Communicating Security Efforts: Informing Consumers of Data Protection Programs Helps Build Trust

By John Parmigiani

The American Recovery and Reinvestment Act has both pushed and trumpeted the emergence and attendant benefits of a healthcare environment where patient safety and improved patient outcomes are directly linked to shared digitized patient information. However, with this has come media hype of the increased threat of patient information falling into the wrong hands.

As healthcare moves into an enhanced electronic environment, providers need to reassure their customers they are doing everything reasonable to safeguard their information from inappropriate access, use, and disclosure.

They should ask themselves if their patients are aware of the safeguards they have put in place to prevent and mitigate loss of confidentiality, or if patients hear about the organization's security provisions only after a breach, when the organization is scrambling defensively to limit damage to the victims and to the organization's image in the community?

Negative public relations can blur an organization's good efforts and leave patients lacking trust in its efforts to maintain their confidentiality. Healthcare providers can actively communicate their efforts to safeguard the confidentiality, integrity, and availability of patients' protected health information by informing their patients and their communities of their efforts. Gaining consumer trust in health IT is vital to its success, and organizations that communicate their privacy and security efforts are more likely to follow through on them.

Consumer Messages

An organization needs to let its consumers know that it is aware of both the benefits of technology as well as the need for strengthened security and privacy. It is this awareness that encourages the organization to continually look for practical and effective preventive measures. That effort, the organization can explain to its consumers, leads it to institute policies and procedures that guard against unauthorized incursion into its records that could corrupt integrity, timely access, and the "need to know."

In an electronic atmosphere marked by increased capture and legitimate use of patient information, the potential risk of identity and medical identity theft is intensified. Now more than ever, trust is critical in healthcare. And a correlation exists between what a patient is willing to share and the effectiveness of healthcare delivery.

Moreover, patient information in the wrong hands, as in the case of identity or medical identity theft, can compromise correct and timely treatment, risk unsafe or fatal outcomes, exhaust insurance coverage, and cause patients to lose their insurance or be unable to find a job due to corrupted medical information.

False entries in health records can pose logistical nightmares for hospitals, physician practices, pharmacies, and insurance companies. Errors may remain undiscovered and be disseminated for years, and correcting corrupted records is very difficult.

Organizations should consider what messages would improve the current community perception. Offered here is a sample consumer message organizations can adopt as they begin an awareness campaign within their community:

> Recent regulatory requirements at both the federal and state levels mandate increased protection of patient information. The new stimulus law fortifies state laws currently in place with the first federal provisions for victim notification of healthcare information breaches. Healthcare organizations are stepping up more robust technology security requirements as the nation marches toward a multilayered e-health environment.

In order to be effective the healthcare industry enlists you, the patient, as a player to optimize the use of technology in protecting your sensitive health information.

[Name of organization] has developed and implemented polices not only to safeguard the confidentiality of your healthcare information but also to ensure its accuracy and availability to your caregivers when they need it. We strive to allow information access only to those who have a need to know and then limit their access to only the information that is necessary to carry out their duties.

We rigorously screen both registering patients and potential hires to validate their identity. We have established ways for you to find out about how your information is used internally and disclosed to parties external to the organization (see our notice of privacy practices). Staff privacy and security training and awareness efforts are ongoing to keep them ever mindful of their duty to protect your information. Sanctions await them if they do not.

We have instituted strong security safeguards that are in strict compliance with federal and state regulatory requirements and mirror industry best practices. And we look to you, the consumer, to help us in this by notifying us of errors in your explanation of benefits such as service type, visit history, and equipment charges.

If you have received healthcare services in our facilities since April 2003, you were offered a paper copy and Web site access to our notice of privacy practices where your information privacy rights and our policies for use and disclosure of your information are explained. Moreover, it touches on the safeguards that we are employing to keep your information from unauthorized access and the penalties that we have set up to act as a deterrent and possible outcomes if violated.

We also have provided a means for you to communicate with us to voice your complaints or suggestions as to how we can better improve our methods of protecting the confidentiality, integrity, and availability of your healthcare information.

We have instituted a notification process that if, despite safeguard efforts, a breach is suspected, we follow a well-defined set of steps to mitigate damage or loss to you.

We are also developing and implementing a customer awareness program to keep individuals who are subjects of individually identifiable health information informed of the organization's commitment to information privacy and security and their individual rights and services. We enlist your ideas to make this program useful to you and helpful to us in better protecting your information.

Getting the Message Out Creatively

Organizations may get their messages out in many ways:

- An occasional local media article or participation in a radio talk show
- The organization's Web site
- Posters in patient waiting areas
- Flat screens in ER and waiting rooms with short messages or reminders
- Mailers, which include a contact person for questions or complaints
- Reminders from physicians during treatments and services
- A note in billed items, insurance payments, and coverage

Organizations should list what patients can do to help the organization and be a partner in protecting their information, including opportunities to get involved in their healthcare such as creating personal health records and looking for discrepancies in their medical information. Organizations should provide a phone number, e-mail address, or mailing address in these messages for patient questions or complaints.

A concerted, good-faith effort to inform patients what steps the organization is taking on a continuous basis to keep their information from falling into the wrong hands promotes trust in the institution and demonstrates due diligence and limits legal risk.

John Parmigiani (jcparmigiani@comcast.net) is president of John C. Parmigiani & Associates.

Article citation:
Parmigiani, John. "Communicating Security Efforts: Informing Consumers of Data Protection

Programs Helps Build Trust" *Journal of AHIMA* 80, no.11 (November 2009): 56-57.