HEALTH
PRIVACY
PROJECT

Health Privacy Stories

What follows are but a sample of stories reported in the press about U.S. incidents affecting the privacy of personal health information. While many of these events took place prior to April, 2003 when the federal Health Insurance Portability and Accountabilty Act of 1996 (HIPAA) took effect, many others here have occurred with HIPAA in force. The federal Office for Civil Rights of the U.S. Department of Health and Human Services is responsible for HIPAA enforcement, but they have yet to impose even one civil penalty in response to the more than 20,000 complaints they have received since HIPAA became the law of the land. The Department of Justice has successfully prosecuted a total of four cases for criminal violations of the law.

These stories, organized into categories, represent only some of the events covered in the press or decided in our courts. Please read to learn more about why Health Privacy Project considers protecting the privacy of personal health information to be of vital importance. Post-HIPAA stories are also displayed in blue below throughout the document.

Post-HIPAA Stories

The California state Department of Health Services inadvertently revealed the names and addresses of up to 53 people living with enrolled in an AIDS drug assistance program to other enrollees by putting benefit notification letters in the wrong envelopes, officials said Friday. The department learned about the mix-up after 12 people in the drug assistance program phoned to say they had received letters addressed to someone else. The department on Friday mailed certified letters to the 54 enrollees, explaining the mix-up and asking that anyone who received a wrongly addressed letter destroy it. It also notified the California Highway Patrol, as is required by a state law on security breaches. The department is looking into ways to make the system more foolproof, such as using envelopes with window addresses, said health services Director Sandra Shewry. HIV/AIDS services and advocacy groups said this was the first known breach of that database. "I would hope this is an anomaly," said Jeff Bailey, director of client services for AIDS Project Los Angeles. (Engel, M., Mix-up breaches confidentiality of dozens in state AIDS program, *Los Angeles Times*, March 3, 2007)

Kaiser Permanente announced this week that a laptop computer containing names, membership identification numbers, dates of birth, gender, and physician information on 38,000 Kaiser Permanente members was stolen in the Denver area in early October from a car belonging to a Kaiser Permanente employee in California. (Laptop with patient info stolen, *Rocky Mountain News*, November 29, 2006)

Two computers containing health records on participants in Indiana's Breast and Cervical Cancer Program were stolen from a Jeffersonville health clinic, leaving more than 7,500 Indiana women at risk of identity theft, according to the Indiana Department of Health. Data stored on the computers may include names, addresses, Social Security numbers, medical information or other data. (Women alerted to possible identity theft, Associated Press, November 27, 2006)

Richard Yaw Adjei of Bear, Delaware pleaded guilty in federal court on November 16 to aggravated identity theft and three counts of fraud for his part in a widespread criminal scheme that used information from a hospital billing service to steal the identities of more than 400 people. U.S. Attorney Colm F. Connolly also announced the indictment of accomplice Linda Danyell Williams, a claims processor at a New Castle medical billing and collection firm, alleged to have sold Adjei information about more than 400 patients for an undisclosed sum. Adjei in turn set up a tax return business and used the stolen information, including names, birth dates, addresses, Social Security numbers, hospital admission dates, doctors' names, and diagnosis codes, to submit bogus tax returns and receive refunds totalling more than $300,000 in the names of at least 163 of the victims. (O'Sullivan, S., ID theft scam used medical billing info, *Delaware News Journal*, November 18, 2006)

The personal health information of more than 200 people was discovered by KPRC Local 2 TV investigators in unlocked garbage Dumpsters outside Houston area Walgreens, CVS and other pharmacies. Investigators found prescription labels, pill bottles and computer printouts disclosing detailed personal medical information. The Texas State Board of Pharmacy is expected to take immediate action. (Pharmacies dump medical information in trash, *KPRC Local 2 (Houston)*, November 15, 2006)

The Department of Veterans Administration confirmed on November 2 that a computer containing the personal data of former military servicemen and women was stolen from the agency's Manhattan hospital. VA spokeswoman Jo Schuda said the laptop computer, used to measure pulmonary function, was stolen from a locked room in a locked hallway at the VA hospital on East 23rd Street. The theft took place September 6, but VA officials sent out a letter to the 1,600 affected veterans only within the past two weeks. Their personal data was on the computer's hard drive. (Raymon, G., Data on veterans missing, Newsday, November 3, 2006)

The Sisters of St. Francis Health Services Inc. began contacting customers on October 9 regarding a July 28 incident with a contracted employee that representatives say left sensitive data of at least 260,000 Indiana and Illinois residents "out of hospital hands" for several days. An employee of Perot Systems, a company contracted to perform medical billing, copied the data onto several CDs to work on it from home. The contracted employee left the CDs in a store inside a bag she returned there. The CDs were recovered when another customer noticed them. Lisa Decker, director of public relations for Greater Lafayette Health Services clients, a subsidiary of the Sisters, said the companies are examining procedures and best practices involving patient information in hopes of preventing future mistakes. She said it was unclear as yet whether a single employee would have the freedom to transport such a volume of data in the future. (Brown, T., 260,000 told of data breach, *Journalandcourier.com* (Lafayette, IN), October 24, 2006)

