Cybertrust
"How the Heck Did This Happen" Presentation
Case C - 1
Full story available at: at http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2003/10/22/MNGCO2FN8G1.DTL
October 2003

A woman in Pakistan doing cut-rate clerical work for UCSF Medical Center threatened to post patients' confidential files on the Internet unless she was paid more money. To show she was serious, the woman sent UCSF an e-mail earlier this month with actual patients' records attached.

The violation of medical privacy - apparently the first of its kind - highlights the danger of "offshoring" work that involves sensitive materials, an increasing trend among budget-conscious U.S. companies and institutions. U.S. laws maintain strict standards to protect patients' medical data. But those laws are virtually unenforceable overseas, where much of the labor- intensive transcribing of dictated medical notes to written form is being exported.

"This was an egregious breach," said Tomi Ryba, chief operating officer of UCSF Medical Center. "We took this very, very seriously. She stressed that the renowned San Francisco facility is not alone in facing the risk of patients' confidential information being used as leverage by unscrupulous members of the increasingly global health-care industry. "This is an issue that affects the entire industry and the entire nation," Ryba said. Nearly all Bay Area hospitals contract with outside firms to handle at least a portion of their voluminous medical-transcription workload. Those firms in turn frequently subcontract with other companies.

In the case of the threat to release UCSF patient records online, a chain of three different subcontractors was used. UCSF and its original contractor, Sausalito's Transcription Stat, say they had no knowledge that the work eventually would find its way abroad. The Pakistani woman's threat was withdrawn only after she received hundreds of dollars from another person indirectly caught up in the extortion attempt.

The $20 billion medical-transcription business handles dictation from doctors relating to all aspects of the health-care process, from routine exams to surgical procedures. Patients' full medical histories often are included in transcribed reports. While it's impossible to know for sure how much of the work is heading overseas, the American Association for Medical Transcription, an industry group, estimates that about 10 percent of all U.S. medical transcription is being done abroad.

For two decades, UCSF has outsourced a portion of its transcription work to Transcription Stat. Kim Kaneko, the owner of the Sausalito firm, said she maintains a network of 15 subcontractors throughout the country to handle the "hundreds of files a day" received by her office. One of those subcontractors is a Florida woman named Sonya Newburn, whom Kaneko said she'd been using steadily for about a year and a half. Kaneko knew that Newburn herself used subcontractors but assumed that was as far as it went. What Kaneko said she didn't know is that one of Newburn's transcribers, a Texas

man named Tom Spires, had his own network of subcontractors. One of these, apparently, was a Pakistani woman named Lubna Baloch.

On Oct. 7, UCSF officials received an e-mail from Baloch, who described herself as "a medical doctor by profession." She said Spires owed her money and had cut off all communication. Baloch demanded that UCSF find Spires and remedy the situation. She wrote: "Your patient records are out in the open to be exposed, so you better track that person and make him pay my dues or otherwise I will expose all the voice files and patient records of UCSF Parnassus and Mt. Zion campuses on the Internet." Actual files containing dictation from UCSF doctors were attached to the e- mail. The files reportedly involved two patients.

"I can't believe this happened," Kaneko said. "We've been working for UC for 20 years, and nothing like this has ever happened before." The files in question were quickly traced to Newburn, the Florida woman, who typically handled about 30 UCSF files every day. An emotional Newburn said in an interview that she's as much a victim as Kaneko. "I feel violated," she said. Nevertheless, she said she's taking responsibility for what happened, even though she said she explicitly told Spires not to send any work overseas. "What he did was despicable," Newburn said.

Spires could not be reached for comment. E-mail to his company, Tutranscribe, was returned as undeliverable this week. Newburn said she contacted Spires as soon as she learned about Baloch's threat and obtained a number to reach the Pakistani transcriber at her home in Karachi. "I spoke with her," Newburn said. "She was very upset but said she wouldn't have really released the files. So I said she had to take back the threat." Newburn agreed to pay a portion of the money Baloch claimed she was owed - about $500 - and Baloch said she would tell UCSF that its files were safe.

