

# Information Security and Confidentiality: Coming to a Health Care Organization Near You

*Sandra R. Fuller, MA, RHIA*

*Dale W. Miller*

**H**ealth information confidentiality is the protection of patient information from unauthorized access. Confidentiality is a subset of a greater issue—health information security—which is protection from not only unauthorized access, but also from fires, floods, system outages, and a host of other threats. Somewhat intertwined, these 2 issues require the health care industry's complete attention. **Figure 1** illustrates the complexity of the flow of information both inside and outside of the health care industry and the many opportunities for breaches of security and confidentiality.

## **BARRIERS TO SECURITY**

Several factors stand in the way of health information security:

- Securing information is an added expense and does not generate revenue
- Securing information can conflict with an institution's practice or intent to use such information for other purposes (eg, soliciting recent patients or their families for donations or bequests to a hospital foundation)
- Securing information is an arduous task

For these reasons, many health care organizations, including physician practices, have not yet dealt with the confidentiality and information security issues in comprehensive or strategic ways. However, it is important they do, because several phenomena will force the health care industry to place a high priority on this issue.

## **WHY CHANGE IS NECESSARY**

### **The Health Insurance Portability and Accountability Act**

The Health Insurance Portability and Accountability Act (HIPAA; also known as the Kassebaum-Kennedy bill), passed in 1996, mandated that Congress pass confidentiality legislation. Although Congress

missed its self-imposed August 1999 deadline for passing such legislation, congressional action still may occur. HIPAA also mandated that the United States Department of Health and Human Services promulgate confidentiality regulations. These proposed regulations were posted for public comment in November 1999, with final rules expected to be released in 2000 or early in 2001.

HIPAA also calls upon the health care industry to put into place basic information security processes and procedures. Final HIPAA regulations regarding information security are also expected at the end of 2000 or early in 2001. Once final, the industry will have 2 years to comply with the security requirements.

## **The Media and Public Opinion**

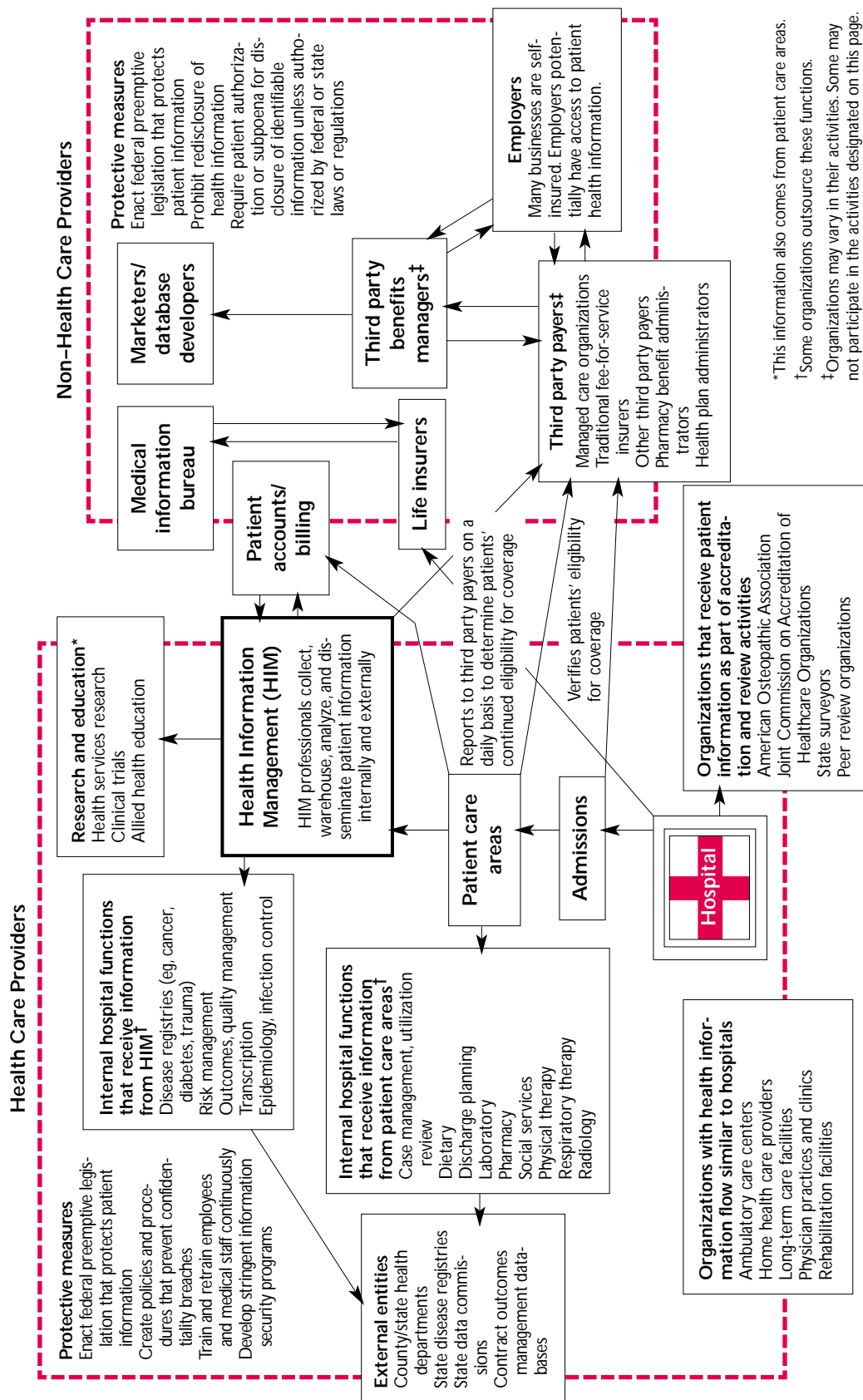
Media coverage has also helped emphasize the importance of health information confidentiality and security. Americans are becoming increasingly aware that few activities, ranging from grocery shopping to visiting a physician, are completely private. Although a good reputation for stringent confidentiality processes may never be on par with the importance of quality of care, confidentiality processes are likely to become a factor consumers consider when choosing individual physicians or group practices associated with their health plans. Also, health care organizations may need to consider the cost of a poor reputation for confidentiality in terms of its impact on their public image.

