

P2P Breach Leads to Walter Reed Data Leak

Patient records compromised

6/4/2008

An investigation launched Tuesday into the possible compromise of about 1,000 patient records at Walter Reed Army Medical Center serves as a stern reminder of how dangerous peer-to-peer (P2P) and other social networking applications can be, security experts warn.

The names, Social Security numbers, and birth dates of the patients were among the personally identifiable information in a computer file that was shared without authorization, according to a [statement](#) made by the Washington, D.C. U.S. Army hospital.

The risk of data breaches will only increase as use of file-sharing software becomes prevalent in the workplace, according to Paul Zimski, vice president of product solutions for Scottsdale, Ariz.-based Lumension Security.

"What's alarming about this incident is that it's not something you can stop at the network level," Zimski added. "Even hard drive encryption doesn't really work because when you file share, default installers will share out your My Documents, as well as your settings and Windows files."

Security pros such as Zimski say that if internal policies and procedures, periodic security audits, or both automated and manual whitelisting of acceptable applications aren't deployed at different enterprises, intrusions from file sharing will not only be more frequent but more sophisticated.

For its part, Walter Reed said in its statement that the Health Insurance Portability and Accountability Act of 1996 "protects patients from unauthorized release of their health records." It added that the hospital has "a robust information assurance program that meets all program standards and requirements."

According to media reports early Tuesday, the military officer in charge of Walter Reed, Col. Patricia Horoho, [circulated a memo](#) asking managers to ensure that the staff was not "loading or downloading programs that are not authorized by the command as it increases our vulnerability and possibly can cause a breach in protected." The memo was reportedly posted on the Walter Reed Web site before being taken down.

Security experts say that in cases like these, relying on an "honor system" is not sound policy.

"I think this is absolutely a case where unacceptable software should have been listed and banned beforehand," Zimski said. "ISPs have been trying to deal with peer-to-peer incursions for a long time and what companies need to know is that these applications are real stealthy on the network and not easily defensible unless the enterprise-wide system is locked from the inside."

--Jabulani Leffall

More From Newswire

- [First Look: Fedora 10 OS](#)
- [Linux-Based VDI a Reality](#)