

AHP in the News
6,000 UCSF Patients' Data Got Put Online
San Francisco Chronicle, May 2, 2008
by Elizabeth Fernandez

AHP's Response on May 2 San Francisco article "6,000 UCSF Patients' Data Got Put Online"

Dear Editor:

Rarely is any nonprofit entity in the fundraising community in violation of the Health Insurance Portability and Accountability Act (HIPAA) privacy laws, as your May 2 story about the unfortunate release of patient data online might seem to imply. Nor was the tax-exempt hospital conducting a "little-known practice" of fundraising as the article states.

Not-for-profit, tax-exempt hospitals and health care organizations have been raising funds from grateful patients and the community for over 100 years. This professional activity by the hospital is a well-established and welcomed practice by grateful patients and the health care institution's community. It is those grateful patients and their families' donations that fund a wide range of programs, including pre-natal screening, free dental care, community clinics, hospice programs, drug recovery programs, cancer screening initiatives, mobile mammography vans, coverage for the uninsured and large capital expenditures. Let's not forget that many not-for-profit hospitals rely on philanthropy in this day of razor thin profit margins.

In fact, the current HIPAA regulations recognize that fundraising is a part of the institution's health care operations and it permits health care organizations to contact grateful patients for that purpose. The health care institutions' fundraising "arm" is permitted access to demographic information, which the article did state. And the article is correct that medical information is not permissible under HIPAA. AHP provides its members with an in-depth analysis of the regulations on its Web site, as well as providing articles and virtual learning sessions on the topic.

And AHP has worked closely with the Office for Civil Rights (OCR) of the U.S. Department of Health and Human Services. In fact, OCR recently told the Association for Healthcare Philanthropy (AHP) that practically none of the complaints it has received alleging violations of the HIPAA privacy rules involve fundraising. Through February 2008, the Civil Rights Office has received a total of 33,916 complaints, a minimal number when compared to the billions of medical records that exist, since the rule's April 14, 2003 effective date.

AHP wants Californians to know that notwithstanding this unfortunate incident, the philanthropic health care organizations that belong to AHP have fostered voluntary compliance of the highest order and have fully cooperated with the Federal government on HIPAA.

AHP, established in 1967, is a not-for-profit organization whose 4,600+ members manage philanthropic programs in 2,200 of North America's not-for-profit health care providers. We take our HIPAA compliance responsibilities very seriously. AHP has launched a Performance Benchmarking Service, an integrated database of business practices and performance metrics which helps participating hospitals and health care system development offices improve philanthropic fundraising and fosters greater transparency, a key factor contributing to HIPAA compliance.

Very truly yours,

William C. McGinly, Ph.D., CAE
President, Chief Executive Officer

6,000 UCSF Patients' Data Got Put Online
San Francisco Chronicle, May 2, 2008
by Elizabeth Fernandez

San Francisco -- Information on thousands of UCSF patients was accessible on the Internet for more than three months last year, a possible violation of federal privacy regulations that might have exposed the patients to medical identity theft, The Chronicle has learned.

The information accessible online included names and addresses of patients along with names of the departments where medical care was provided. Some patient medical record numbers and the names of the patients' physicians also were available online.

The breach was discovered Oct. 9, but the medical institution did not send out notification letters to the 6,313 affected patients until early April, nearly six months later.

The consequences of health care data breaches can be significant, said experts. Sensitive information can be used by employers, health insurers and other entities to discriminate. Additionally, thieves can use purloined information to obtain medical treatment and prescription drugs and to file false medical claims.

"This is a large and very significant data breach," said Pam Dixon, executive director of the World Privacy Forum, a nonprofit public interest research and consumer education group. "To commit medical identity theft, all you need is a patient's name, address and the name of the hospital. If you have a doctor's name and the medical department where the patient was being treated, it is gold. If you add a medical record number, it is a disaster for patients."

Hospital officials say there's no indication of identity theft to date. Identifying potential donors

UCSF had shared information on its patients with a vendor, Target America Inc., which mines electronic databases amassing information about a nonprofit's potential or existing donors.

Target America, whose Web site says it maintains "the highest standards of security," tunnels through millions of electronic records to help nonprofits identify and cultivate future donors as well as current donors "who could be giving you more." Additionally, it unearths financial information about donor friends and business acquaintances - even offering maps of a donor's neighborhood.

The breach was discovered, said UCSF officials, when the hospital was alerted that a patient's name had been queried on the Internet "and it was listed in association with UCSF."

