provision of training and awareness; disaster recovery; ongoing monitoring of access; and keeping abreast of technological and regulatory changes. This area was further expanded with the impending Health Insurance Portability and Accountability Act of 1996 (HIPAA) to include the appointment of a corporate privacy officer, a much more robust privacy program, and an expanded organizational structure defined to oversee the provision of information security and patient confidentiality (see GHS HIPAA Compliance Development Functional Organizational Chart, figure 1). While some of the

Figure 1. GHS HIPAA Compliance Development Functional Organizational Chart



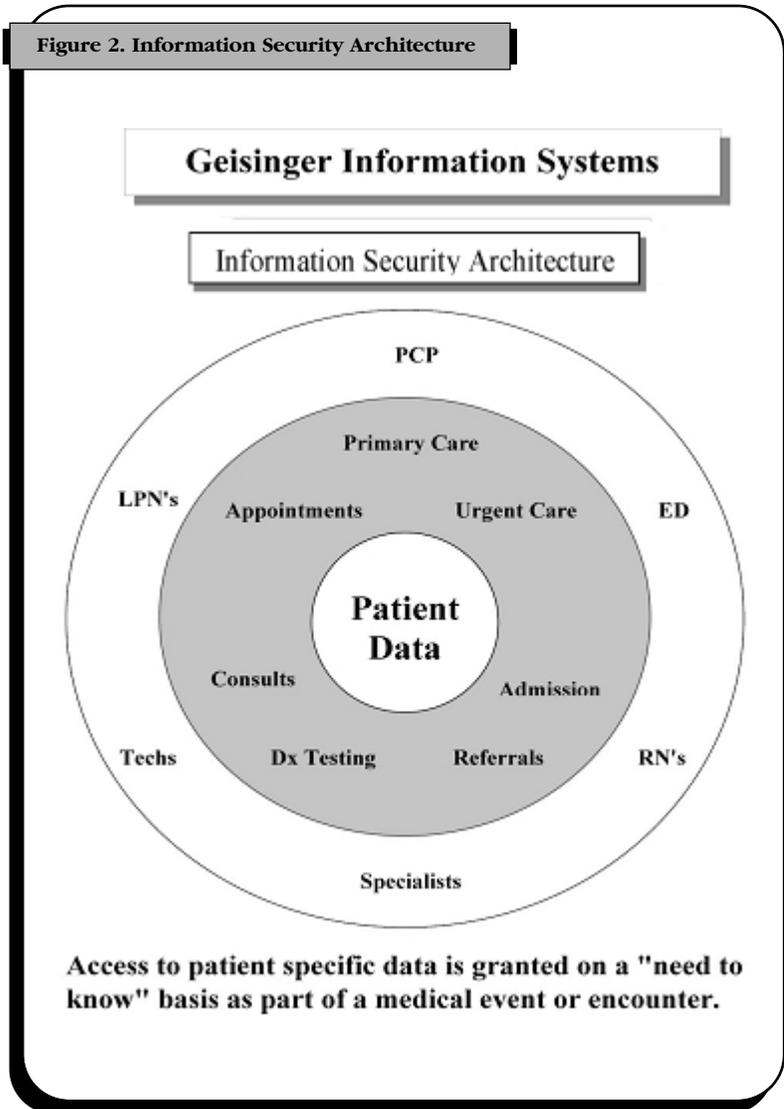
boxes (functions) are specific to HIPAA and will go away after the project, most will remain in effect into the future and constitute the functional information security and confidentiality organizational structure.

- Access to patient identifiable information should be on a "need to know" basis. Role-based access was the order of the day. Access would be granted based on the role of each person in the provision of patient care. Furthermore, the caregivers should only access the records of those patients for whom they were providing care. (See Information Security Architecture, figure 2)
- If the capability to tie physicians and patients together to control access is not implemented, then more stringent audit controls and monitoring should be instituted. Geisinger restricts access on a "need to know" basis through policy and education as opposed to software features. Geisinger would rather err in regard to confidentiality than make a mistake where information was withheld and treatment was compromised.
- The system should be designed with sufficient redundancy to minimize the risk of system downtime or data

loss. Disaster recovery plans would be required. With the need to have access to patient information 24 hours a day seven days a week for the provision of care, this aspect of the system is extremely important. Eventually, all of the records of the patients will be in electronic form and loss of access to this data could jeopardize patient care. Care should be taken to provide the correct services for the risk involved. Backup copies of data and shadow copies of data with fail-over capabilities are some examples of how Geisinger protects its data resources. Applications such as the electronic medical record (EMR) will have the most stringent mechanisms in place to ensure continued operation and data integrity, and to minimize risk.

