

Sensitive Information Requires Sensitive Handling

By Pamela Lewis, *Institutional Advancement*

Riding in an elevator, the supervisor of marketing heard people discussing proposed marketing strategies for the institution's practice plan. Unfortunately, she didn't know the people or how they acquired the information, which was being discussed without any consideration for who else was in the elevator.

No biggie, you say? Think again.

Sensitive information about UT Health Science Center students, employees, strategies and operations is proprietary and must be protected as such. Employees who handle sensitive information must follow all administrative, technical and physical safeguards implemented by the health science center for the protection of such information.

Employees may use or request sensitive information to perform their jobs. However, that information must not be shared with others, inside or outside of the health science center, unless the individuals have a legitimate business need to know and the information is shared in compliance with the applicable laws, regulations, policies and procedures, according to Karen Parsons, J.D., director of Institutional Compliance.

What does the institution consider sensitive information?

It includes: personnel data, Social Security numbers (see related information below), student information, patient information, research data, financial data, strategic plans, marketing strategies, employee lists and data, supplier and subcontractor information, and proprietary computer software.

Confidential Nature of Social Security Numbers

All employees must comply with the provisions of Business Procedures Memorandum No. 66, Protecting the Confidentiality of Social Security Numbers, which includes the following provisions:

- Employees may not request disclosure of a Social Security number if it is not necessary and relevant to the purposes of the health science center and the particular function for which the employee is responsible;
- Employees may not disclose Social Security numbers to unauthorized persons or entities;



- Employees may not seek out or use Social Security numbers relating to others for their own interest or advantage; and
 - Employees responsible for the maintenance of records containing Social Security numbers shall observe all institutionally established administrative, technical and physical safeguards in order to protect the confidentiality of such records.
- For more information, consult Business Procedures Memorandum No. 66, Protecting

the Confidentiality of Social Security Numbers, and Handbook of Operating Procedures, Policy 17.01, Responsibility for the Use of Information Resources, at <http://www.utsystem.edu/bpm/66.htm> and http://www.uth.tmc.edu/ut_general/admin_fin/planning/pub/hoop/17/17_01.html, respectively.

Questions related to these issues may be directed to the Office of Legal Affairs and Institutional Compliance, 713-500-3268. ★

Proper Use of Information Technology Helps Keep Sensitive Information Secure

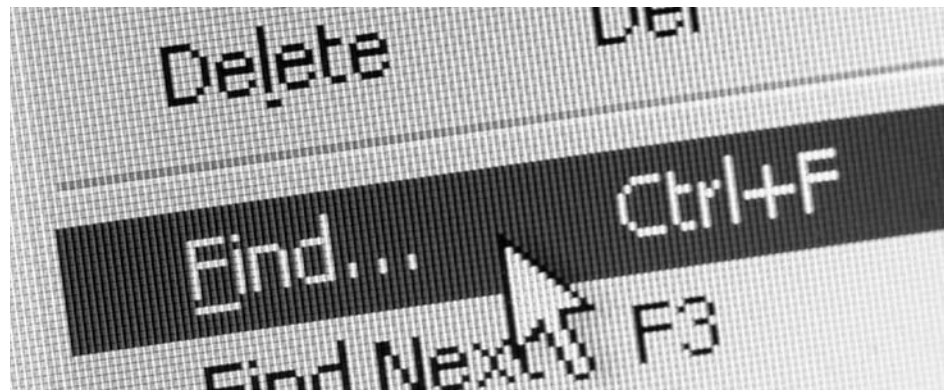
By Pamela Lewis, *Institutional Advancement*

Did you ever have the sneaking suspicion that you might have lost some of the UT Health Science Center's sensitive data by not taking proper care of it electronically?

Thomas F. Madden, chief information security officer, knows that it can happen without intent. But, he says, intent doesn't really matter. "If sensitive data is inadvertently released, it can cause major problems for everyone at the university." (See Sensitive Information, above.)

Among the ways that sensitive data can be lost is through:

- putting unencrypted information on a laptop that is then lost or stolen;
- leaving your office open with sensitive information on your computer while you are away from your desk;
- being "hit" by thieves trolling the World Wide Web using social engineering and technical subterfuge to steal consumers'



personal identity data and financial account credentials.

