File-sharing software potential threat to health privacy

March 1 2010

The personal health and financial information stored in thousands of North American home computers may be vulnerable to theft through file-sharing software, according to a research study published online today in the *Journal of the American Medical Informatics Association*.

Healthcare professionals who take patient information home to personal computers containing peer-to-peer file-sharing software are jeopardizing patient confidentiality, note the authors of the study titled The Inadvertent Disclosure of Personal Health Information through Peer-to-peer File Sharing Programs.

"Computer users may be unaware that sensitive information in their personal files on their personal computers can be exposed to other users, because some vendors use software containing dangerous sharing features," says Prof. Khaled El Emam, Canada Research Chair in Electronic Health Information and lead author of the study.

El Emam's CHEO team used popular file sharing software 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. The research for the study was approved by the CHEO ethics board.

The study is the first of its kind to empirically estimate the extent to which personal health information is disclosed through file-sharing applications.

North Americans use file-sharing software such as Limewire, BitTorrent and Kazaa primarily to share and access music, videos, and pornography.

During their research on this project, 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," stated El Emam. "Very simple search terms were quite effective in returning sensitive documents."

Most Canadians would be better off not using file-sharing tools if they want to protect their sensitive information. "Trying to use the programs' own privacy safeguards requires considerable information technology expertise," add Dr. El Emam.

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.

The security of financial information has gained more public attention, and researchers did find that a higher percentage of downloaded files contained personal financial information. But as the United States and Canada move towards more digitization of health records, ensuring the privacy of health information is becoming a hot button issue.

A sample of the private health information the CHEO team was able to find by entering simple search terms in file-sharing software:

- an authorization for medical care document that listed an individual's Ontario Health Insurance card number, birth date, phone number and details of other insurance plans;

- a teenage girl's medical authorization that included family name, phone numbers, date of birth, social security number and medical history, including current medications;

- several documents created by individuals listing all their bank details, including account and PIN numbers, passwords and credit card numbers.

The study, financed by the Canada Research Chairs program, includes recommendations for managing risks when using file-sharing software.

Provided by Children's Hospital of Eastern Ontario Research Institute