On Oct. 8, UCSF received a second e-mail from Baloch. "I verify that I do not have any intent to distribute/release any patient health information out and I have destroyed the said information," she wrote. "I am retracting any statements made by me earlier." The problem, however, will not go away so easily. "We do not have any evidence that the person has destroyed the files," acknowledged UCSF's Ryba.

Moreover, how can UCSF or any other medical institution prevent something like this from happening again? Should legislation be passed barring U.S. medical data from going overseas? "I don't know the answer to that," responded Amy Buckmaster, president of the American Association for Medical Transcription. "We don't say that outsourcing is a terrible thing. We say that it needs to be disclosed."

UCSF has reached the same conclusion. Ryba said the medical center is revising its contracts with transcription firms to require up-front notice of all subcontracting. At the same time, she accepts that with a growing percentage of transcription work being exported abroad, there will always be a chance that something like this could happen again.

"We'll have to live with this risk on a daily basis," Ryba said.

TruSecure Corporation
"How the Heck Did This Happen" Presentation
Case C - 2
Full story available at: : http://sfgate.com/cgi-bin/article.cgi?file=/c/a/2004/04/02/MNGI75VIEB1.DTL&type=printable
October 2003

Extortion threat to patients' records Clients not informed of India staff's breach

An Ohio company that outsources U.S. medical files to India, including patient records from several California hospitals, was the victim of an extortion attempt in October by its own workers in Bangalore, who threatened to reveal confidential materials unless they received a cash payoff.

The security breach was alarmingly similar to a threat received by UCSF Medical Center just three weeks earlier from a Pakistani woman who was transcribing the Bay Area hospital's files.

Yet Steven Mandell, head of Toledo's Heartland Information Services, failed to mention the extortion incident when he was summoned last month by anxious California lawmakers to testify on steps his industry is taking to safeguard outsourced information. "No one asked me about it" at the hearing, he said. "If anyone had asked me, I would have been more than willing to discuss it."

Mandell acknowledged, though, that there was no reason lawmakers would have thought to bring up the subject. He said Heartland kept the incident to itself and did not even inform clients about what had happened. "Heartland Information Services is very serious about maintaining its commitment to keeping patient information private," he said in his testimony. "Patient data is one of the most valuable assets a health care organization possesses, and it deserves the utmost protection."

But according to an internal memo issued to Heartland employees on Nov. 6 and obtained recently by The Chronicle, the company was the victim of an extortion attempt last fall by two workers at its Bangalore site. "Through an anonymous e-mail, they threatened to release confidential patient records to the public if certain demands were not met in a specified time frame," Tracy Boesch, Heartland's chief operating officer, wrote in the memo. She did not specify the demands made by the Bangalore workers, except to say that they "attempted to extort certain concessions from the company."

Heartland handles transcription of doctors' dictated notes for dozens of U.S. hospitals, including Riverside Community Hospital in Southern California. The company is a subsidiary of HCR ManorCare, a leading operator of nursing homes. Mandell said Thursday that Heartland took the threat very seriously as soon as the workers' e-mail was received at the Toledo headquarters shortly after 10 a.m. on Oct. 28. He said company officials in Ohio and India quickly mobilized to track down the senders.

Within hours, Mandell said, it was learned that a manager's office in Bangalore had been broken into. He insisted that no patient information was stolen, only training documents

containing details of medical procedures. Heartland then traced the e-mail to a local Internet cafe and determined which employees lived nearby.

"We managed to identify the employees, and they confessed," Mandell said. "We recovered the documents, and the employees were arrested by the Indian police. They were locked up in jail for three days and are now out awaiting trial." He said one of the workers told authorities that he wanted an unspecified sum of money, "and the other said he didn't like who we appointed as managers." Mandell said he felt he was under no obligation to inform clients about the episode.

"Why?" he asked. "No patient information was ever at risk. It was nothing more than disgruntled employees. This shows that the system works." Sen. Figueroa said she would have wanted to know at last month's hearing about the theft of internal documents and the threat against Heartland. "It certainly seems relevant to what we were discussing," she said.

But ***Mandell said his goal was to "explain why I have the most secure system in the world. And that's what I did."***