Weighing the Pros and Cons of IM: Instant Messaging Offers Instant Conveniences, Instant Complications

by Angela K. Dinh, MHA, RHIA

Communications technologies such as mobile devices and e-mail have taken healthcare and its practice into uncharted territory. Now organizations can add to this list instant messaging, or IM. More and more businesses are using IM in their daily operations.

According to America Online's most recent survey, 26 percent of its users use IM at work. Of that 26 percent, 58 percent use IM to communicate with colleagues, and 49 percent use it to get answers and make business decisions.[1]

Because IM allows communication in real time, it has the potential to increase productivity, reduce time on the phone, fax, and e-mail, and reduce errors in the translation of messages. However, its use in healthcare has both pros and cons, and organizations must consider the risks carefully and mitigate them accordingly.

The Bright Side and Dark Side

There are two schools of thought on IM use for business operations. Some believe that IM poses limited risks, while others believe IM opens doors to dangerous risks.

IM allows users to transfer files and images, which can be dangerous. IM was originally designed for entertainment purposes. The software did not take into account the possible transfer of sensitive data such as electronic personal health information.

IM software has a very basic technology structure, which creates many security issues. Users who are logged on to IM broadcast a signal to the Internet showing they are online. Hackers and other users can find that signal and attach themselves to it. IM creates a door into a user's computer, exposing it to worms, viruses, and other harmful malware.

These dangers can also find their way into a system through messages, file attachments, or transferred or shared drives. IM is capable of bypassing a computer's firewall and other security settings, unintentionally permitting a full view of a user's computer.

On the other hand, IM in the workplace offers several conveniences. It allows for easy communication between employees and reduces time spent on the phone, fax, and e-mail. Since IM is immediate, employees can get what they need quickly and proceed with their day.

For management, IM can be an easy way to communicate and monitor staff to see who is available and online and who is away from their desk. IM can provide easy, real-time access to remote staff.

The Effects of IM on HIM

Managing records of IM chats is tricky and exists in a gray area legally. Are IM chats part of daily business records and thus the patient's record? Depending on the content of the discussion, certain messages may need to be kept. Activity that contains electronic personal health information or involves a patient and that's passed between users should be logged and audited.

How does the new federal electronic discovery rule affect IM chats? By definition and based on content, IM could be included as discoverable information.[2] Therefore organizations must determine what information discussed through IM would be released as part of a request and be prepared to provide IM records if required during discovery.

IM clearly presents privacy and security obligations. If personal health information is exchanged, the need for privacy safeguards is a given. When it comes to security, physical and technical safeguards must be active.

The HIPAA security rule requires organizations to maintain audit logs and perform data audits. Some IM software has the ability to automatically log content of an IM conversation, but not all have this function. Legal counsel should be consulted when it comes to determining what IM conversations must be kept and what can be disregarded.

Safety and Security of IM

The reality for many organizations is that IM is already in use, regardless of the threats involved. Ways to reduce risk do exist, but there is no guarantee of full security. Microsoft and Symantec, two vendors of popular IM software, offer useful guidelines.[3,4] The best way to ensure protection is to use the best practices possible. Below are some recommendations:

- **Create a policy and procedure for the use of IM.** Establish the type of information that may and may not be discussed over IM, if file transfer is permitted, who has permission to use IM, and who employees may contact via IM. Allowing only employees and third-party business associates to IM will help reduce risk.
- **Allow only one IM software to be used,** and set firewall and security settings to prevent users from installing other versions. The more IM software versions in use throughout the organization, the more open the organization is to the Internet.
- **Restrict software downloads and installations to IT staff only.** This helps ensure that only the IM software itself is downloaded. Many times additional programs and plug-ins are offered for download with the IM software.
- Enable software settings to allow IM-ing with **only approved users** on the contacts list.
- **Encrypt all IM messages.** This is difficult to do, especially if users outside the organization have different encryption levels. Even if the organization has a high level of encryption, security is compromised if the message goes to a vendor with a lower level of encryption.
- **Use IM through a server.** Running all IM traffic through a server rather than direct PC-to-PC is safer because servers have more security levels than individual computers.
- Train users to **exit and log off of IM** at the end of every day. Just because users exit does not mean they are logged out of the IM software. Until users log off, their signals continue broadcasting on the Internet.
- **Hire an outside consulting group** to scan traffic to verify the electronic personal health information that is going in and out of the facility and adjust processes and management accordingly.[5]

To IM or not to IM, that is the question. IM has its advantages and disadvantages. Do the risks outweigh the benefits or do the benefits outweigh the risks? Every organization should carefully consider both when deciding whether or not to use IM.

If an organization chooses to use IM, it must develop policies on its use, outline processes, and continuously monitor employee use. Healthcare organizations must ensure the safety and security of patient information in any and all formats.

What Is IM and How Does It Work?

IM is a protocol-based Internet application that allows individuals to communicate through a variety of different devices. These devices include desktop computers and mobile devices such as PDAs and cell phones. This article focuses mostly on IM use through desktop computers.

IM offers real-time communication between two or more users. It allows users to carry on multiple conversations at the same time. More than two people can also participate in the same conversation (known as a chat room).

Like E-mail, but Different

IM works similar to e-mail; however, it differs in its delivery method. With e-mail, a message is sent and received through a server. Messages may be delayed in delivery depending on the server's security settings. IM is immediate and mimics a face-to-face conversation. Like e-mail, current IM software allows users to transfer files.

Unlike e-mail, IM users must have the same software to IM one another. However, recent advances allow for interoperability. All users must be online at the same time in order to IM.

Users must download IM software (most of which is free) to their computers. They then must create a unique screen name and password for log-in.

IM Basics

In order to begin IM-ing, users must first create a list of users with whom they wish to communicate. Any other contact information (such as e-mail address) is optional.

To initiate a conversation, a user simply clicks on the individual's screen name, types a message, and clicks send. An individual's personal settings can be set so the only people able to contact the user are those who appear on the buddy list.

IM also allows users to know when someone is online and available or away from their computer. Away messages can range from "out to lunch" to "in a meeting." Away messages are usually turned on and off by the user. After a certain amount of inactivity, IM will show the user as idle.

Notes

1. America Online. "Third Annual Instant Messaging Survey." Available online at www.aim.com/survey/#IM%20at%20Work.
2. AHIMA e-HIM Work Group on e-Discovery. "New Electronic Discovery Civil Rule." *Journal of AHIMA 77,* no. 8 (Sept. 2006): 68A–H.
3. Microsoft. "10 Tips for Safer Instant Messaging." Available online at www.microsoft.com/protect/yourself/email/imsafety.mspx.
4. Symantec. "Securing Instant Messaging." Available online at www.symantec.com/avcenter/reference/secure.instant.messaging.pdf.
5. Pierson, Ed. "Security: The Only Constant Is Complexity." AHIMA 77th National Convention and Exhibit Proceedings, October 2005. Available online in the FORE Library: HIM Body of Knowledge at www.ahima.org.

Angela K. Dinh *(angela.dinh@ahima.org) is a professional practice resource manager at AHIMA.*

Article citation:
Dinh, Angela K.. "Weighing the Pros and Cons of IM: Instant Messaging Offers Instant Conveniences, Instant Complications." *Journal of AHIMA* 78, no.8 (September 2007): 58-59.