A laptop computer containing the names and Social Security numbers of about 14,000 of Allina Hospitals and Clinics obstetrics patients was stolen from a nurse's car on October 8. Although two passwords are needed to access the information on the laptop, Allina acknowledged the potential for identity theft, according to a letter sent patients this week. The nurse whose computer was stolen said she had left the laptop in her car when she went in to a Minneapolis lab to drop off a specimen. The nurse believes she locked the vehicle, he added.In the future, Kanihan said, the laptops no longer will contain Social Security numbers. (Lonetree, A., Stolen laptop held personal data of thousands of Allina patients, Minneapolis-St. Paul Star Tribune, October 20, 2006)

Security weaknesses have left millions of elderly, disabled and poor Americans vulnerable to unauthorized disclosure of their medical and personal records, federal investigators said Tuesday. The Government Accountability Office said it discovered 47 weaknesses in the computer system used by the Centers for Medicare and Medicaid Services to send and receive bills and to communicate with health care providers. The agency oversees health care programs that benefit one in every four Americans. Its massive amount of data is transmitted through a computer network that is privately owned and operated. However, CMS did not always ensure that its contractor followed the agency's security policies and standards, according to the GAO report. "As a result, sensitive, personally identifiable medical data traversing this network are vulnerable to unauthorized disclosure," the federal investigators said. The network handling Medicare claims transmits extremely personal information, such as a patient's diagnosis, the types of drugs the patient takes, plus the type of treatment facility they visited, including treatment centers for substance abuse or mental illness. (Freking, K., Auditors: health records at risk, *Associated Press*, October 3, 2006)

The husband of a federal prosecutor in Seattle was one of 42 people whose personal information was stolen by a sophisticated identity-theft ring that stole patient data from Virginia Mason Medical Center between May 2005 and September 17. Susan Harrison discovered she and her husband were the victims of identity theft after thousands of dollars suddenly disappeared from their checking account in December. Two former medical center employees allegedly used fake ID badges to enter Virginia Mason facilities at night and lift data from the files of patients who had appointments the next day. (Bowermaster, D., Identity theft: it could happen to anyone, *Seattle Times*, September 28,2006)

Providence Health Systems agreed to reimburse the state of Oregon more than $95,000 in costs as part of a deal to settle a nine-month invetigation into the largest data breach ever reported in Oregon. Medical records of 365,000 patients, stored on computer disks and digital tape, were in a car stolen from a Providence home services employee. The data was not encrypted. The theft revived efforts to enact stronger privacy protections in Oregon and spurred some patients to back a class-action lawsuit seeking damages from Providence. (Rojas-Burke, J., Providence settles data breach, *The Oregonian*, September 27, 2006)

New York City's public hospital system will suspend 39 employees without pay for peeking at the private medical records of Nixzmary Brown. The case of the 7-year-old girl, who died in Brooklyn in January from beatings and torture, become a tabloid and TV news sensation, and dozens of workers at the Woodfull Medical and Mental Health Center apparently couldn't resist looking at the child's computerized medical file. The suspensions will last from 30 to 60 days, and each of the sanctioned employees will be required to undergo training in patient privacy rules before they return to work. (Caruso, D., Prying N.Y. hospital workers suspended, *Washington Post*, September 25, 2006)

A retired school teacher -- with two feet -- was stunned when hospital bill collectors demanded she pay for the amputation of her right foot. The victim of medical identity theft, Lind Weaver says trying to catch errors in her medical records and clear up hospital bills fraudulently run up in her name has "become a 40-hour-a-week job." Meanwhile, Anndorie Sachs received a call from a Utah state social worker that her hospitalized infant had tested positive for methampehtamine, yet Sachs hadn't delivered a baby in two years. A woman had used Sachs' stolen drivers license to check into the hospital to give birth. Weaver and Sachs join at least 200,000 Americans who have become victims of medical identify theft, according to a 2003 federal report. (Menn, J., ID theft infects medical records, *Los Angeles Times*, September 25, 2006)

A primary care clinic in Sorora, California released the Social Security numbers of 22 veterans to at least two patients signing in for appointments. Charles Kavanaugh was second in line for a blood test when he was given the list by a desk attendant. Officials of the Sonora Regional Medical Center, who operate the clinic, believe it was an isolated event. (Wyman, A., Blood lab slips up, releases SS info, *Union Democrat (Sonora, CA),* September 14, 2006)

A federal grand jury in Miami indicted Isis Machado, a former employee of the Cleveland Clinic and Health Management Associates and her cousin Fernando Ferrer Jr., who owned Advanced Medical Claims of Naples, with identity theft, computer and healthcare fraud, and violating the Health Insurance Portability and Accountability Act. Machado served as front desk coordinator at the clinic, had access to confidential patient information, and sold the information to Ferrer, who allegedly submitted fraudulent Medicare claims. A Cleveland Clinic spokesperson said the identities of 1,100 patients could be at further risk. Machado and Ferrer each face 30 years in prison and $750,000 in fines if convicted. (Taylor, M., "Former Cleveland Clinic worker, kin charged with fraud, HIPAA violation," *HIT Strategist*, September 11, 2006)

The Government Accountability Office issued a report calling for Medicare to exercise more oversight over how private plans transmit personal health records. Nearly half of all Medicare Advantage contractors surveyed reported breaches of private health records during the last two years. Information breaches most often occur when private contractors outsource health records to other companies for additional processing. According to GAO, 90 percent of Medicare contractors reported outsourcing health records domestically in 2005. (Perrone, M., "GAO urges more Medicare plan oversight," *Houston Chronicle*, September 5, 2006)

