

<http://www.sciam.com/article.cfm?id=peer-to-peer-file-sharing-security>

February 20, 2009 in



## **Hospital Workers Sharing Music? They May Also Be Sharing Your Medical Records**

By Larry Greenemeier

Health care workers using Gnutella or other peer-to-peer (P2P) networks to share music and video, may be putting you at risk for medical identity theft, Dartmouth researchers find

**HEMORRHAGING DATA:** A team of Dartmouth researchers found peer-to-peer (P2P) networks littered with sensitive health care information inadvertently made available by employees of hospitals and other health care facilities, as well as their collection agencies and other business partners.

If Obama has his way, the medical records of every American will be digitized by 2014. The stimulus package ([read the text here](#)) includes [\\$19 billion](#) in funding to pay for the effort and calls for the appointment of a chief privacy officer to advise the [U.S. Department of Health and Human Services](#) on how best to protect this sensitive information. If a new study of how easily your medical records can be found online by others is any indication, the new chief privacy officer (to be appointed over the next 12 months) will have his work cut out for him because an increase in digital medical records would likely mean an increase in medical identity theft.

Using software written specifically for scanning [Internet](#)-based peer-to-peer (P2P) file sharing networks, [Eric Johnson](#), an operations management professor at Dartmouth College's Tuck School of Business in Hanover, N.H., and colleagues recently found confidential medical files, involving thousands of people, including patient billing records and insurance claims containing Social Security numbers, birth dates, medical diagnoses and psychiatric evaluations. (The same type of information could have been found without the special search software, although not as quickly because the researchers would have had to search individual computers on each of the P2P networks they visited.)

Johnson's team found the data by trolling P2P networks such as [Gnutella](#), [FastTrack](#), [Aries](#) and [e-donkey](#). (A visit to the eDonkey2000 Network indicates it is no longer available.) The leaked information came from the health care organizations themselves, their employees working remotely, and from businesses that perform billing and other services for these organizations. "Our goal was to see the kinds of information that was leaking out, and P2P was simply a window into those organizations," says Johnson, who will present his findings on Monday at the [Financial Cryptography and Data Security '09 conference](#) in Barbados.

In P2P people share information stored on their computers with other people on a particular network, a practice first made popular by the music-swapping service [Napster](#). Often, P2P users must download software on their computers that allows others to search their computer for different files. [Allowing other P2P users to access your computer](#), however, means dropping your defenses (including firewalls meant to keep out snoopers and hackers).

Searching P2P networks, the researchers, for example, found a government application for employment that included detailed background information, including the applicant's Social Security number, full name, date and place of birth, and mother's maiden name. Ironically, the document also included a three-page intro highlighting the [Electronics Communications Privacy Act](#) measures undertaken by the government to protect the information in the document. Still, "it somehow ended up on to a P2P network," adds Johnson, who is also director of the Dartmouth's Glassmeyer/McNamee Center for Digital Strategies.

P2P users—there were an estimated 10 million of them in 2007, [according to an earlier study by Johnson and colleagues](#)—generally think that, because they're just looking to share music, the rest of the files on their computers are off-limits, says Alan Paller, director of research for the [SANS Institute](#). "But there are no defenses once you let someone inside your computer."

Over a two-week period last year, Johnson and his team used special P2P network analysis software developed by Cranberry Township, Pa.-based [Tiversa, Inc.](#), to search for information related to or mentioning the top 10 publicly traded U.S. health care providers, including two in Tennessee: Nashville-based [Hospital Corporation of America](#), and Community Health Systems in Franklin, the latter of which [in 2007 bought health care giant Triad Hospitals](#). When their searches turned up a file containing medical information on a particular computer, the researchers were able to use [Internet](#) Protocol (IP) addresses to trace that computer back to a particular location. In some cases, these files were located on computers connecting to the network from work, in others the computers were connecting wirelessly from homes, hotels or Starbucks.

In one case, Johnson and his team found two databases with detailed information on more than 20,000 hospital patients from the computer of a collection agency working for the hospital. Another search turned up a 1,718-page report with nearly 9,000 patient names, Social Security numbers, birth dates, insurers, group numbers and identification numbers. The researchers also found a pdf form for writing

prescriptions that was blank, except for a doctor's signature at the bottom. "This document could be used for medical fraud by prescription drug dealers and abusers," Johnson noted in his report.

Stolen medical information can be used to steal your identity and ruin your credit, or to affect your medical records, Johnson says. "If I assume your identity to obtain medical services, such as using your insurance information to go to the hospital for treatment, it's not only insurance fraud, it's also adding false information to your medical records," he adds.

P2P file sharing has become the "bane of the security officer's life" at many corporations, as well-intentioned employees put their personal information as well as their company's proprietary information at risk, says Nick Selby, a vice president and research director with [The 451 Group](#), a New York City-based technology research firm. People often use their work computers for personal reasons because they have higher bandwidth at the office, making it easier to download large music and video files. Although some P2P software allows users to specify which information they want to make available to the network, Selby adds, this software can easily be misconfigured and sensitive data made available to the network because people are using technology do not really understand how it works.

Johnson points out that the shift to digital health care records will not be easy. "The (Obama) administration is moving toward a national electronic health care records system," he says, "but the transition is going to be painful. It's not until they understand how to secure these records that we'll be safe." (The new chief privacy officer will have to not only secure new digital medical records but also promote ways to protect existing data.) The nirvana is to store this information in high-end databases systems that are well-secured, rather than in spreadsheets, e-mail and Word documents that can be left on someone's PC, he says, adding: If this cannot be done soon, hospitals and other health care organizations will need to restrict employee access to patient data.