Corinna Kaarlela, UCSF director of news services, said immediate action was taken to close off the information. Ten days after the breach's discovery, UCSF ended its business agreement with Target America.

Nancy Johnson, president of Target America, said she could not discuss the matter because of client confidentiality.

The breach spotlights a little-known practice among medical institutions to plow the ranks of patients for fundraising purposes.

Hospitals and other health care providers are turning patients into "fundraising free-fire zones," said Dr. Arthur Caplan, chairman of the department of medical ethics at the University of Pennsylvania School of Medicine.

"The breach is a symptom, but the real ethics challenge is the extent to which health care institutions are tracking patients and their families for nonmedical reasons - for fundraising, marketing, advertising," Caplan said. "I don't think people are aware of the degree to which this is occurring, whether it's by a hospital or a nursing home or a hospice."

Vast patient list provided

Since 2004, UCSF said it provided the names and addresses of 30,590 patients to Target America, paying the company \$12,000 a year.

Hospital officials said it contracted with the company to assist "with identifying names of individuals who could potentially receive communications from UCSF."

"Identification of potential donors who were active in the philanthropic community was one objective, along with identifying individuals who had corporate relationships, such as board service, or were affiliated with relevant community programs and health care biomedical organizations," Kaarlela said.

After the breach was discovered, the hospital said it required Target America to hire "an objective third-party firm" to investigate. UCSF received the forensic analysis report March 26. It showed that information was potentially accessible from July 1 to Oct. 9 last year "if a query for a specific name was made." Notification letters were mailed to patients April 4.

To Dixon, the expert on medical identity, the disclosure lag was far too long.

"In Internet years, that's a century," she said.

In January, California began requiring health care providers to alert consumers if their medical information is breached. Swift notification is considered important so consumers can monitor credit reports and bills.

According to Joanne McNabb, chief of the California Office of Privacy Protection, notice should be given "in the most expedient time possible, without unreasonable delay."

"It's a judgment call, the how and the when part," McNabb said. "The idea is to give early warning so that people can take defensive action. On the other hand, you don't want to needlessly worry people."

How patients are at risk

While UCSF officials stressed that the breach did not involve Social Security numbers, Dixon said that patients could nonetheless be at risk for harm.

"With medical identity theft, there is so much on the line - only minimal information needs to go out for there to be a problem," she said.

Linking patients to the departments where they were treated, for instance, is problematic because it can serve as a key identifier of a patient's health condition.

A federal privacy regulation known as HIPAA, the Health Insurance Portability and Accountability Act, sets standards to protect personal health information. Health care entities are allowed, for fundraising activities, to release to business associates - without explicit individual authorization - certain demographic information, such as names, addresses and dates of treatment, but not information about health or health care.

"You cannot provide other information for fundraising purposes," said a senior official with the U.S. Department of Health and Human Services' Office for Civil Rights.

In the UCSF breach, the names of patients treated at four care units were released: chest and pulmonary, vascular surgery, pediatric surgery, and pediatric multiple sclerosis.

"It seems they may have released more information than permitted," said Gail Sausser, a HIPAA consultant and adjunct professor of health law at Seattle University's School of Law.

UCSF officials say the use of a department's name is not prohibited under HIPAA. But it acknowledged that such a disclosure is against its own "best practice" policy.

"Steps have been taken to reinforce this practice," Kaarlela said.

For one outraged UCSF patient whose name was part of the online data disclosure, the incident involved an alarming breach of medical trust.

"They told a fundraising company that I'm a patient - morally this should not ever be done by any health care provider," said the patient, a retired executive living in San Francisco. He asked that his name not be published.

"Medical records are supposed to be of utmost privacy," he said. "The University of California is high up in the totem pole for quality medical care. When you go there, the first thing you see are notices regarding patient privacy. Why in the world would they give out my private information? It boils down to monetary greed."

Online resources

Learn more about medical identity theft protection and your rights at these Web sites:

links.sfgate.com/ZDFS

links.sfgate.com/ZDFT

links.sfgate.com/ZDFU

Guard your identity

If you suspect medical identity theft:

- Request an "accounting of disclosures" from your health care provider and health insurer.
- Request a copy of current medical files from each health care provider.
- Watch your credit report.
- Correct false information in your file.

To help prevent medical theft:

- Closely monitor "explanation of benefits" sent by health insurer.
- Once a year, request a listing of benefits paid in your name by your health insurer.

Source: World Privacy Forum