A Washington state mental health care provider, Compass Health, has notified authorities that a laptop computer containing data on an undisclosed number of patients was stolen more than a month ago. According to a media alert issued by Compass Health, the laptop contained information on clients of the clinic and its partners since October 1st, 2005. The information included Social Security numbers, "along with other clinical and demographic information." The theft occurred June 28. Compass did not say why it waited so long to issue the alert. (Bosworth, M., "Mental health clinic loses laptop bearing patient data," *ConsumerAffairs.com*, August 30, 2006)

Pediatric Services of America, Norcross, Ga., doing business as PSA HealthCare, has announced it will sell a business unit but has no new information about a stolen laptop computer with the personal information of 51,000 patients. The laptop contained the personal information of current and former patients, including their names, Social Security numbers and, "in a limited number of cases, personal healthcare information," according to a company news release. (Conn, J., "Stolen laptop delays company's financial forecast," *Modern Healthcare*, August 29, 2006)

The homecare division of William Beaumont Hospital, Royal Oak, Mich., asked the public to help it recover a laptop filled with three years of personal information on home-health patients, including names, Social Security numbers, medical data and insurance information. The laptop was stolen with an employee's car. The system said the information was encrypted and password-protected, but the laptop belonged to a new employee who had stored the ID access code and password with the computer. ("Mich. system says stolen laptop holds patient data," *Crain's Detroit Business*, August 23, 2006)

HCA, the Nashville-based group of hospitals, late last week said burglars broke into a regional office and stole ten computers containing names and Social Security numbers for thousands of patients treated at its facilities from 1996 until this year. The computers contain 15,000 to 18,000 files with information on Medicare and Medicaid patients who have uncollected copayments and deductibles. (Galloro, V., "10 PCs stolen at HCA office," *HIT Strategist*, August 14, 2006)

Madrona Medical Group, a is asking its patients to watch their credit reports after a former employee was charged with illegally downloading 6,000 patient files onto his personal laptop computer. (Gallagher, M., "Madrona patients may face ID theft," *The Bellingham Herald*, August 11, 2006)

A desktop computer containing personal information for up to 38,000 patients treated at Veterans Affairs Department medical centers in Pittsburgh and Philadelphia over the past four years was reported missing from the Reston, VA offices of VA contractor Unisys Corp. The VA and Unisys says the computer contained names, addresses, Social Security numbers and dates of birth. It may also have included insurance carrier and billing information, claims data and medical information. (Robeznieks, A., "Another computer with VA data goes missing," *HIT Strategist*, August 8, 2006)

The personal information of about 160,000 Northern California Kaiser Permanente members who receive hearing aid services was stolen with a computer from a secure office in Oakland. The information stolen included names, addresses, phone numbers, ages or dates of birth, appointment type and dates of service. (Raskin-Zrihen, R., "Patient data stolen from Kaiser," *Vallejo Times Herald,* August 7, 2006)

A laptop containing personal information about 257,800 patients of Poughkeepsie's Vassar Brothers Medical Center was stolen in late June, but some patients did not receive a letter of notification of breach until this week. The information in the laptop covers about 20 years of patient activity. ("Patient information stolen from N.Y. medical center," *Associated Press*, August 4, 2006)

An Indiana-based consultant was able to download the names, Social Security numbers and dates of birth for between 5,600 and 23,000 Georgetown University Hospital patients when he accidentally discovered the unsecured data on the website of e-prescribing vendor InstantDx. The consultant reports he accessed the data using a password he discovered hard-coded into Medisoft, a popular medical practice application. InstantDx was quick to accept responsibility for the breach. (Poulson, K., "E-health gaffe exposes hospital," *Wired Magazine*, July 25, 2006)

A state government computer was stolen during a July Fourth break-in at the offices of a drug dependency program, and officials were trying to determine Friday whether it contained sensitive information. Many top officials in state government were unaware Friday morning that a Public Health and Human Services computer had been stolen from a state office building on Tuesday. The agency later said it took a few days for the information to filter to top officials. ("Computer taken from Montana office," *Bismarck Tribune*, July 8, 2006)

Three laptops, one of them containing personal information on thousands of blood donors -- including Social Security numbers and medical histories -- were stolen from a locked closet in the Farmers Branch office of the American Red Cross during two separate incidents in May. Donors were not notified of the theft. Red Cross officials say they aren't overly concerned because the information was encrypted. The computers were recovered by officials on June 28, who report it appears that personal information had not been compromised. (Schreier, L., "Donor data stolen at local Red Cross," *Dallas Morning News*, July 1, 2006)

A backup tape containing the dates of birth, medical records and Social Security numbers of more than 16,000 held by the Department of Veterans Affairs Regional Counsel Office in Indianapolis. The VA might offer credit monitoring for anyone who could have been impacted by the security breach. The incident occurred two days after a laptop containing the personal information of more than 26 million veterans was reported stolen in Maryland. ("Veterans records tape missing from Indy office," *TheIndyChannel.com*, June 29, 2006)

Two Ohio University graduate students have filed lawsuits against the university due to recent data thefts from school computers. The plaintiffs are two of possibly 173,000 students, employees, or faculty whose Social Security numbers, names, addresses, medical records, and home addresses were stolen in five separate instances since March 2005. On the same day the suit was filed, the university announced its decision to spend $4 million to heighten computer security on campus, and last week it suspended its director of computer and network services pending an investigation. (Two students sue university, *ChannelCincinnati.com,* June 27, 2006)

