Going High-Tech?

How Privacy and Security Issues Come Into Play

by Michele Hayunga

Security and privacy issues are foremost in the minds of both providers and consumers using new technologies in aging services. This look at the most pressing issues includes:

- How thorough education of clients on the benefits and risks of telehealth technology protects one provider
- How another provider structures its home health security system so it is driven by clients and their family members
- The importance of a good understanding of the HIPAA security and privacy rules
- The four basic concepts of data security, and why common sense should prevail

It is often said that the power of technology is the ability to have information at one's fingertips. But when this information concerns a person's physical and mental health, "whose fingertips?" is a question worth asking.

As leading technology companies have set their sights on older adults, new products are making their way to the marketplace. From in-home monitoring systems that use sensors to track activities of daily living to telehealth devices that analyze an array of physiological tests, instant information is a common theme.

"Almost every technology in some way involves capturing information," explains Russ Bodoff, executive director of AAHSA's Center for Aging Services Technologies (CAST). "If consumers are going to accept these advances, we have to establish a high level of confidence in who gets to see what pieces of information."

Straight Talk From the Start

One organization that has wrestled with this issue is Northeast Health, a not-for-profit network in upstate New York. Since October 2000, its Eddy Visiting Nurse Association has operated a telehomecare program that allows nurses to make "video visits" to clients' homes.

Using ordinary telephone lines, the telehomecare system enables a live audio and video connection between clients and nurse specialists. A central monitoring unit placed at Eddy VNA's office electronically connects with a small unit placed in the home. The live, two-way transmission gives nurses close-up pictures of the clients, as well as heart, lung and bowel sounds, blood pressure readings and blood oxygen levels.

The organization is working with GE to test a sensor-based system that can infer common activities, such as going to the bathroom or making a meal.

In implementing these new technologies, Northeast Health has made it a point to integrate privacy and security considerations every step of the way, explains Lisa Gaudet, director of remote care technology. She stresses that most problems can be avoided by making sure clients fully understand the technology—including its benefits and risks.

"We have a separate consent form for people who participate in our telehomecare program," she says. "It outlines what telemedicine is, explains the benefits and risks, and discusses who will see the information, such as clinicians or possibly the vendor. We want to spell out any potential risk of disclosure."

Gaudet is an advocate of straight talk, because no technology is 100 percent guaranteed. "One issue for us with the telehomecare is that the transmissions are coming over traditional phone lines," she says. "While they're very reliable, there is always a possibility that the information could be incomplete or that someone could get into the system."

Making sure people understand the risks is particularly important when dealing with beta projects, which may still have some glitches. "Part of that is about protecting our organization legally, but also from an ethical standpoint, people should be fully aware of the benefits and drawbacks," Gaudet says. In her experience, the sharing of data with clinicians, researchers and vendors has not been a big concern for clients.

That's not to say that people are willing to forgo their privacy or dignity. With in-home monitoring systems, the first question that typically arises is whether cameras are involved. "People want to know that they can walk around in their underwear without being photographed," Gaudet says. In addition, many seniors she spoke with felt it would be very important for them to control who had access to the information.

While disclosure and common sense seem to be the key principles for introducing new technologies to seniors, Gaudet acknowledges there can be additional hurdles to clear. For example, when her organization installed a telehomecare system in one of its (non-medical) independent living communities, HIPAA unexpectedly became a factor.

The system allows residents to track health measurements using swipe cards that identify them individually. Even though it is intended for wellness and education purposes, because health-related information is involved, Northeast had to conduct HIPAA training for staff and get users to sign consent forms.

A Consumer-Driven Experiment

New Jersey-based Meridian Health is another provider delving into new technologies. The organization is participating in a six-month pilot program to test the QuietCare 24/7 Home Health Security System from Living Independently.

The QuietCare system uses five wireless activity sensors and a small communicator placed strategically in the senior's home. Initially, data from the sensors are collected to create a baseline for activity. Alerts are then automatically generated and sent to the caregiver when significant changes are reported. For example, if a senior does not exit the bathroom for an extended period, QuietCare alerts the caregiver via a phone call, e-mail, page, fax or secure Web page.

Meridian Health is testing the system both in assisted living and with older adults living in the community. However, consumers contract directly with QuietCare and then sign a waiver giving Meridian Health permission to view client information including alerts.

"We structured the pilot so family members are responsible for responding to the alerts," explains Sandra Elliott, Meridian's director of aging and senior service development. "Our goal is to learn how families use information regarding alerts and trends and assist in guiding them regarding options for care and service." In addition, this model minimizes the risk to Meridian Health, as well as any HIPAA concerns.

"We were very adamant that the family caregiver and older adult are the drivers of access to the information," Elliott says. Like Gaudet, she found that most people were willing to share information if it meant receiving assistance and peace of mind. Should Meridian Health decide in the future to take responsibility for responding to the alerts, additional HIPAA and liability issues would have to be considered.

The Letter of the Law

As more aging-services providers look to new technology ventures, it will be important to incorporate HIPAA into strategic planning, advises attorney Maureen Weaver chair of the long-term care practice at Wiggin and Dana. The first step is to determine what type of information is involved and which of the HIPAA rules apply.