5. An ongoing audit trail must be implemented for all transactions and accesses to the system. Random and directed review of the audit trail should be accomplished regularly to test compliance with confidentiality policies. Attention should also be given to feeder systems in reviewing audit trail capabilities. These could be vulnerable without proper information security and auditing capabilities.
6. Provision for restricted visit types (HIV, EtoH, drug treatment, and mental health) and restricted records (VIP, employees, etc) should be made. Access to this protected information for those not already providing direct care should be via "break the glass" access, creating an audit trail.
7. It would be imperative to follow federal and state regulations on medical record information to continue to be in compliance. At the time of these policy recommendations, the HIPAA regulation was not receiving widespread attention and was only a gleam in a legislator's eyes. As it turns out, some of Geisinger's provisions were right in line with the proposed regulations...a solid foundation on which to build our privacy program.
8. Database review and report generation for purposes other than direct care will be restricted. Care must be taken to ensure that printed patient information would be afforded similar measures as the electronic versions. Release of information would continue to be handled by health information management. Research requests would continue to be reviewed by the institutional review board. Data leaving the Geisinger Health System (GHS) should only contain patient identifiers

Figure 2. Information Security Architecture



when absolutely necessary as required by law, rule, or regulation. Creation of secondary databases, especially those containing protected health information, would be strongly discouraged because they pose a significant risk to confidentiality. They are also subject to corruption, and hence repeated or later queries against a secondary database may lead to erroneous conclusions. Information becomes out of date very quickly. It should also be noted that "secondary databases," while they may contain the same information as the "original" EMR, may not be subject to the same protections — firewall, antivirus, back-up, etc. — as the EMR and thus represent an area for increased risk of "hacking" and possible disclosure.

9. Remote access capabilities for caregivers should be provided with maximum protection against unauthorized access. The concept of accessing patient informa-

tion “where you need it” and “when you need it” was adopted. This would evolve into a more robust access methodology including encryption and strong authentication. It was believed this would improve productivity and “quality of life” for physicians. One of the mindset changes our organization went through was moving from a geographical record to “healthcare without walls.” Being electronic and accessible from anywhere is quickly becoming the norm.

10. Printers represent a significant problem with confidentiality. Their location, access, and use must be carefully protected. Temporary paper copies of portions of the electronic medical record represent an important risk to confidentiality, and their use, storage, and disposal should be managed appropriately.
11. Procedures for regular backup of the database must be established to include the capability to reload the database in case of disaster.

To support the policy statements, the workgroup created several documents that required signing prior to providing access to electronic patient information:

1. Electronic Signature Authorization Agreement to Participate
2. Password Authorization Agreement

Further Workgroup Considerations

Philosophically speaking, what constitutes an EMR? In the paper world, it was much easier to define. Generally speaking, it was what was inside the record jacket. In the electronic setting, this expands to many more data points. For instance, ECHO and EKG images may be stored in their respective databases with the EMR having pointers to this data. In some organizations ECHO and EKG applications may not have traditionally come under IT purview and thus may not be afforded the same protections.

When a patient makes a request for release of information, what will we give them in this new environment? Will orders and requests be included as part of the record?

It is important to cast away the paper world thinking and take a new view. This new view will undoubtedly require new thinking for information security and confidentiality as well.

Additionally, we are seeing a shift in how data is being presented so that the patient can easily understand its meaning. Another shift that is occurring is from the data belonging to the caregiver to a model where the provider or healthcare system is the repository of patient-owned and controlled data.