Federal Centers for Medicare and Medicaid Administrator Mark McClellan reported that 17,000 beneficiaries covered by Humana, Inc. health care plans are at risk from unsecured computer data containing their personal information. McClellan says Humana's lapse violates Medicare's privacy and information security policies. The news follows reports of the theft of about 250 Humana plan applications last month in Minnesota. (U.S. Medicare official says Humana data not secured," *Reuters*, June 5, 2006)

Laptop computers with personal information on 72,000 Ohio low-income, disabled, and elderly Medicaid recipients stored on four computers were stolen from a private managed-care agency. Although the computers themselves were password protected, the files themselves were not. Data on the files included names, Social Security numbers, and addresses. ("Laptops stolen with Medicaid, Buckeye health member data," *The Toledo Blade*, June 3, 2006)

The Medicare prescription drug benefit applications for 268 people from North Dakota and Minnesota were stolen in a Minnesota car burglary. The applications for coverage by Humana's health insurance company included applicants' names, addresses, Social Security numbers, and bank routing information and were left in a briefcase in the car. North Dakota Insurance Commissioner Jim Poolman said he did not believe the company was being forthcoming about the extent of the data loss. He suspects customer information was also stored on a stolen computer inside the case. (Wetzel, D., "Medicare data at risk of theft of forms," *St. Paul Pioneer Press*, June 2, 2006)

A laptop containing personal information about 24,000 Cumberland County, N.C. emergency medical patients cannot be located by its owner, the local health department. Local police are investigating whether the computer was stolen, and the health department is reviewing its policies and procedures. ("Fayetteville police look for laptop containing patients' info," *wral.com*, June 21, 2006)

The University of Alabama in Birmingham earlier this month reported a laptop computer containing confidential information about 9,800 kidney donors, organ recipients, and potential recipients was stolen in February from its kidney transplant program offices. UAB said it took months for officials to reconstruct the information stolen in order to contact those affected. ("Data on 9,800 people missing after theft of computer," *Associated Press*, June 21, 2006)

A former Randolph County, NC nurse who stole the identity of 12 patients and ran up credit card bills in their names was sentenced to a prison term of almost three years. Having obtained patient names and Social Security numbers, Susan Pugh White used the information to create fake documents in order to obtain credit cards in the patients' names. Law enforcement discovered personal information on another dozen patients in White's possession. (E. Collins, "Nurse sentenced for identity theft," *News-Record.com,* June 16, 2006)

One of the world's largest insurers, American International Group, said yesterday a burglar stole computer equipment in March from one of its Midwest offices that contained personal information about 930,000 people. A company spokesperson said the data consisted of names, Social Security numbers and "fragments of medical information." The information was provided to AIG by insurance brokers seeking quotes for coverage on high levels of health insurance for employees of companies around the country. AIG declined to name these companies. (J. Treaster, "Insurer reports theft of data on 930,000," *New York Times*, June 15, 2006)

The Veterans Affairs Department announced it has been investigating allegations that an offshore medical transcription subcontractor threatened to expose 30,000 veterans' electronic health records on the Internet in a payment dispute with a VA contractor. According to testimony of VA's assistant inspector general for auditing, Michael Staley, at a House Veterans Affairs Committee hearing, "Contracts do not specify criteria for how to protect information." Staley also reported that a 2005 audit of information management security found instances where out-based employees send veterans' medical information to the VA regional office through unencrypted email, monitoring remote network access and usage does not routinely occur, and off-duty users' access to VA computer systems and sensitive informaton is not restricted. (M. Mosquera, "Rep. Buyer: Department CIO needs IT security enforcement authority," *Government Computer News*, June 14, 2006)

A computer file containing the data of 17,000 Medicare beneficiaries enrolled in Humana health care plans is not secure, according to a finding by the HHS inspector general. Applications with personal data for 250 people applying for Humana plans were stolen last month from an insurance agent's car. ("Humana computer data not secure," *Reuters*, June 5, 2006)

The names, birth dates, Social Security numbers, and, in some cases, disability ratings of as many as 26.5 million veterans were stolen recently from the home of a Department of Veterans Affairs employee on May 3 in suburban Maryland. The VA Inspector General is very critical of the Veterans Affairs department for its lax information security and emphasizes that the employee was not authorized to remove such sensitive material. This theft represents the biggest unauthorized disclosure of Social Security data ever. (C. Lee and S. Vogel "Personal Data on Veterans is Stolen," The Washington Post, May 23, 2006, Page A01)

In one of Oregon's largest security breaches, Providence Health System in January disclosed that a burglar stole medical records on 365,000 patients kept on disks and tapes that were left overnight in an employee's van. Then in two car break-ins, on Feb. 27 and March 3, thieves took laptops containing records on a total of 122 Providence hospice and home-care patients in Snohomish County, Wash. (J. Rojas-Burke, "Breach fuels privacy legislation," The Oregonian, May 23, 2006)

Twenty-five laptop computers that were stolen from Iowa Methodist Medical Center in DesMoines throughout May 2006 turned up on eBay near the end of that month. Although the computers did not contain sensitive information, they were most likely taken by a hospital employee as they had been stored in a locked room. No arrests have been made. (*The Associated Press*, May 18, 2006)

