Helping Consumers Manage Their PHRs

Save to myBoK

by Clarice Pittillo Smith, RHIA, CHP

Personal health records (PHRs) are a primary piece of the growing consumer empowerment movement in healthcare. Many consumers already maintain paper copies of their medical information in personal files at home. But as more of their information becomes digital in their providers' offices, the logical next step for them is an electronic personal record that can manage that information.

Consumers have many choices when it comes to PHR products and services. Many are exploring Web-based services. While functionality and cost are always concerns when selecting a PHR vendor, consumers should be equally concerned about the privacy and security of the information being captured and stored online. HIM professionals can help by educating consumers on important privacy and security aspects of PHR maintenance.

Components of a PHR

The healthcare industry has yet to settle on a universal definition of the PHR, but it's important that consumers expect certain guarantees of accessibility, control, privacy, and security from any PHR service.

AHIMA defines the PHR as an "electronic, universally available, lifelong resource of health information needed by individuals to make health decisions. Individuals own and manage the information in the PHR, which comes from healthcare providers and the individual. The PHR is maintained in a secure and private environment, with the individual determining rights of access. The PHR is separate from and does not replace the legal record of any provider."[1]

What Consumers Should Consider when Establishing a PHR

In most emerging technologies, regulations and safeguards lag behind the practical application of the concept. This holds true for the PHR.

However, many state and federal laws and regulations that currently address the protection of paper-based health information also cover electronic information. These regulations can be used as a baseline to determine if a PHR vendor can adequately protect consumer information.

Consumers should consider these questions when establishing a PHR.

Who owns the data? By AHIMA's definition, the consumer owns the data. However, that may not be the case for every service. Consumers should clarify this with potential vendors. They should ask:

- If the consumer decides to move his or her data to another vendor, will the current vendor allow the transfer?
- With any large database of this size, data mining for various reasons will be a temptation. Does the consumer's contract or agreement allow or prevent this from happening?
- How are requests for information from law enforcement agencies handled?
- What happens to the data when the consumer dies?
- If there is nonpayment of the account, will the vendor hold the consumer's information hostage until the account is paid?
- Is there an exception that will allow the provider to access the information in an emergency?

How are data accessed by healthcare providers when providing care?

- Before registering with a service, consumers should verify that the providers in their area have the technology necessary to access the service, also. For instance, does access require more than an Internet connection and a Web

browser? The individual may want to check directly with his or her primary providers to confirm their ability to use the service.
- What type of authentication is required of the provider in order to access the data? Do providers require a password, user ID, PIN, or biometric identifier?
- Is written authorization or consent required by the vendor? If so, is it stored in the PHR? If not, where is it stored?
- In the event of an emergency, can a provider gain access to pertinent information without prior consent? If so, are these instances tracked?
- How does the provider identify the consumer to access or add information to the consumer's PHR? If the consumer's Social Security number is used, are adequate measures in place to guard against identity theft?

How are data added to the PHR?

- If a provider is given access to view a consumer's PHR, does this automatically give the provider the ability to update the record, also?
- What is the process for exchanging data?
- Once given access, does the provider retain it indefinitely until the right is revoked?
- Can the consumer alter information added by the provider? The system should not provide the consumer with this functionality.

Does the vendor provide adequate online security controls? Do they include:

- Encryption
- Firewalls
- Virus protection
- Unique user identification
- Automatic log-off
- Method of ensuring data integrity during transmission
- Audit controls
- Disaster recovery plan
- Contingency plan
- 24-hour availability
- Log of who viewed or updated the data and when
- Incident management plan
- Consumer notification of a security breach to data
- Definition of a security breach
- Assistance in mitigation of harm in the event of a security breach

Look for the Seal of Approval

This security information should look very familiar to HIM professionals since these are the basic HIPAA requirements. However, many consumers will be unable to obtain this information from their vendors or may not be knowledgeable enough with the technology to have this type of discussion.

There are several certification agencies that evaluate Web sites against industry standards for security. Once certified, the sites display a certification seal. Consumers should only do business with a vendor whose site displays one of these seals. There are several certification agencies, such as BBB Online, TRUSTe, and CPA Web Trust.

Protecting Employees

Companies are beginning to develop PHRs as a benefit for employees and as a mechanism to reduce ever-increasing healthcare costs. This has raised obvious concerns regarding privacy and security of data, particularly for individuals with chronic illnesses who worry they could be subject to limited promotions or termination.

While the PHRs are developed with the best of intentions, current legislation does not protect the employee enrolled in the employer-maintained PHR. However, there are other regulations such as the Americans with Disabilities Act that would

provide some protection to the employee if the employer misused the data or if privacy were to be breached by the employer.

Consumers are becoming increasingly wary of online databases due to the growing incidence of identity theft. For the PHR to be successful, the consumer must be assured that their information will be private and secure.

HIM Next Steps

AHIMA offers free PHR education seminars as part of its mission to provide effective management of personal health information needed to deliver quality healthcare to the public. The PHR Community Education Campaign allows HIM professionals to share their knowledge of health information and medical records directly with the public (at the community level) in order to help them better understand how to access, manage, and protect their personal health information.

This public service initiative is delivered through AHIMA's network of 52 affiliated component state associations (CSAs). AHIMA and its CSAs provide training and materials to interested volunteer members in order to create a uniform national campaign that can be delivered at the local level. If you are interested in participating or would like more information, contact your CSA leaders.

Note

1. AHIMA e-HIM Personal Health Record Work Group. "The Role of the Personal Health Record in the EHR." *Journal of AHIMA* 76, no. 7 (2005): 64A-D.

Reference

International Association of Privacy Professionals. "IAPP Information on Privacy." Certification educational materials.

Clarice Pittillo Smith *(clarice_smith@chs.net) is a regional health information management director with Community Health Systems, in Nashville, TN.*

Article citation:
Smith, Clarice Pittillo. "Helping Consumers Manage Their PHRs" *Journal of AHIMA* 77, no.3 (March 2006): 50-51,53.