Views of patient data will probably be tailored to each patient and be more individualized. If you have a particular condition such as diabetes, you will be provided information tailored to that particular condition — for example, a

patient portal with a section called My Diabetes. This will lead to a fundamental shift, providing the patient with more control of their care.

Exam Rooms/Offices

Physicians would be required to “secure” their screens whenever they leave the room to maintain confidentiality of patient information. Logging in and out of the application each time they left a computer would be too burdensome and time consuming, as physicians go back and forth from office to exam room many times a day.

Instead, a feature of the EMR system would be utilized (secure screen) that enables the caregiver to initiate a curtain over the patient data. This would provide for confidentiality while enabling the caregiver to pick up where they left off in the electronic medical record. This was accomplished by simply re-entering their user identity and password.

Current technologies such as biometrics and proximity badges are being investigated to further reduce the amount of time a physician must spend entering user identity and password. Care must still be taken to ensure that balance is maintained between ease of access and confidentiality.

An example of this increased risk versus access is the potential practice of physicians wanting to have “concurrent sessions” under their user identity: one in the exam room for charting, and one in their private office for answering e-mail. Such a physical situation has minimal confidentiality issues, and certainly reduces the onerous task of “logging on” for the physician, but does raise significant issues with authentication. What if while the physician worked in the exam room an office worker conducted an e-mail session under the physician’s user identity? In the virtual world, the identity of the physician can become clouded.

The emergency room is a place where conventional methods for information security will be challenged. Time is of the essence, and physicians and nurses do not have time to be burdened with lengthy procedures to access medical information. EMR and information security vendors need to work in concert for an acceptable solution in this often life-and-death setting.

Access to Information

The use of a unique user identity and password combination is still the primary method of providing access to information.

In addition, policy prohibits the sharing of individual electronic access with anyone. This constitutes a change in behavior from the paper medical record world that may disrupt workflow. In the paper world, it was easy to instruct someone else to do some of the work. In the electronic world, they need appropriate access and may not qualify.

With the introduction of the EMR we have shifted accountability to many more people than when the record

was in paper form. For example, physicians did not need to deal with sign-on to access the paper record. Information is now available on any workstation that has proper access through the network and for any authorized user.

Most healthcare providers do not think of information in the course of their daily work, nor should they have to. It is up to the information security function to educate users on the risks and to provide the appropriate level of information security for the user.

Geisinger Health System has developed policies that regulate the composition of the password and how often it should be changed. The idea of requiring a password to be changed periodically has posed quite a debate for some time. If a password is changed often it is more inclined to be written down, which is against policy, thus creating a potential for others to obtain the password. If it is not changed periodically, how will it be known if it has been compromised? Others could use it indefinitely without being detected. At least if it changes periodically, unauthorized access would be reduced. As stated previously, we are investigating other avenues, e.g., biometrics, to providing authentication of users to access information, which would lead to discontinued need to change passwords periodically.

For remote access to patient information we have implemented the use of nonrecurring one-time passwords supplied via a device the caregiver must carry. The combination of something they know and something they possess is considered strong authentication. This password generator may resolve the debate over changing of passwords since they are never the same and the user will not need to write it down to remember. It is displayed on a mini-screen and is constantly changing.

For the virtual world of medicine, consideration must be given for the use of biometric authentication. This technology takes authentication to the next higher level, for it is a test of "a live presence." Thus the virtual physician interpreting or prescribing remotely can be authenticated to be physically present at the time of intervention, rather than permit the possibility of delegation to a colleague and/or identity theft by having someone else possess a valid password or token. It would certainly appear likely that such validation for "a live presence" would be a possible federal mandate for payment purposes in the future of telemedicine.

As more information becomes electronic and accessible virtually anywhere, more employees will do their work online, i.e., analysis, release of information, and coding. While this is an advantage to the organization, i.e., employees not tied geographically to the record, care will need to be taken to maintain confidentiality and information security.

Failed Logons

Auditors view the suspending of access for failed logons as a preventative control geared at limiting exposure while

providing system administrators with an opportunity to perhaps be advised of an attack on their system. Electronic medical records systems need to provide application security administrators with sufficient tools and information to assist them in determining if this is an attack or simply a user issue.