The names, birth dates, Social Security numbers and medical information for 60,000 students, faculty and staff at Ohio University were stolen in the third electronic security breach in three weeks. The university learned on May 4 that an unauthorized person gained access into a computer server that supports the Hudson Health Center. (J. Gonzalez, Third computer breach at Ohio University; Records involve 60,000 who used health center, *Plain Dealer (Cleveland)*, May 12, 2006)

The Pentagon has sent letters to more than 14,000 people who registered for a 2001 Defense Department conference on health care fraud whose names, Social Security numbers, credit card information and other personal information may have been stolen due to a breach of security of the computer system of Tricare Management System, a government health-care contractor. (S. Barr, Conference attendees' personal data may be at risk, *Washington Post*, May 10, 2006)

A woman reports she secretly removed pages from her medical record showing she was at risk of Huntington's disease, a fatal genetic disorder. Fearing the consequences of the disclosure of the information, She said she removed information from her file to protect the ability of her children to obtain health insurance. (R. Klitzman, The quest for privacy can make us thieves, *New York Times*, May 9, 2006)

A Washington state law requiring customers to sign a log book when purchasing over the counter products containing pseudoephedrine could compromise medical privacy, according to the American Civil Liberties Union, who fear that regular users of such products "may come under suspicion for what's actually an innocent act." (E. Porter, Meth clampdown should compromise medical privacy, *Kiro 7 Eyewitness News (Seattle)*, May 9, 2006)

The University of Texas Southwestern Medical Center sent letters to 1,447 patients in late April telling them of the theft on or about January 1 a computer hard drive containing their names, Social Security numbers and medical diagnoses patients from the center's ophthalmology department. The university's privacy officer delayed informing patients to allow to investigate its own employees, relying on data showing three quarters of such incidents are "inside jobs." (M. Stewart, North Texas patients may be ID theft victims, *CBS 11 News (Dallas),* May 8, 2006)

According to a November 2005 Gartner Inc. survey, nearly 80% of companies said that "managing data security and privacy risks' were very important or most important when disposing of obsolete hardware." Yet 30% admitted they had no policy for ensuring the security of equipment, including hard drives, sold to others. (S. Hildreth, Where hard drives go to die, or do they?, *Searchsecurity.techtarget.com*, May 4, 2006)

A new report by World Privacy Forum has found more than 19,000 complaints of medical ID theft on file with the federal government. (D. Harris, Medical ID theft can wreck victims' health and finances, *ABC News*, May 3, 2006)
An annual survey conducted by the American Health Information Management Association reports fewer health plans and providers consider themselves to be "mostly compliant" with the Health Insurance Portability and Accountabilty Act's privacy regulations than a year before. Although 91 percent said in 2005 that they were mostly compliant, that number dropped to 85 percent this year. HIPAA gives patients a right to know who has seen their records other than the people involved in their treatment, payment or health care operations. More than half of the respondents cited some difficulties in complying with this provision. (N. Ferris, Privacy compliance has declined, FCW.com, April 24, 2006)

A Palm Desert medical marijuana dispensary is being required to turn clients' names over to authorities, and client advocates say that violates their privacy rights. Palm Desert city attorney David Erwin said the deal between the city and the CannaHelp dispensary on El Paseo, is merely meant to ensure that the dispensary is obeying state law. Lanny Swerdlow of Palm Springs, head of the Marijuana Anti-Prohibition Project, a patient support group, believes the data sharing to be a violation of the federal Health Insurance Portability and Accountability Act which ensures the confidentiality of patients' medical records. (K. Kaufmann, Dispensary must turn over names, *The Desert Sun*, April 22, 2006)

The Georgia Division of Public Health has shut down a clinic in Carrollton which provided care to about 75 people living with HIV due to "[c]lient confidentiality required for the privacy of clinical services was not being observed," according to a statement by health officials. (Z. Hudson, Carrollton HIV clinic shut down, *Southern Voice*, April 21, 2006)

Hawaii officials have revealed that more than 43,000 people, nearly half of them government employees, are at risk of identity theft when unauthorized copies of insurance company records listing the names and Social Security numbers of people enrolled in certain health and group life insurance plans were made in 1999. Federal officials in January informed the state that unauthorized copies of some of the records were made, apparently while they were at the copying service. Copies of the records later were found by police on a computer used by a person under investigation for drug offenses, the state officials said. (Hawaii says stolen records could lead to thousands of ID thefts, *Associated Press*, April 14, 2006)

A local Michigan news team discovered patient records in dumpsters outside of physicians' offices and other medical facilities. The news team found personal information in one half of the 20 dumpsters they surveyed. The information included patients' names, social security numbers, work addresses, and treatment information; for one patient, information about a hysterectomy and history of depression was included. (WZZM13, Grand Rapids Michigan, November 9, 2005)

The Ohio State University Medical Center in Columbus, OH mistakenly posted online the personal health information—including names, addresses, social security numbers, and treatment information—of approximately 2,800 patients. ("Patients' Personal Health Information Mistakenly Posted Online," *Associated Press,* November 4, 2005)

Information about 5,000 patients—including birth dates, Social Security numbers, and diagnostic and financial information—was stolen from the Children's Health Council, a treatment center in Palo Alto California that treats emotionally troubled and developmentally challenged children. (Ihealthbeat.org, "Medical Records Stolen From California Children's Clinic," 9/21/05 and Webby, San Jose Mercury News, September 20, 2005)

