

## FILE SHARING RISKY BUSINESS FOR DOCS

### File sharing risky business for docs

March 29, 2010 | Healthcare IT News Staff



OTTAWA – Doctors who use file-sharing software could be putting their patients' medical information at risk, according to a new study.

The study, which was published in the Journal of the American Medical Informatics Association, is the first of its kind to empirically estimate the extent to which personal health information is disclosed through file-sharing applications, said Khaled El Emam, Canada research chair in electronic health information, and the study's lead author.

Researchers used popular file-sharing software such as Limewire, BitTorrent and Kazaa to gain access to documents they downloaded from a representative sample of IP addresses. They were able to access the personal and identifying health and financial information of individuals in Canada and the United States.

"This type of software [LimeWire, BitTorrent and Kazaa] are like a hacker's dream," said Andrew Sroka, CEO of Fisher International, a data security provider.

"Peer to peer file-sharing software is designed to share files. When you authorize these programs on your computer, you are in effect offering up that hard drive to other users to search, copy and download," Sroka said.

For example according to Wikipedia in order to install Kazaa, you must install third-party spyware, which delivers pop-up ads and may collect personal data.

El Emam said he and his colleagues found evidence of outsiders actively searching for files that contain private health and financial data.

"There is no obvious innocent reason why anyone would be looking for this kind of information," he said. Researchers advised against using file-sharing tools to protect sensitive data.

Although this is a simple answer, says Robert Grapes, chief technologist of the Cloakware team in Irdeto, the reality is that most doctors are using their computers for more than just accessing patient records.

"E-mail, scheduling, bill payment, medical research, conference bookings and much more are normal activities for these computers, so it makes sense that some, not all, doctors will also install and use file sharing systems," he said. But trying to use the file-sharing software's own privacy safeguards requires considerable information technology expertise, said El Emam.

"File and folder encryption are reasonably simple approaches to bolster the protection of these records, but these security methods come with their own management and use challenges that also must be well understood," Grapes said.

"And even when the best security practices available to these programs are employed, it is still weak enough that it barely serves to slow down the professional hacker," said Sroka.

His take - physicians are using business tools in an environment that should be beyond reproach when it comes to the security process.

Only a small proportion of the IP addresses the researchers examined contained personal health information, but since tens of millions of people use peer-to-peer file-sharing applications in North America, that percentage translates into tens of thousands of computers, they said.