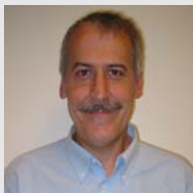


THE AUTHORS



Doug Jacobson, PhD.

- President & CTO of Palisade Systems, Inc.
- Director of the Information Security curriculum at Iowa State University
- Performed research for National Security Agency, U.S. Department of Defense, and the National Science Foundation.



Mark Glowacki, PMP

- Senior HIPAA specialist and lead instructor for the HIPAA Academy
- 20 years experience in application development for the healthcare industry
- Served on the Governor's Technical Advisory Subcommittee of the Iowa Community Health Management Information System



HIDDEN THREATS TO HIPAA

HIPAA Privacy Rule

Congress passed the Health Insurance Portability and Accountability Act of 1996 (HIPAA) to ensure the security and privacy of patient records. These laws mandate that all healthcare institutions take the necessary steps to protect patient information, especially electronic data, for administrative and financial functions.

The HIPAA Privacy Rule, which took effect on April 2003, requires all organizations that handle protected or patient health information (PHI) to put in place administrative, physical and technical safeguards for PHI in all forms, including electronic media. The recently published Security Rule focuses on electronic PHI or “e-PHI” to further stress the importance of protecting health information. Any occurrence of an unauthorized leak of information from an individual’s medical record is a breach of these rules. In order to comply with HIPAA regulations, American hospitals will spend as much as \$43 billion over the next five years according to estimates by the Blue Cross Blue Shield Association.ⁱ

These issues are also the concern of third party contractors who work with PHI. They are contractually obligated to provide the same safeguards as the doctors, hospitals and insurance companies who are directly regulated by HIPAA. The risk of having client information leaked cannot be ignored, as it can result in fines, exposure to lawsuits, and damage to public relations for the healthcare organization.

Security Issues

In the face of stringent security regulations, the rise in popularity of peer-to-peer (P2P) file sharing and instant messenger (IM) applications within the workplace is cause for alarm. File-sharing programs, such as KaZaA, can easily locate open ports on a firewall to defeat blocking attempts. These applications, while seeming benign, allow employees to covertly communicate and share virtually any file with an outside party. P2P and IM applications are almost impossible to detect, log, and manage with existing security methods, such as firewalls, intrusion detection systems (IDS), or Internet filtering. These security methods also require large investments of money and time.

FILE SHARING APPLICATIONS

File Sharing Dangers

In September 2002, the Aspen, Colorado city government learned about the threat of P2P file-sharing. City officials received an e-mail indicating that someone downloaded police department passwords and sensitive city information over KaZaA from its network. The user was searching for a movie and came across the entire contents of the network administrator’s hard drive.ⁱⁱ Organizations that allow P2P file-sharing applications to run unmonitored on their networks have lost control over what data can be shared outside of the organization.

Unintentional Sharing

Although some cases of sharing confidential client information are malicious, most involve users who are not savvy enough to restrict access only to appropriate files. A study conducted by Nathaniel S. Good and Aaron Krekelberg on the unintentional sharing of confidential files found “that the majority of the users in the study were unable to tell what files they were sharing, and sometimes incorrectly assumed they were not sharing any files when in fact they were sharing all files on the hard drive.”ⁱⁱⁱ The Good-Krekelberg study determined when looking for specific files accidentally shared on KaZaA, like e-mail accounts, that 61% of all searches performed returned one or more hits for these types of files.

Other Security Issues

Beyond the unintentional or deliberate sharing of sensitive information, peer-to-peer file sharing can expose healthcare companies to security risks that directly cause or indirectly facilitate HIPAA violations. These violations can occur through a variety of ways including:

- Files downloaded from P2P networks may contain viruses, worms, or hostile code. Organizations with any P2P users may be at risk as viruses and worms can spread undetected to a co-worker on the network. This would violate the HIPAA requirement for guarding against malicious software.
- Vulnerabilities in P2P applications may allow hackers to illegally access and alter PHI. This would violate several HIPAA requirements pertaining to accessing and maintaining the integrity of PHI.
- Spyware contained in P2P programs may allow the unauthorized collection and distribution of PHI or other confidential information. These programs are a part of the standard installation of Morpheus, KaZaA, and Bearshare. Exploitations using spyware would constitute a HIPAA access violation.

INSTANT MESSAGING APPLICATIONS

Instant message applications such as AOL Instant Messenger (AIM), MSN Instant Messenger, and ICQ can be an undetected conduit for sharing patient information. In early 2001, a hacker posted hundreds of pages of instant messages from Sam Jain, CEO of eFront, to a Web site for anyone to see. The logs revealed very sensitive corporate information to his employees, partners, and suppliers, and crippled his business.^{iv}

IM applications provide no control over the sharing of confidential materials. Employees using IM applications for communications related to patients opens an institution to critical information leaks which can be a breach of HIPAA access requirements. It would be easy for employees to illegally share PHI with outside parties, either unintentionally or maliciously, without the detection or knowledge of the healthcare organization. This defeats the purpose of the Privacy Rule's requirement that individuals be given an account of any unauthorized disclosures of their PHI, and violates several access requirements.

Besides violating HIPAA's Privacy Rule, free IM applications can evade firewall detection and create a porous security environment that can be exploited by hackers and other threats. Hackers can:

- Leverage well-documented IM security vulnerabilities to take over computers. Buffer overflow vulnerabilities have been reported consistently for MSN Chat, MSN IM, and AOL IM. Buffer overflows allow an attacker to run malicious code on a system that contains the vulnerability and take full control of the device. This could allow the attacker to compromise the integrity of PHI.
- Use viruses and worms to infect IM applications. Worms or viruses can compromise PHI and lead to violations of HIPAA integrity and access requirements.

According to a survey conducted by Osterman Research, the company found that IM is being used officially or unofficially in 84% of organizations. Over the next twelve months, they have forecasted this number to rise to 94%.^v Given the pervasiveness of instant messaging in the business world, it is critical to control the situation to avoid violating HIPAA mandates.

ⁱ Om Malik. A Y2K bug for health care. RedHerring. February 27, 2002.

URL: www.redherring.com/mag/issue111/1817.html

ⁱⁱ Michael Fitzgerald. P2P or Not P2P. InfoSecurity Magazine. October 2002.

URL: www.infosecuritymag.com/2002/oct/news.shtml#p2p

ⁱⁱⁱ Nathaniel S. Good, Aaron Kreckelberg. Usability and privacy: a study of Kazaa P2P file-sharing. Hewlett Packard Laboratories. June 5, 2002. Source: www.hp.com

^{iv} Paul Festa. ICQ logs spark corporate nightmare. CNet News.com. March 15, 2001.

URL: <http://news.com.com/2100-1023-254173.html?legacy=cnet>

^v Osterman Research. Osterman Research Survey on Instant Messaging. September 10 – 18, 2002.

URL: www.ostermanresearch.com/results/surveyresults_im0902.htm