Sensitive information about 57,000 Blue Cross Blue Shield of Arizona patients—including addresses, phone numbers, Social Security numbers, birth dates, and treatment histories—was stolen from Arizona Biodyne, a Phoenix-based managed care company that coordinates behavioral health for Blue Cross of Arizona. (Matt Hanson, "Medical Firm's Files with Personal Data Stolen," The Arizona Republic, July 13, 2005)

Seventeen hospital workers (including doctors, supervisors, and lab technicians) tried to access the record of former President Bill Clinton as he was undergoing heart surgery at New York's Columbia Presbyterian Hospital. ("Hack Attack, How Safe is Your Computer," *Physician's Practice*, June, 2005)

Kaiser Permanente Northern California left the names, addresses, phone numbers and lab results of approximately 150 patients posted on a publicly accessible website for up to four years.   In violation of both state law and Kaiser's policy, the site was developed without patient consent. It was not until a disgruntled employee linked the website to her online blog that the breach became public. Still, Kaiser did not remove the site until federal civil-rights authorities learned about it in January. Further, Kaiser did not inform state regulators or patients about the breach until March—when it was reported in the media. The state Department of Managed Health Care levied the largest fine for a privacy violation to Kaiser in the amount of $200,000. ("Privacy Breach Costs Kaiser," *San Jose Mercury News*, June 21,2005)

The University of Pittsburgh Medical Center was using an insecure online form to collect patient information, including name, Social Security number, and prescription information. After the form was brought to UPMC's attention, they removed it from their site. More than 100 patients were believed to have used the form. (Christopher Snowbeck, "UPMC Pulls Online Drug Form," Pittsburgh Post-Gazette, May 27, 2005)

About 16,000 patients were notified by Christus St. Joseph Hospital of Houston, TX that a computer was stolen that contained files including their names, social security numbers, and health information. The computer was taken from Gateway File Systems, Inc., which was in the process of converting paper-based medical records to electronic records for St. Joseph. (ROBERT CROWE, “Patients warned that stolen data could be theirs; Letters are sent to 16,000 whose records were on computers taken from St. Joseph,” *The Houston Chronicle*, April 26, 2005*)*

The Northwestern Memorial Physicians Group belatedly notified patients of a local health clinic that their blood and stool samples had been stolen weeks previously, along with their Social Security numbers, names, and other identifying information. (Jeremy Manier and Carlos Sadovi “Clinic red-faced about blood theft; Patients angered by delay in reporting theft of specimens,” *Chicago Tribune*, April 22, 2005)

Two computers that contained the names, addresses, Social Security numbers, and medical information of 185,000 people were stolen from the San Jose Medical Group in California. (Glennda Chui, “Medical Data Thefts Spur Worry,” San Jose Mercury News, April 12, 2005)

A Palm Beach County Health Department statistician and epidemiologist mistakenly attached a list containing more than 6,000 names of HIV/AIDS patients to an e-mail sent out to 800 of the department's 900 employees (Mary McLachlin, “HIV E-mail Leads to Changes,” *Palm Beach Post,* February 23, 2005).

A Nassau County (NY) District Attorney’s office uncovered an insurance scam in which hospital employees were paid to disclose the medical information of Hispanic emergency room patients who were involved in automobile accidents. (Office of the District Attorney, Press Release: Numerous Arrests in Connection to Sale of Confidential Patient Information, November 23, 2004)

A New York City emergency medical technician was suspended after sharing a patient’s medical record with friends as a joke. The FDNY medical technician found the patient’s medical circumstance funny, and stole the medical record from the ambulance, scanned it, and e-mailed it to friends and colleagues. In addition to medical information, the record contained the patient’s name, address, and Social Security number. (F. Santos, Joke bad ca-rear move for city EMT, *New York Daily News*, October 29, 2004.)

In the first criminal conviction under the HIPAA Privacy Rule, a Washington state man was convicted of wrongfully accessing a patient’s protected health information. Richard Gibson, an employee at a Seattle provider of cancer treatment, admitted that he obtained a cancer patient's name, date of birth and Social Security number. Mr. Gibson admitted to using the information to get four credit cards in the patient's name. (“First Criminal Guilty Plea Offered,” www.thompson.com, August 20, 2004)

Sally Scofield’s medical records, including her name, address, and details of her recent operation, were released to a marketing company in the spring of 2002. She received a phone call from the company asking her about her experience with knee surgery. Once she realized that anything she told her doctor could be disclosed to marketing companies without her consent, Ms. Scofield decided to stop going to the doctor. (T. Francis, “Trial will test privacy rules for health files,” *The Wall Street Journal*, December 10, 2003, p. B1).

Medical records from the University of California – San Francisco Medical Center that had been sent to Pakistan for transcription were nearly made public when a Pakistani transcriber threatened to post them on the Internet. Although the transcriber ultimately agreed not to post the records, UCSF could not confirm that she had destroyed them. The American Association for Medical Transcription, an industry group, estimates that about 10 percent of U.S. medical transcription is done abroad, where U.S. privacy laws are virtually unenforceable (D. Lazurus, “A Tough Lesson on Medical Privacy: Pakistani Transcriber Threatens UCSF over Back Pay,” *San Francisco Chronicle*, October 22, 2003, p. A1).