## **Legal Liability**

Another consideration is liability—confidentiality

---

*Sandra R. Fuller is Vice President of Professional Development Services, American Health Information Management Association, Chicago, IL. Dale W. Miller is Director of Consulting Services for Irongate, Inc., San Rafael, CA, a health care information security consulting firm.*



**Figure 1.** Flow of patient health information both inside and outside the health care industry. Additional potential risks to health information confidentiality include credit card companies, which can create databases based on cardholder purchases; e-mail, which can be intercepted in transit (employers can legally access and read employees' e-mail messages); employer health clinics, which are likely to keep records of employee visits (problematic if these records are commingled with other employee records); and companies and/or third parties, which can monitor and keep records of the e-mail addresses of visitors to Internet chat rooms and Web sites. Adapted with permission from Patient Health Information: Where Does It Go? Chicago: American Health Information Management Association, 1999.

(continued on page 24)

(from page 22)

breaches can lead to civil or even criminal action. Legal expenses and settlements can be expensive.

#### CREATING CONFIDENTIALITY AND SECURITY POLICIES

It is highly unlikely that any law passed or any regulation promulgated will give physician practices specific blueprints from which to build information security systems or protect patient information. Instead, the government will likely set parameters, and health care providers will determine how to implement them.

According to the American Health Information Management Association (AHIMA), a national association for health information management and medical record professionals, it is important to begin planning even before the final HIPAA rules are promulgated. Procrastination can lead to hurried and shortsighted decision making and extra costs, which, for large group practices, hospitals, and health care organizations, can run into hundreds of thousands of dollars. In general, the planning process includes:

- Becoming familiar with HIPAA and its final and proposed rules
- Assessing existing confidentiality and security measures
- Identifying opportunities for improvement
- Planning for and implementing needed changes

#### Implementing a Plan: First Steps

Before implementing a plan, physicians and practice managers must fully support the concept of confidentiality. This commitment to confidentiality must be embraced by employees, health plans, business partners, and medical staff. Information confidentiality and security requires the development of clear policy, incentives, continuous training and retraining programs, and continuous enforcement.