In addition, we need to select the number of consecutive failed logons as a trigger to suspending access. This is a delicate balance especially when a patient may be present and the caregiver cannot access the patient's record due to a failed logon suspension. This is a situation that we need to eliminate. Geisinger has established three consecutive failed logons as its standard.

We do not want to create an impediment to adopting the use of systems. On the other hand, we need to weigh the risks of a breach and implement the appropriate safeguards.

We hear complaints from users who say they cannot remember their user identity and password, yet we know some of these same people use ATM machines that require similar memory skills. There is a perception that information security just slows us down. Geisinger will look to new secure technologies to assist in this area. Possibly using biometrics, tokens, or proximity devices would reduce the number of failed logons.

In the future, audit trails with concomitant alarm functions may well need to be expanded beyond the traditional failed login parameters. Consideration must be given to audit trails that are more granular, i.e., the authorized and authenticated EMR user that attempts to view records for those patients not currently under their care or perhaps those of relatives, which traditionally has been discouraged by the American Medical Association.

Policies and Procedures

GHS has a termination policy requiring notice to the information security office of all employees terminating employment with the organization. Steps are taken to remove all access to data in conjunction with the termination.

Since the patient information does not belong to the caregiver, they cannot take it with them when they leave without patient authorization. A good termination policy will include this directive. As part of our HIPAA compliance efforts we will implement a release and acknowledgement form that the terminating user will be required to sign, acknowledging they are not removing any protected informational assets of the health system.

GHS has other policies covering risk acceptance, access, application criticality, Internet access, e-mail usage in a clinical setting, confidentiality, and remote access, to name a few. As part of the compliance for HIPAA, we have developed many more policy statements as required dealing with privacy, security, and transactions.

Information Security Organizational Structure

The information security function at GHS is a decentralized structure for application security administration, and a centralized structure for policy and procedure development. The director of information security and confidentiality is responsible for the development and implementation of the corporate information security and confidentiality program.

Most applications have their own information security administrator who is part of the user area and establishes the requested level of access based on the authorization of the data manager. A data manager is defined as a senior manager (e.g., vice president, department head, administrator, etc.) in a user department with responsibility to control and supervise specific data and to authorize access by users.

Access to applications and the information are controlled by the owners of the information, e.g., the finance department owns the financial information. They work within a framework that has been established by a central information security function that administers the program.

As with many paradigms, there are advantages and disadvantages to the decentralized information security model. One positive aspect is that it permits a much reduced response time and sensitivity to the needs of the business unit, thus permitting information security not to be perceived as a significant barrier to operations. The downside for the decentralized model is that it is much harder to maintain consistent application of policy and procedure. One way to remedy this shortfall is the creation of an information security officer's council composed of the business unit-based information security individuals. Such a group would meet on a periodic basis to review information security policy and procedure and discuss problematic areas.

Privacy

As defined earlier, privacy is the right of an individual to control disclosure of his or her own medical information. "Privacy," an influential journalist and editor wrote in *Scribner's* magazine in 1890, "is a distinctly modern product, one of the luxuries of civilization."

One of the earliest technologies, writing, enabled a new and enduring form of private communication. The printing press popularized reading, an intensely private affair. The wristwatch privatized time. The gummed envelope boosted expectations of privacy in the mail. The single-party telephone line, television, and radio are also examples of how technology has created private forms of communication.²

Today privacy is not a luxury. National surveys have shown that privacy is now something that most consumers and patients demand. They are keenly aware of what can go wrong when their information is stored in electronic form and, by accident or by malicious intent, their most private information is made public. Under intellectual property law, should that which was desired to be privileged

become public? Sanctions and remuneration can be imposed in an attempt to "make whole" the injured party. How does one compensate a patient whose genetic make-up is now public and has been used against them?

In the paper world it is impossible to know who has looked in the record as it flows from the central files to the requestor. This could be for a patient appointment or for review of case or filing of additional information. At least with the electronic record, in our case, each person accessing the record is recorded and date and time stamped, providing a record of all access to the patient's information.

