

4 March 2009

By: Lucian Constantin, Web News Editor



Confidential medical records are being shared on P2P networks
Medical Data Systems

[Loads of Sensitive Medical Records Found on P2P](#)

Academic uncovers thousands of confidential files leaked from medical institutions on file-sharing networks

In a recently-released report, M. Eric Johnson, director of Dartmouth College's Center for Digital Strategies, describes how he has easily found an impressive amount of sensitive patient records being shared on peer-to-peer networks. Their origins have not been particularly named, but they include hospitals, clinics, centers and medical contractors, [Wired reports](#).

Mr. Johnson claims to have found around 160 files, which contain patient names, birth dates, Social Security Numbers, as well as insurance information and diagnosis codes, which can be used to determine what diseases they have been or are being treated for. According to the academic, no specialized search techniques have been used to track down the documents, except for regular search queries using simple keywords.

The files raising the most serious privacy concerns contain data such as psychiatric evaluations from several mental health institutions and the addresses and names of the patients of an AIDS clinic. Other documents pose significant identity theft or identity fraud risks. So are the ones containing the billing information of patients of a rehabilitation center or detailed insurance and personal information of those of a medical testing lab.

Another intriguing file is a drug prescription .pdf template, complete with the doctor's signature. Such a form could be used by virtually anyone to easily forge a prescription and acquire high-risk drugs. "For criminals to profit, they don't need to 'steal' an identity, but only to borrow it for a few days, while they bill the insurer carrier thousands of dollars for fabricated medical bills," is being pointed out in the report.

The research concludes that such data breaches add to the dangers that the health industry faces, besides their current problems. "The inadvertent disclosures we found and documented in this report point to the larger problem facing the industry. Clearly, such hemorrhages may fuel many types of crime. While medical fraud has long been a significant problem, the crime of medical identity theft is still in its infancy."

The leakage of sensitive data on peer-to-peer networks is mostly attributed to employee negligence or failure to enforce proper network security policies. The P2P file sharing technology is not dangerous by default, but can pose serious risks when it's not used properly. While in a corporate environment its employment can be easily controlled by enforcing network-wide filters and rules, this level of protection does not extend to employees who install such software on their company-issued laptops or computers while at home and expose confidential files to the entire world.

We have recently [reported](#) that the full design specs for the U.S. presidential helicopter, called "Marine One," have been detected on the Gnutella file-sharing network by employees from Tiversa, a P2P intelligence company. One of the computers found sharing the "Marine One" avionics package, which was leaked by a defense contractor employee, was located in Tehran, the capital of Iran.