Confidentiality and security policies and procedures must be comprehensive. They must account for all areas of the health care practice, its employees, health plans, and external entities with which the practice contracts or shares information. Policies must be uniform, and they must apply equally and fairly to all employees, including physicians. The organization CPRI-HOST (Computer-based Patient Record Institute and Healthcare Open Systems and Trials) provides documents covering the establishment of information security guidelines and security education programs as well as sample confidentiality statements and agreements. CPRI-HOST can be accessed on the Internet at [www.cpri-host.org](http://www.cpri-host.org). AHIMA ([www.ahima.org](http://www.ahima.org)) also provides several docu-

ments and guides for establishing confidentiality and security policies.

Confidentiality and security policies should be developed with input from key individuals (eg, representatives of medical and support staff, legal counsel). Once the policies are approved by the senior management of the organization, the responsibility for overseeing policy and procedure development and implementation should rest upon a single individual, such as a health information management director or a privacy, security, or compliance officer.

#### Evaluation of Current Security Risks

Once a clear confidentiality and security program is initiated, it becomes time to evaluate current security and confidentiality risks. **Table 1** can help providers get started.

#### SECURING COMPUTER SYSTEMS

A host of potentially compromising situations can result from the way computer systems are designed. Very costly incidents can occur when health care organizations do not do enough to protect the information within their computer systems.

One of the main prerequisites to securing information is maintaining physical control of computer hardware. A good starting point for implementing security measures is to make sure individual workstations and network servers are protected from unauthorized access, theft, and damage. Because so many health care work areas—especially in older facilities—were designed and built without considering computer equipment, computers and network servers often get placed in areas where they cannot be protected. Instead, these systems should be located in areas that are inaccessible to unauthorized individuals and can be locked when no one is using them.

#### Storage of Back-up Tapes

It is not uncommon to find backup tapes stacked near local area network (LAN) servers. Ideally, backup tapes should be stored off-site in secure facilities, such as safe deposit boxes at local banks. It is important to note, however, that tapes stored in safety deposit boxes will be accessible only during regular banking hours. If tapes are stored on-site, they should be kept in locked cabinets or drawers.

#### Software Considerations

The security features of different software products can vary greatly, so it is important to gain a full understanding of them before making purchases. However,

**Table 1.** Health Care Information Security Risks and Solutions

| <b>Scenario Involving Risk</b>   | <b>Solution</b>   |
|--|---|
| <b>Placement of personnel, office equipment:</b><br>Patient files, computer equipment, printers, and fax machines are accessible to unauthorized personnel                                       | Place all patient files, computer equipment, printers, and fax machines in areas where they can only be accessed by authorized personnel, and/or keep such materials/equipment locked   |
| <b>Copiers:</b><br>Discarding imperfect copies of patient health information in trash cans adjacent to copy machines   | Place secure disposal containers adjacent to copy machines or arrange for secure recycling or shredding   |
| <b>Faxes:</b><br>Faxing confidential information to unauthorized persons   | Verify recipients' authority to receive confidential information prior to transmission  |
| <b>Telephones:</b><br>Unauthorized access to voice response systems  | Establish procedures for controlling access to voice response systems and limits on information distributed on these systems  |
| <b>Voice pagers:</b><br>Confidential messages overheard when received on the pager   | Prohibit sending confidential messages to voice pagers  |
| <b>E-mail:</b><br>Sending confidential messages via the Internet, resulting in disclosure of patient information   | Train employees on how e-mail works and the implications of using it; establish policies regarding what specifically can and cannot be included in an e-mail; establish policies governing the forwarding of e-mail messages; use encryption technology |
| <b>Dictation and transcription:</b><br>Managing dictation system passwords so poorly that they are subsequently disclosed to unauthorized parties<br>Dictation overheard by unauthorized persons | Include confidentiality provisions in contracts for transcription; protect dictation system passwords from disclosure<br>Dictate only in private offices or examination rooms where the dictation cannot be heard by anyone other than the patient      |
| <b>Internet:</b><br>Sending unencrypted patient information via the Internet, resulting in unauthorized access   | Use security safeguards such as encryption technology; employ secure access and authentication systems  |
| <b>Telemedicine:</b><br>Compromising the privacy of patients who are in the background of videos for other patients  | Provide private facilities for telemedicine and teleconferencing  |

software programs should have the ability to:

- Assign unique ID or access codes to each user
- Assign unique passwords (at least 7 characters long) to each user
- Change passwords (this should be done at least every 90 days)
- Set limits on access to information based on an individual employee's job function
- Prevent anyone, including system managers, from looking up or printing any passwords

- Maintain access logs

**Access Through Modems**

Controlling outbound and inbound access is important when systems are linked to medical centers and regional databases. Setting modems and ISDN routers to limit inbound calls to specific numbers helps reduce the likelihood of computer break-ins. If systems are equipped with modems for dialing out (eg, to use the Internet or to verify insurance eligibility) and in-bound access isn't required, the modem's auto-answer feature should be disabled.

