



Trends in  
**Medical Research**

ISSN 1819-3587



Academic  
Journals Inc.

[www.academicjournals.com](http://www.academicjournals.com)

## Security Weaknesses in File-Sharing Methods Used in Clinical Trials Revealed

*Patients who participate in clinical trials expect that their personal information will remain confidential, but a recent study led by Dr. Khaled El-Emam, Canada Research Chair in Electronic Health Information at the CHEO Research Institute, found that the security practices used to transfer and share sensitive files were inadequate.*

The two-part study, entitled "How Strong Are Passwords Used to Protect Personal Health Information in Clinical Trials?," published February 16 in the Journal of Medical Internet Research, showed that the majority of passwords used to protect files are poorly constructed and easily cracked using commercial password recovery tools. Study coordinator interviews indicated that electronic information shared in the context of clinical trials may put personal health information at risk.

"The patients in these trials expect that their personal information will be protected," said Dr. El-Emam. "This is critical for maintaining the trust of clinical trial participants, and the public in general."

In the course of the study, passwords for 14 out of 15 sensitive files transmitted by email were successfully decoded. Of these 14, 13 contained sensitive health information and other potentially identifying factors such as name of study site, dates of birth, initials, and gender. File sharing practices were also found to be insecure, with unencrypted patient information being shared via email and posted on shared drives with common passwords.

"Cracking the passwords proved to be trivial," said Dr. El-Emam. "Choices included passwords as simple as car makers (e.g., "nissan"), and common number sequences (e.g., "123"). It was easy for the password recovery tools to guess them."

Poor security practices can be harmful to patients participating in clinical trials, who are at risk of being identified and possibly stigmatized by the disclosure of personal health information. There is also a potential for both medical and non-medical identity theft. In the context of international clinical trials, inadvertent disclosure of personal health information is considered a data breach in countries like the United States, which can lead to penalties in some states.

Dr. El-Emam believes that with some effort file sharing in clinical trials can be made secure: "There are protocols and tools that can be employed for secure file sharing. It may take more effort on the part of those who conduct clinical trials, but the alternative would not be acceptable."

Dr. El-Emam makes several recommendations, including enforcement of strong passwords and encryption algorithms, encrypting all information sent via email including site queries, and minimizing password sharing.

The study was financed by the Natural Sciences and Engineering Research Council of Canada (NSERC) and the Canada Research Chair program.

**Source:** Khaled El Emam, Katherine Moreau, Elizabeth Jonker. How Strong are Passwords Used to Protect Personal Health Information in Clinical Trials? Journal of Medical Internet Research, 2011; 13 (1) DOI: 10.2196/jmir.1335