Internet

No article on confidentiality and information security would be complete without discussing the Internet. This is the fastest growing method of access to information in the world. All that is needed is a personal computer with a modem, a phone line, and an Internet service provider, and you are connected. While there are other devices, such as cell phones and personal digital assistants, that can access the Internet, for our purposes we will stay with the personal computer. Many of the issues will be the same regardless of the device.

The Internet is open and used as an easy method to communicate with people around the globe. Just consider the number of people who use e-mail, which is offered free on many sites. So what you have are millions of people who have access to the Internet and the information that resides and flows over the electronic highway. Much of this information is not protected by encryption.

So enter the use of the Internet for healthcare applications and the flow of patient information over this conduit. Physicians want to be able to access this type of information when they need it and where they need it. This could be at home or while they are off to conferences. The Internet provides an ideal avenue for this type of access. Unfortunately, not everyone who is connected to the Internet is trustworthy. Some even go out of their way to be disruptive and some even prey on unsuspecting individuals.

Patients today are expecting to communicate with their physicians via e-mail, and they do this easily over the Internet. They want to be able to access their personal health records online any time of the day or night. Again enter the Internet. Not everyone is going to embrace this technology and some may even object.

Relationships between patient and physician are built on trust. Patients must have trust that their most private information will be kept confidential. This was easier for the patient to accept when the record consisted of paper and was stored at a single location. With the advent of the electronic medical record and access over the Internet, healthcare needs to find new methods to ensure confidentiality and maintain trust.

Patients who want to access their medical information online are required to go through an enrollment process so positive identification can be made before allowing them to access their personal data online. Coupled with that, encryption tools are used to scramble information so it is not readable if intercepted as it travels over the Internet. Once it reaches your personal computer it is unscrambled and readable only to the owner.

E-mail is handled in much the same manner with messages being deposited in a mailbox that is located at the provider site and only accessible by the owner through an encrypted online session. Reminders are sent to patients letting them know that an e-mail exists for their retrieval. These reminders are void of any patient information.

In conjunction with the implementation of the electronic medical record, the use of electronic means of communication with patients and other providers has become more prevalent. As a result, Geisinger Health System has developed Guidelines for the Use of Electronic Mail in Clinical Communications.

Patient Access from Home

Geisinger has introduced a patient portal to view and manage their healthcare. With the patient portal, patients can:

- View their health information
- View lab results for several common tests
- Send e-mail to their provider
- Review their scheduled appointments and request new appointments
- View past and future office visits
- Request prescription renewals
- Request referrals
- Review their medical history

This leading edge health management tool requires additional safeguards, and Geisinger has taken steps to provide them.

Patients who elect to sign up for this service receive a random access code, with authentication of the individual being done either in a face-to-face session or via online enrollment. This is accomplished by comparing “in-band” and “out-of-band” data points as a means of authenticating the user.

For information security reasons once authentication has occurred, the random access code is no longer valid. In addition, the random access code has a short life cycle in case it is not used promptly. The patient must sign on and create their own user identity and password. Since they choose their own user identity and password, and Geisinger does not have a record of their password, they are the only one who can access their information. The patient is instructed to use caution not to share their access information with anyone else.

While using the patient portal, all communications between the patient and their Geisinger healthcare team are carried over a secure, encrypted connection. This secure connection utilizes, at a minimum, industry standard Secure Socket Layer (SSL) 128-bit encryption as well as server-side digital certificate authentication to ensure secure data transmission between the patient and Geisinger.

Information Technology and Vendor Personnel

This group of people requiring access can pose an especially touchy problem. To do their job, some of them require “keys to the kingdom” access. Virtually all data is available to them whether it be patient, application, or operating system.

Special monitoring must be provided of these individuals via audit trails. Information security personnel need to review this special type of log information on a daily basis. Providing a data backup process is extremely important to be able to restore information in the event of an incident.

Personnel with this level of access should be made aware of the monitoring they will be under and should have annual reminders of the access they possess. This is accomplished at GHS through signing a confidentiality statement on an annual basis.