### Working with Equipment Maintenance Contractors

Repair and support of computer systems often requires contracting with external programmers. Contracts should include confidentiality agreements. They also should include liability provisions that hold contractors responsible for confidentiality breaches that occur as a result of their actions. Contracts also should stipulate that taking patient information out of the office is forbidden.

It also is important to disable outside programmers' access codes or change their passwords when they are not in use. In addition, systems should have mechanisms to make staff members aware each time software vendors provide support via modem. In fact, vendor access should be disabled until it is needed. Modems should be turned off, or phone lines should be unplugged at times when they are not in use.

Individuals performing hardware repairs should be required to sign confidentiality agreements as well, and all information should be removed from any systems that are taken out of service for repairs or replacement.

### Software Installation

Procedures should be established for installing and modifying software. Allowing anyone to install software without prior approval compromises system integrity and leaves practices vulnerable to viruses. One person, and an appropriate backup person, should monitor and maintain accurate records of all installation activity. Another note: A small battery backup power supply permits graceful system shutdown in the event of power failures. It also reduces the likelihood of file corruption.

### CONCLUSION/SUMMARY

For facilities that have not yet begun addressing the privacy and security requirements outlined in HIPAA legislation and regulation, now is the time. A good first step is to appoint a motivated project manager to establish direction and develop a vision and future strategies for producing the necessary changes. The time-consuming and complex process of assessing current confidentiality and security measures, identifying opportunities for improvement, and implementing the necessary changes can then begin in an orderly manner, with the support of all internal stakeholders of an

organization. Just as health care organizations attained Y2K compliance, with the right project manager, input from key personnel within the institution, and appropriate administrative support, they can attain HIPAA compliance as well. **HP**

### ACKNOWLEDGMENT

Many of the recommendations in this commentary were derived from articles by Mr. Miller published in the AHIMA publication *In Confidence*.

### BIBLIOGRAPHY

- Allen B: Y2K: What time is it? *In Confidence* January/February 1999;7(1):1-3.
- Fuller SR, Welch J: A HIPAA checklist. *JAHIMA* 1999;70(4):64A.
- Fuller SR: *Security and Access: Guidelines for Managing Electronic Patient Information*. Chicago, American Health Information management Association, 1997.
- Fuller SR: Implementing HIPAA security standards—are you ready? *JAHIMA* 1999;70:36-40,42-44,47-48.
- McKenzie DJP: Healthcare trend improves security practices. *In Confidence* May/June 1996;4(3):1-3.
- Miller DW: Developing an information security plan: taking the long-term view. *In Confidence* March/April 1998;6(2):4-5.
- Miller DW: Preserving the confidentiality of e-mail communications. *In Confidence* September/October 1996;4(5):4-5.
- Miller DW: Protecting information on hand-held computers. *In Confidence* May/June 1996;4(3):8-9.
- Miller DW: Protecting information on computers in physicians' offices. *In Confidence* July/August 1997;5(4):6-7.
- Miller DW: Using system logs to protect confidentiality. *In Confidence* January/February 1996;4(1):1-3.
- Myjer D: Compromise: the key to successful information security policies. *In Confidence* May/June 1999;7(3):4-5.
- Patena KR: Making healthcare intranets secure, part 1. *In Confidence* March/April 1998;6(2):6-7.
- Patena KR: Making healthcare intranets secure, part 2. *In Confidence* May/June 1998;6(3):6-7.
- Smith RE: Setting realistic computer security goals." *In Confidence* January/February 1998;6(1):3,11.
- Welch J: On the line: professional practice solutions. *JAHIMA* 1999;70:80.
- Welch J: Remote access security. *In Confidence* January/February 1998;6(1):4-5.

Copyright 2000 by Turner White Communications Inc., Wayne, PA. All rights reserved.