# MANAGING SECURITY RISKS *in* TELEREHABILITATION

*One of the most complicated topics in health care today is the security of patient health information.*

Most Americans are aware that the Health Insurance Portability and Accountability Act of 1996 (HIPAA) mandates privacy and sets rules and limits on who can access a person's health information. Many even have some knowledge that the Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009 addresses the privacy and security concerns associated with the electronic transmission of health information. Still, questions about security arise as new technologies emerge and drive the delivery of health care services.

One question in particular looms: Is patient health information at risk when services are delivered through consumer-based, Voice over Internet Protocol (VoIP) videoconferencing systems?

Associate Professor Valerie J. M. Watzlaf and her colleagues in the Department of Health Information Management have been researching the subject for more than a year. In two thought-provoking articles published recently in the *International Journal of Telerehabilitation,* they discuss risk analysis for privacy, security and HIPAA compliance as they apply to VoIP systems used in telerehabilitation.

The discussion revolves around three types of information security risks – confidentiality, integrity and availability – that have been developed by the National Institute of Standards and Technology (NIST) and used in HIPAA regulations. Confidentiality refers to the need to keep information secure and private. Integrity refers to information remaining unaltered by unauthorized users, and availability includes making information and services available for use when necessary.

Watzlaf sees the benefits of VoIP videoconferencing systems; "They provide a tremendous convenience for patients who might otherwise not be able to receive services. On the provider side, most offer a high-quality yet low-cost alternative to office teleconferencing systems. However," she continues, "to determine if VoIP technology is private, secure and compliant with HIPAA, a risk analysis should be performed."

To assist with that goal, Watzlaf developed a comprehensive HIPAA compliance checklist that guides clinicians and health care facilities in determining if the VoIP software system they are using meets basic privacy and security provisions.

The checklist* addresses a multitude of issues concerning how a VoIP company handles patient health information. Can it be accessed by employees within or outside of the VoIP company? How long do they retain personal information? What is the procedure if legal authorities request information? Can information be shared in other countries? Does the VoIP contain links to other websites that may have different privacy and security policies? Is the VoIP system encrypted for security?

In addition, Watzlaf suggests that health care providers form a team of clinical, legal and HIM professionals who understand the privacy and security policies of their VoIP system and who are willing to keep up to date on changes in federal and state policies regarding VoIP use.

*Watzlaf concludes that health care providers should consider using VoIP systems that are built specifically to provide telemedicine and telerehabilitation services.*

Obviously, clinicians and other rehabilitation personnel should be educated and trained in all aspects of privacy and security as they relate to telerehabilitation. Watzlaf also recommends that patients sign an informed consent that explains how the VoIP software will be used and why.

"There's a lot to consider here," muses Watzlaf. "But there's also a lot at stake."

"Recently there has been much discussion about whether VoIP systems are considered 'business associates' of the health care provider," she adds. "As such, they would be required to meet the new HIPAA requirements detailed under the HITECH Act."

Watzlaf concludes that health care providers should consider using VoIP systems that are built specifically to provide telemedicine and telerehabilitation services.

Platforms like VISYTER (Versatile and Integrated System for Telerehabilitation), which was developed in the Department of Health Information Management, support high-quality telerehabilitation within the home or clinical setting. Users must log in to a private server and enter a room that is restricted to the users who have privileges in that room.

All traffic data are encrypted, and there is no public ID or personal information that is accessible to others.

Ellen Cohn, associate professor in the Department of Communication Science and Disorders and associate dean for Instructional Development, has a strong interest in telerehabilitation, and looks forward to the treatment of more patients through this technology.

"Telerehabilitation's potential is perhaps unimaginable at this moment, due to rapidly emerging technologies and new applications, with more to come," observes Cohn. "What is not difficult to imagine is that health information professionals such as Professor Watzlaf and her colleagues will play key roles on telerehabilitation teams – safeguarding the security and privacy of electronic health records and Internet-based telerehabilitation encounters."

**The HIPAA Compliance Checklist may be found at http://telerehab.pitt.edu/ojs/index.php/Telerehab/article/view/6056.*