Vendors are also granted access to applications on an as-needed basis. Occasionally, issues arise that require their expertise. Prior to granting access that might include patient data, a few things must be established:

- Vendor contract includes clauses on confidentiality. With HIPAA near, a business associate agreement will be utilized. Refer to the HIPAA privacy regulation for complete details. It can be found at: <http://www.hipaadvisory.com/programs/documents/complete.htm>
- Vendor confidentiality statement.
- The capability to toggle vendor access on and off, providing access only when required, and controlled by Geisinger.
- Procedures covering the monitoring of vendor access through audit logs. Notification and involvement of the business unit-based analyst responsible for the application to ensure that vendor monitoring is timely.

Vendors typically design applications to provide functionality. Customers buy applications for that very same reason. We would propose that applications will need more robust information security functionality since healthcare providers are going to be required to implement more stringent information security measures, not only because HIPAA says we need to, but because it makes good business sense. And we in healthcare need to include information security as part of our daily routine, and not as an afterthought as was the case in the past.

It sometimes seems that the technology is not able to keep up with the fast-changing environment. Policies, procedures, and well-defined training programs can be used to fill gaps.

Application Upgrades

Internal information technology (IT) policies and procedures should include change control. Whenever new versions of the application are introduced, thorough testing should be done. This testing should happen in a non-production environment. This is done to ensure that the application functions properly and without any flaws prior to being introduced in production.

An integral part of this testing needs to be the information security functionality. This is especially true when dealing with patient information. Care should be taken to ensure the information security features continue to protect the confidentiality of the information.

Only after rigorous testing should the new version of the application be moved to the production environment. Remember, in today's world our patients are users of the application through the introduction of the patient portal.

The patient portal allows access to portions of a patient's record through an encrypted link over the Internet into their homes. Secure e-mail is used to convey information such as appointments, test results, prescription refills, and physician communication.

While change control mechanisms may seem burdensome, they are certainly preferable to doing them twice. For example, what would occur if the change was not tested properly and required a second or third attempt to get it correct? If there is time to do it over, there is time to do it right the first time.

Change control should be used for operating systems, equipment, processes, etc., and not just for healthcare applications. Change control procedures are a way of identifying where you have come from and where you want to go.

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA was initially designed to provide employees with portability of their health insurance from one employer to the next without loss of coverage. Along the way, items such as privacy, security, electronic transactions, and standard code sets were added. Specifically, the privacy and security aspects will have an effect on the electronic storage and transmitting of patient health information.

Conclusion

The patient/physician relationship is built on trust. To earn that trust, a physician and the organization must prove to patients their respect for confidentiality. There is more risk inherent with our environment today, and it will continue to be a challenge.

While the EMR may be the primary source of access to patient information, remember that many systems may in fact be feeding information to the EMR. When designing an information security program, remember to include the feeder systems. It is also important to pay attention to the secondary databases that are so easy to establish and use in this day of desktop tools.

We are sharing much more information with many more people than we did in the past. We need to operationally balance the risks of business and service while protecting patient confidentiality. In addition, dual systems (paper and electronic) will be in place for many years to come.

Privacy is not absolute. It is one of the primary goals, but there are many. For instance, in an emergency department setting, survival of the patient overrides information security. Healthcare is no longer one patient and one physician. Many people and services are involved, and they all need access to the same accurate, complete data to provide excellent care.

We must always be on guard to ensure the confidentiality of our most trusted information - patients' healthcare data. It is essential that an organization in this new world of instantaneous access from anywhere ensure they have a robust information security program in place. We need to create an information security consciousness within all organizations.

Acknowledgements

A very special thanks to the following individuals for their contributions:

- Jean Adams, Director I, Ambulatory/Physician Systems
- Dr. Joseph Bisordi, Associate Chief Medical Officer
- Kevin Kerestus, Vice President, System, Internal Audits
- Janet Anderson, Director, Medical Information Management
- John Gildersleeve, Director, Information Security/Confidentiality Administration

About the Author

Gary L. Kurtz, FHIMSS, is Associate Vice President of Information Services for Geisinger Health System, Danville, PA.

References

¹Nicholson, L., ed. *The Internet and Healthcare*. Chicago, IL: Health Administration Press, 1999, p. 94.

²Lester, T. "The Reinvention of Privacy," *The Atlantic Monthly*, March 2001, 287(3), 38.