The HIPAA privacy rule covers all protected health information, which is individually identifiable information about a person's physical or mental health that is transmitted or maintained in any form or medium. "It's inevitable that health information will be involved at some point along the way with these technologies, but the key is whether or not there are identifiers connected with it, such as a Social Security number or e-mail address," Weaver says.

American Telecare

Northeast Health makes sure its telehealth clients thoroughly understand how the technology works, and the benefits and risks that they incur by using it.

Providers are held to the HIPAA security rule when electronic protected health information (EPHI) is involved, Weaver explains. This includes any protected information that is maintained and transmitted in electronic form through electronic storage media. The key question is whether the information existed in electronic form before it was transmitted.

"Frequently people are confused about whether they're dealing with EPHI when information is transmitted through phone lines," Weaver says. "The basic rule is that voice mail and fax are not considered EPHI, but if you have a dial-up function with a computer on the other end that's giving or taking information, then it could be considered EPHI."

Resources

Northeast Health, Troy, N.Y.
Contact: Lisa Gaudet, manager, Office of Remote Care Technology, *gaudetl@nehealth.com* or (518) 271-3149.

Meridian Health, Neptune, N.J.
Contact: Sandra Elliott, director of aging and senior service development, (732) 751-3475.

Wiggin and Dana, New Haven, Conn.
Contact: Maureen Weaver, Esq., chair of long-term care practice group, *mweaver@wiggin.com* or (203) 498-4384.

University of Virginia Medical Automation Research Center, Charlottesville, Va.
Contact: Dr. Majd Alwan, director of robotics and eldercare technologies, *ma5x@virginia.edu* or (434) 924-2265.

Peter Swire, Bethesda, Md.
www.peterswire.net.

Providers also need to pay special attention to whether they are considered covered entities. For example, a senior housing provider who is not normally held to that standard might become a covered entity if it is participating in a telehealth pilot project or assisting residents in using the technology.

Another major issue is that implementing new technologies almost always involves interactions with non-covered entities, such as software vendors or device manufacturers. Yet, under the HIPAA security rule, it's the covered entity—in other words, the aging-services provider—who is obligated to ensure the confidentiality, integrity and availability of the protected information.

"The big picture is that covered entities must maintain reasonable and appropriate administrative, technical and physical standards to ensure the integrity and confidentiality of the information, and to protect against any reasonably anticipated threats, hazards, unauthorized uses or disclosures," Weaver says. She notes, however, that it's not an absolute standard. "The regulators have translated 'reasonable' and 'appropriate' to take scalability into account."

With this in mind, the main way providers can protect themselves is through the contracting process. "The focus should be on getting robust security provisions in contracts," Weaver says. "You need detailed representations that there is a disaster recovery and security plan, and that there are audit trails and safeguards in place."

Weaver cautions providers to be wary of vendors who claim their product is HIPAA-compliant. "There is no such thing as a standard for what makes something HIPAA compliant," she says. "You want to make sure that what you're buying will enable you to comply with HIPAA."

In addition to federal regulations, providers must be aware of state privacy laws. One emerging trend, which originated in California, is legislation requiring organizations to notify consumers when their personal information has been compromised. According to research by the Public Interest Research Group, as of January, at least 23 states had passed security breach notification laws.

Data Security 101

To minimize the risk of breaches and better evaluate potential vendors, providers must have a basic understanding of the technical aspects of data security.

There are four basic concepts of data security, explains Dr. Majd Alwan, director of robotics and eldercare technologies at the University of Virginia's Medical Automation Research Center: *authorization*, which involves issuing user names; *authentication*, which is a piece of information, such as a password or electronic signature, that serves to verify identity; *encryption*, which involves scrambling and coding sensitive data; and *surveillance*, which includes measures to detect and deter attempts at unauthorized access.

"Data security is often divided into the physical network and data security during transmission," Alwan says. "However, you cannot take care of data security during transmission but leave your workstations logged in and left open to the public. The same way you secure charts, you need to secure your data access devices and computers."

In data transmission, a key consideration is whether the information contains any identifiers. For example, in the case of in-home monitoring systems, if a sensor is simply communicating measured values to a data-acquisition device in the home, security is not a large concern; however, when that device transmits values along with information that specifically identifies a patient—such as to the care provider's server— security becomes paramount.

In general, when approaching the technical aspects of the HIPAA privacy rule, the guiding principle should be common sense, says Peter Swire, professor of law at the Moritz College of Law. From 1999 to early 2001, Swire served as the Clinton administration's chief counselor for privacy. "It requires reasonable security measures—not space-age NASA measures," he says. "It's supposed to be scalable, and we hope it's something we can all do."

Swire believes that the government recognizes the challenge of balancing security with usability. "You have to have a system that's good enough for a temporary nurse who's only there for two weeks to be able to give care to the patient," he says. "Any system which is that open is not going to be perfect."

Fortunately, for both providers and consumers, in most cases "good enough" is sufficient. "You're not designing systems against bank robbers," Swire says. "You're trying to set up pretty good systems that work for ordinary people."

Michele Hayunga is a freelance writer covering health care and business topics. She lives in Eldersburg, Md.