Following the rape accusations against basketball player Kobe Bryant, the alleged victim's medical records were subpoenaed by Bryant's defense lawyers from a Colorado hospital. After a hospital employee released the asked that the judge throw out the subpoenas and destroy the records already received by him, citing state and federal medical privacy laws. Attorneys for the victim also attempted to prevent Bryant's defense team from gaining access to her medical records from two other hospitals. However, a number of news stories have published sensitive medical information that reporters allege came from hospital employees. (M. Miller, "Issues of Privacy in Bryant Case," Los Angeles Times, September 8, 2003)

Software developed by Hospice Systems, Inc., the for-profit subsidiary of Hospice of the Florida Suncoast, disclosed the medical records of patients treated at the Hospice. The software, which contains patient names, address, social security numbers and diagnoses, is currently used by approximately 100 hospices. Patients whose privacy was allegedly violated filed a lawsuit in Pinellas-Pasco circuit court in May 2003. ("Lawsuit alleges that hospice released private information," *St. Petersburg Times*, May 2, 2003)

Individuals Exposed

The California state Department of Health Services inadvertently revealed the names and addresses of up to 53 people living with enrolled in an AIDS drug assistance program to other enrollees by putting benefit notification letters in the wrong envelopes, officials said Friday. The department learned about the mix-up after 12 people in the drug assistance program phoned to say they had received letters addressed to someone else. The department on Friday mailed certified letters to the 54 enrollees, explaining the mix-up and asking that anyone who received a wrongly addressed letter destroy it. It also notified the California Highway Patrol, as is required by a state law on security breaches. The department is looking into ways to make the system more foolproof, such as using envelopes with window addresses, said health services Director Sandra Shewry. HIV/AIDS services and advocacy groups said this was the first known breach of that database. "I would hope this is an anomaly," said Jeff Bailey, director of client services for AIDS Project Los Angeles. (Engel, M., Mix-up breaches confidentiality of dozens in state AIDS program, *Los Angeles Times*, March 3, 2007)

Richard Yaw Adjei of Bear, Delaware pleaded guilty in federal court on November 16 to aggravated identity theft and three counts of fraud for his part in a widespread criminal scheme that used information from a hospital billing service to steal the identities of more than 400 people. U.S. Attorney Colm F. Connolly also announced the indictment of accomplice Linda Danyell Williams, a claims processor at a New Castle medical billing and collection firm, alleged to have sold Adjei information about more than 400 patients for an undisclosed sum. Adjei in turn set up a tax return business and used the stolen information, including names, birth dates, addresses, Social Security numbers, hospital admission dates, doctors' names, and diagnosis codes, to submit bogus tax returns and receive refunds totalling more than $300,000 in the names of at least 163 of the victims. (O'Sullivan, S., ID theft scam used medical billing info, *Delaware News Journal*, November 18, 2006)

The personal health information of more than 200 people was discovered by KPRC Local 2 TV investigators in unlocked garbage Dumpsters outside Houston area Walgreens, CVS and other pharmacies. Investigators found prescription labels, pill bottles and computer printouts disclosing detailed personal medical information. The Texas State Board of Pharmacy is expected to take immediate action. (Pharmacies dump medical information in trash, *KPRC Local 2 (Houston)*, November 15, 2006)

A primary care clinic in Sorora, California released the Social Security numbers of 22 veterans to at least two patients signing in for appointments. Charles Kavanaugh was second in line for a blood test when he was given the list by a desk attendant. Officials of the Sonora Regional Medical Center, who operate the clinic, believe it was an isolated event. (Wyman, A., Blood lab slips up, releases SS info, *Union Democrat (Sonora, CA),* September 14, 2006)

A federal grand jury in Miami indicted Isis Machado, a former employee of the Cleveland Clinic and Health Management Associates and her cousin Fernando Ferrer Jr., who owned Advanced Medical Claims of Naples, with identity theft, computer and healthcare fraud, and violating the Health Insurance Portability and Accountability Act. Machado served as front desk coordinator at the clinic, had access to confidential patient information, and sold the information to Ferrer, who allegedly submitted fraudulent Medicare claims. A Cleveland Clinic spokesperson said the identities of 1,100 patients could be at further risk. Machado and Ferrer each face 30 years in prison and $750,000 in fines if convicted. (Taylor, M., "Former Cleveland Clinic worker, kin charged with fraud, HIPAA violation," *HIT Strategist*, September 11, 2006)

The Government Accountability Office issued a report calling for Medicare to exercise more oversight over how private plans transmit personal health records. Nearly half of all Medicare Advantage contractors surveyed reported breaches of private health records during the last two years. Information breaches most often occur when private contractors outsource health records to other companies for additional processing. According to GAO, 90 percent of Medicare contractors reported outsourcing health records domestically in 2005. (Perrone, M., "GAO urges more Medicare plan oversight," *Houston Chronicle*, September 5, 2006)

An Indiana-based consultant was able to download the names, Social Security numbers and dates of birth for between 5,600 and 23,000 Georgetown University Hospital patients when he accidentally discovered the unsecured data on the website of e-prescribing vendor InstantDx. The consultant reports he accessed the data using a password he discovered hard-coded into Medisoft, a popular medical practice application. InstantDx was quick to accept responsibility for the breach. (Poulson, K., "E-health gaffe exposes hospital," *Wired Magazine*, July 25, 2006)

Two Ohio University graduate students have filed lawsuits against the university due to recent data thefts from school computers. The plaintiffs are two of possibly 173,000 students, employees, or faculty whose Social Security numbers, names, addresses, medical records, and home addresses were stolen in five separate instances since March 2005. On the same day the suit was filed, the university announced its decision to spend $4 million to heighten computer security on campus, and last week it suspended its director of computer and network services pending an investigation. (Two students sue university, *ChannelCincinnati.com,* June 27, 2006)

