TruSecure Corporation
“Planning for Failure” Presentation
Case A
Full story available at WashingtonPost.com

Hacker Accesses Patient Records

By Robert O'Harrow Jr.
Washington Post Staff Writer
Saturday, December 9, 2000; Page E01

A hacker gained access to confidential medical information at the University of [ABC] Medical Center, using the Internet to download thousands of files containing patient names, conditions, home addresses and Social Security numbers, hospital officials said yesterday.

Working through a publicly available Web site, the intruder planted a software program to sniff out passwords for the school's sprawling internal network. Then he assumed the identity of a legitimate computer user and tapped into two databases containing 4,000 or more patient records in May and June.

The break-in is one of the most penetrating breaches of medical privacy in memory. Specialists say it demonstrates the increasing vulnerability of confidential records as the health-care system rushes to computerize files and make them available via computer networks. University officials in Seattle said they first determined that the center's computers had been invaded in late June, but weren't sure any electronic records had been taken until late Thursday, after a reporter sent them a copy of one record.

"I don't think anything is secure anymore," said John C., 60, of Kent, Wash., a heart-transplant patient and victim of the intrusion. A copy of his record contains details about medical procedures, his Social Security number, his height, weight and date of birth. "It's nobody's business unless I choose it to be someone's business," he said. Edwin G., another heart patient whose records were pilfered, said he worries that some people might lose their jobs or insurance if their conditions became public. "Sometimes the consequences of having your medical records revealed could cost you a great deal," said Edwin, 65, of Seattle. "It's really bothersome to feel that there's so little security."

The hacker was motivated by a desire to publicize weak security at the hospital, not selling or misusing the records, said the online journalist who first disclosed the incident this week. The hacking incident also underscores how fragile data protections become when people with little training in security link computers or networks containing sensitive records to the Internet. Officials at the medical center acknowledged that the hacker exploited just this kind of arrangement. They described the case as a criminal act and on Thursday referred it to the Federal Bureau of Investigation.

Tom M., the director of information systems at the medical center, acknowledged that poor security procedures and the growing nexus of databases at the medical center made the intrusion easier for the hacker. He said in an interview that a Web site in the health sciences department of pathology, which served as the platform for the hacker, previously had about as much security as a computer dedicated to history or literature, even though it was linked to databases containing patient records. The university has improved security, Tom M. said, but challenges remain.

"Your whole network security is only as good as its weakest link," said Tom M. He added that before the improvements the center's network was like "a party line" that allowed the hacker's computer program to lurk in wait for passwords and user names. Now the system does a better job of blocking access to unauthorized users, he said. "We need to continue to be vigilant about this, because the types of technologies change, and so do the types of attacks," Tom M.said.

Janlori Goldman, director of the health privacy project at Georgetown University, said the episode shows the health-care system should slow down its use of computerized records. "Right now we've got a huge push to put patients' medical records online so that doctors, hospitals and health plans can quickly and cheaply share information," Goldman said.

"It is irresponsible to go forward without strong and enforceable privacy and security laws, which we don't have at the federal level yet." New federal rules governing the security and privacy of electronic medical records have been mandated by Congress, but won't take effect until 2003.

The computer break-in was made public Wednesday by Kevin Poulsen, an online journalist who has served time in prison after pleading guilty to computer crimes. He described the man he says broke into the medical center's files as a 25-year-old security expert from the Netherlands, who uses the name Kane. He declined to provide more details, but said the hacker approached him, through intermediaries, just over a week ago.

Poulsen is editorial director of a site called SecurityFocus.com. He said Kane gave him some 4,000 electronic records, saying he wanted to publicize the security risks at the medical center as a public service. Kane denied any plans to sell, make public or otherwise misuse the records, Poulsen said. "From his point of view, he is more of a whistle-blower than a criminal," said Poulsen, who provided The Washington Post with images of several electronic records. Medical center officials verified the records came from their databases.

A decade ago, while still a hacker, Poulsen broke into telephone systems. On one occasion, he used his hacking skills to win a radio call-in contest for a Porsche. He later pleaded guilty to several counts of computer crimes, and was sentenced to time served awaiting trial. He said that hacking hospital records has been one of the "looming menaces." The breach at the University of [ABC] hospital shows such threats have "gone from an apocryphal horror story to a reality," Poulsen added.

University officials said an analysis of computer logs found the hacker had probably penetrated security in May. After snaring a password using what's called a "sniffer program," the hacker accessed an administrative database set up for tracking patients receiving follow-up care. The stolen records contained limited information about patients' conditions and treatment, Tom M.said. The hacker did not get access to the hospital's primary patient-care records, he said. "Tools are getting so simple to use," he continued. "This is a database created essentially . . . without any regard to security or the sensitivity of the information."

Tom M.said computerized records are important for research and to provide better care. But he said the effects of bad security can be devastating for patients.

"The consequences are awful, there's no question," he said. "Because of the risks, etcetera, it becomes everybody's responsibility."