Social-engineering schemes use "spoofed" e-mails to lead consumers to counterfeit Web sites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers.

If you've gotten an e-mail claiming to be

from banks, e-retailers and credit card companies that you do or do not do business with, you've been "phished." Unfortunately, says Madden, phishers often convince recipients to respond. To check out confirmed phishing messages, visit http://its.uth.tmc.edu/aware_phish.htm. Through that site, you can also report phishing attempts to the Anti-Phishing Work Group, to which the health

science center belongs.

In addition, technical subterfuge schemes can plant crimeware on PCs to steal credentials directly, often using a type of spyware.

And then there are "pharming" schemes, in which crimeware misdirects computer users to fraudulent sites or proxy servers, typically through DNS hijacking, an Internet hacking trick that replaces the address of a valid Internet server with an intermediate one. Then people using that particular DNS server to visit <http://www.uth.tmc.edu> or "<http://www.uth.tmc.edu>" <http://www.uth.tmc.edu>, for example, are instead sent to an online gambling site. They have fallen victim to a DNS poisoning attack.

For more information about how to keep information on your computer secure, take a bit of time to read the latest IT Security Sense newsletter at <http://its.uth.tmc.edu/securitysense.htm>.

For more IT security information in general, visit http://its.uth.tmc.edu/aware_home.htm. ★

★ ★ ★ NewsBriefs ★ ★ ★

Medical School Pediatricians to Consult with State on Child Abuse Cases

The University of Texas Medical School at Houston will be the flagship site for a Texas Department of Family and Protective Services statewide program to provide expert consultation for suspected child abuse cases.

The program will target rural areas where experts who can spot the signs of child abuse are not readily available. The one-year, \$3.4 million agreement also provides for ongoing training for Children's Protective Services (CPS) workers on child abuse and related issues.

Rebecca Girardet, M.D., associate professor of Pediatrics at the UT Medical School, said CPS workers now can contact child abuse experts from anywhere in the state using a toll free number.

"They can ask questions, give us case descriptions and send us pictures, and the physician provides consultation concerning whether or not abuse has occurred. This allows the CPS worker to determine how best to protect the child," Girardet says. The network also is developing a Web-based system for electronic consultations and

learning modules.

"This program will allow us to have a coordinated center approach to address suspected child abuse cases," says Margaret McNeese, M.D., associate dean of Admissions and Student Affairs and professor of Pediatrics at the medical school. "We are looking forward to collaborating with other physicians across the state to help us deliver this much-needed care."

— *Melissa McDonald*

SPH to Lead National Research Seeking Stem Cell Therapies for Heart Disease

The Coordinating Center for Clinical Trials at The University of Texas School of Public Health (SPH) has received a new, \$17.9 million grant to serve as the hub of a nationwide network conducting research on emerging stem cell-based treatments of cardiovascular disease. Funded by the National Heart, Lung, and Blood Institute (NHLBI) of the National Institutes of Health, the five-year grant runs through 2011.

"We are excited to have this opportunity to participate in research to test the efficacy of stem cell therapy.

Our Coordinating Center for Clinical Trials has extensive experience in coordinating large clinical trials and looks forward to working with stem cell therapy researchers and the NIH to advance the knowledge base for this new type of medical treatment," says SPH Dean Guy S. Parcel, Ph.D.

A multi-center Cardiovascular Cell Therapy Research Network (CCTRN) will be organized to conduct phase I and II collaborative clinical trials. The SPH's Coordinating Center for Clinical Trials (CCCT) in the Texas Medical Center will select and oversee a core cell processing

center, chemistry labs or imaging centers in support of the selected studies.

"Over the next five years, the clinical centers will carry out a number of important stem cell research efforts," said principal investigator Lemuel A. Moyé, M.D., Ph.D., professor of Biostatistics at the UT School of Public Health. "Our role is to coordinate that network and design, execute and analyze clinical protocols that constitute the early clinical phase of stem cell research."

— *David R. Bates*