Some in Public Health Wary of Pandemic Duty

Some 16% were unwilling to respond to a pandemic flu emergency no matter what.

BY KATHRYN DEMOTT

About one in six surveyed public health workers said they would not report to work in the event of an influenza pandemic emergency, according to an survey of more than 1,800 public health employees in Minnesota, Ohio, and West Virginia that was conducted online.

Overall, 16% of the health workers said they were unwilling to "respond to a pandemic flu emergency regardless of its severity," according to the findings of the survey, which was conducted from November 2006 to December 2007.

Nonetheless, that represents an improvement over the 40% of public health employees who in 2005 said they would be unlikely to report to work under the same pandemic circumstances, according to the researcher team that conducted both surveys. The current survey findings were published in the July 24 issue of the journal PLoS one.

Responses from the 1,835 public health employees in the current survey were analyzed using the Extended Parallel Process Model, which describes an individual's willingness to follow instructions in an emergency, given that person's perception of a threat and his or her belief in the ability to have a positive impact on the threat (PLoS One 2009;4:e6365).

Individuals who had a perception of high threat and high efficacy were nearly 32 times more likely to say they would be willing to report to work during a flu pandemic, compared with those who reported a low threat and low efficacy perception.

"These results … reveal a unique opportunity to induce change," according to the researchers.

"The first step is to better educate public heath workers as to their designed roles during this emergency scenario, and then motivate them with an understanding of why this role makes a difference," they continued.

Those who had a perception of high threat and high efficacy were nearly 32 times more likely to say they would be willing to report to work during a flu pandemic.

"Employee response is a critical component of preparedness planning, yet it is often overlooked.

"Our study is an attempt to understand the underlying factors that determine an employee's willingness to respond in an emergency," said the study's lead investigator, Dr. Daniel Barnett, assistant professor in the department of environmental health sciences at the Johns Hopkins Bloomberg School of Public Health in Baltimore.

The study was funded by the Centers for Disease Control and Prevention's Centers for Public Health Preparedness Program, and by the CDC's Preparedness and Emergency Response Research Centers program.

The authors of the study reported having no conflicts of interest. ■

Expert Offers Advice on Coping With Red Flags Rule

BY JOYCE FRIEDEN

WASHINGTON — The federal Red Flags Rule that requires creditors to check for identity theft may mean a few new procedures for office-based physicians, Patricia King said at the American Health Lawyers Association's annual meeting.

"Do health care providers have to comply with the Red Flags Rule? Yes, if they're [considered] creditors," said Ms. King, assistant general counsel at Swedish Covenant Hospital in Chicago.

The rule requires creditors to establish formal identify theft prevention programs to protect consumers.

Aimed primarily at the financial industry, the regulation was originally scheduled to go into effect on Nov. 1, 2008. However, to give small businesses more time to prepare for compliance, the Federal Trade Commission (FTC) delayed enforcement until May 1, and then until Aug. 1, and most recently until Nov. 1.

Earlier this year, the AMA and physician specialty societies argued that physicians are not creditors because they bill insurance companies, not individual consumers, Ms. King said. "But the patient does get billed for copays, deductibles, and excluded services, so unless all those charges are collected up front, the health care provider is billing and possibly deferring payment for the cost of services."

To address health care providers' concerns, the FTC has published guidance and developed a template for identity theft prevention program for low-risk creditors. (The information is available at www.ftc.gov/bcp/edu/pubs/articles/art11.shtm.)

Low-risk providers who see the same patients regularly can adopt a simple identity theft program, she said, adding that personnel involved with front desk, medical records, and patient account functions should be involved in the program.

Physicians need to identify which patient accounts will be covered by the rule—such as those patients who need to make repeat payments—and develop appropriate policies and procedures, Ms. King said.

"The final [Red Flags] rule had 26 examples of identity theft. Look through them and see which ones are most applicable to you."

Providers also need to look at what information they collect when patients register. "Many of us need to re-think our standard registration procedures and beef them up," said Ms. King. One example might be to ask for a photo ID.

To give small businesses more time to prepare for compliance, the FTC delayed enforcement from Nov. 1, 2008, until May 1 2009, and then until Aug. 1, and most recently until Nov. 1.

Procedures for guarding against identity theft need to be approved by the organization's board of directors and overseen by senior management, according to the rule, "because this is intended to be a high-priority program, not something that's delegated to a lower-level manager."

Typical "red flags" that practices should watch for include:

- ► Insurance information that cannot be verified;
- ► No identification;
- ► A photo ID that does not match the patient;
- ► Documents that appear to be altered or forged;
- ► Information given that is different from information already on file;
- ► An invalid Social Security number;
- ► A patient who receives a bill or an explanation of benefits for services he or she didn't receive;
- ► A patient who finds inaccurate information on their credit report or on a medical record; or
- ► A payer that says its patient information does not match that supplied by the provider.

When a particular patient raises one or more red flags, the practice has two options, according to Ms. King. It could refuse to provide service, although this might raise a problem under the Emergency Medical Treatment and Active Labor Act (EMTALA), a law that prohibits providers from not treating persons with questionable identification who require emergency care.

Or the practice could provide the service, but ask the patient to bring in the correct information to his or her next visit. Ms. King cautioned providers about freely providing medical records to a patient suspected of identity theft, because it could lead to more identity theft.

Patients also will have to be educated about the new rule, Ms. King said. "Providers are going to run into problems with patient expectations. Patients have gotten used to coming to their doctor … with either no identifying documents or only their insurance card. They will need some education in advance by being informed when they call on the phone to schedule an appointment, or by signs in the waiting room, that you really need to have identifying documents with you."

Ms. King encountered a case of identity theft at her own hospital involving two elderly women, one of whom had a public assistance card, while the other one didn't.

The two of them thought it would be all right if the woman without the card used her friend's public assistance card to get care. The identity theft was discovered by radiologist in the hospital who noticed that the women's scans were different.

She noted that under EMTALA, a hospital cannot delay performing the medical screening examination or stabilizing treatment, to inquire about insurance or payment, "but it can follow reasonable registration processes as long as the medical screening exam is not delayed by the process. So after the patient has been triaged and is sitting in the waiting room waiting to be seen for the medical screening exam, you can ask them for identifying information. But if they don't have identifying information, you can't turn them away. You have to provide the [screening exam] and necessary stabilizing treatment."

Providers also should note that compliance with the Health Insurance Portability and Accountability Act (HIPAA) does not shield them from complying with the Red Flags Rule.

"One of the questions we get is, 'I already comply with HIPAA; aren't I done?' The answer is, 'Probably not,' " said Naomi Lefkowitz of the division of privacy and identity protection at the Federal Trade Commission.

"The Red Flags Rule is really about fraud protection, and HIPAA is more about data security. There is certainly some overlap, and to the extent that, for example, someone is checking photo IDs … to make sure that the person only has access to their [own] medical record, that's a policy that might do double duty under the client's identity theft program as far as verifying identification.

"But merely having the HIPAA program is probably not going to make [providers] compliant with Red Flags," she added. ■

Mary Ellen Schneider contributed to this article.