Two Laptop Computers Stolen from UCLA Medical Center

UCLA began mailing letters June 5 about the theft of a laptop computer from a locked van at a UCLA blood drive last November. The computer held a database containing personal information from some 145,000 people who have donated blood and platelets to the UCLA Blood and Platelet Center since 1985.

The password-protected information included donors ' names, birth dates and Social Security numbers, but no medical data other than blood type.

A second laptop was stolen two weeks ago from a UCLA Healthcare financial office that could put an additional 62,000 patients at risk. The hospital will notify these people by letter in the next few weeks.

Both thefts were reported to the University of California Police Department.

"When the first laptop was stolen in November 2003, the hospital reported the crime to the police as a property theft," explained Frances Ridlehoover, chief operating officer for UCLA Medical Center. "When we were reviewing and updating our patient-privacy policies in the spring, we realized that persons named on the stolen blood-donor database could be at risk for identity theft. We immediately began to inform all donors who were potentially at risk.

"We deeply regret our delay and the security breach," she said. "We have put new measures into place to better assure that sensitive data stored on laptops are encrypted, protected and limited to essential need."

"Blood donors are generous people who sustain the lives of thousands of UCLA patients each year. We would feel terrible if any harm befell them, "said Dr. Priscilla Figueroa, director of transfusion medicine for UCLA Medical Center.

"While this is worrisome, we have no evidence that anyone has extracted the private information and is using it," she added. "We wanted to advise our donors to be extra alert to signs of possible misuse of their personal identities."

When administrators recognized the security breaches in May, management began an educational campaign throughout UCLA Healthcare to reemphasize the importance of security. The medical center is expanding encryption on all laptop and desktop computers and limiting what confidential information is stored.

Social Security numbers will display only the last 4 digits wherever possible. Helpdesk staff will assist UCLA Healthcare employees in removing private information from laptop and desktop computers and relocating it on secure network servers. Employees must encrypt any sensitive information that needs to remain on their computer's local drive.

The administration is preparing to send an email to all managers to apprise employees of the new procedures and explain how to contact the helpdesk for assistance in completing the process.

Blood donors and patients who have questions are encouraged to call a free UCLA hotline at 866-776-6575, to e-mail questions to IDInfo@mednet.ucla.edu or log onto http://idinfo.medctr.ucla.edu. The Web site includes frequently asked questions, information on the UCLA theft and resources to protect one's credit against identity theft.