A woman reports she secretly removed pages from her medical record showing she was at risk of Huntington's disease, a fatal genetic disorder. Fearing the consequences of the disclosure of the information, She said she removed information from her file to protect the ability of her children to obtain health insurance. (R. Klitzman, The quest for privacy can make us thieves, *New York Times*, May 9, 2006)

A Washington state law requiring customers to sign a log book when purchasing over the counter products containing pseudoephedrine could compromise medical privacy, according to the American Civil Liberties Union, who fear that regular users of such products "may come under suspicion for what's actually an innocent act." (E. Porter, Meth clampdown should compromise medical privacy, *Kiro 7 Eyewitness News (Seattle)*, May 9, 2006)

Hawaii officials have revealed that more than 43,000 people, nearly half of them government employees, are at risk of identity theft when unauthorized copies of insurance company records listing the names and Social Security numbers of people enrolled in certain health and group life insurance plans were made in 1999. Federal officials in January informed the state that unauthorized copies of some of the records were made, apparently while they were at the copying service. Copies of the records later were found by police on a computer used by a person under investigation for drug offenses, the state officials said. (Hawaii says stolen records could lead to thousands of ID thefts, *Associated Press*, April 14, 2006)

The Ohio State University Medical Center in Columbus, OH mistakenly posted online the personal health information—including names, addresses, social security numbers, and treatment information—of approximately 2,800 patients. (“Patients’ Personal Health Information Mistakenly Posted Online,” *Associated Press,* November 4, 2005)

Seventeen hospital workers (including doctors, supervisors, and lab technicians) tried to access the record of former President Bill Clinton as he was undergoing heart surgery at New York's Columbia Presbyterian Hospital. ("Hack Attack, How Safe is Your Computer," *Physician's Practice*, June, 2005)

A New York City emergency medical technician was suspended after sharing a patient's medical record with friends as a joke. The FDNY medical technician found the patient's medical circumstance funny, and stole the medical record from the ambulance, scanned it, and e-mailed it to friends and colleagues. In addition to medical information, the record contained the patient's name, address, and Social Security number. (F. Santos, Joke bad ca-rear move for city EMT, *New York Daily News*, October 29, 2004.)

Sally Scofield's medical records, including her name, address, and details of her recent operation, were released to a marketing company in the spring of 2002. She received a phone call from the company asking her about her experience with knee surgery. Once she realized that anything she told her doctor could be disclosed to marketing companies without her consent, Ms. Scofield decided to stop going to the doctor. (T. Francis, "Trial will test privacy rules for health files," *The Wall Street Journal*, December 10, 2003, p. B1).

Following the rape accusations against basketball player Kobe Bryant, the alleged victim's medical records were subpoenaed by Bryant's defense lawyers from a Colorado hospital. After a hospital employee released the asked that the judge throw out the subpoenas and destroy the records already received by him, citing state and federal medical privacy laws. Attorneys for the victim also attempted to prevent Bryant's defense team from gaining access to her medical records from two other hospitals. However, a number of news stories have published sensitive medical information that reporters allege came from hospital employees. (M. Miller, "Issues of Privacy in Bryant Case," Los Angeles Times, September 8, 2003)

Software developed by Hospice Systems, Inc., the for-profit subsidiary of Hospice of the Florida Suncoast, disclosed the medical records of patients treated at the Hospice. The software, which contains patient names, address, social security numbers and diagnoses, is currently used by approximately 100 hospices. Patients whose privacy was allegedly violated filed a lawsuit in Pinellas-Pasco circuit court in May 2003. ("Lawsuit alleges that hospice released private information," St. Petersburg Times, May 2, 2003)

The medical records of an Illinois woman were posted on the Internet without her knowledge or consent after she was treated at St. Elizabeth's Medical Center following complications from an abortion performed at the Hope Clinic for Women. The woman has sued the hospital, alleging that St. Elizabeth's released her medical records without her authorization to anti-abortion activists, who then posted the records online along with a photograph they had taken of her being transferred from the clinic to the hospital. The woman is also suing the anti-abortion activists for invading her privacy. (T. Hillig and J. Mannies, "Woman Sues Over Posting of Abortion Details," *St. Louis Post-Dispatch*, July 3, 2001, p. A1)

Terri Seargent, a North Carolina resident, was fired from her job after being diagnosed with a genetic disorder that required expensive treatment. Three weeks before being fired, Terri was given a positive review and a raise. As such, she suspected that her employer, who is self-insured, found out about her condition, and fired her to avoid the projected expenses. (R. Weiss, "Ignorance Undercuts Gene Tests' Potential," *The Washington Post*, December 2, 2000, p. A1)

Country singer Tammy Wynette's medical records were sold to the National Enquirer and Star tabloids by a hospital employee for $2,610. William Cox retrieved medical information about Wynette from the hospital's databases and faxed it to the tabloids without her consent. Cox pleaded guilty to one count of wire fraud and was sentenced to six months in prison. ("Selling Singer's Files Gets Man Six Months," *Houston Chronicle*, December 2, 2000, p. A2)

The medical records of a Maryland school board member were sent to school officials as part of a campaign criticizing his performance. The records revealed that the member had been treated for depression. (C. Samuels, “Allen Makes Diagnosis of Depression Public; Medical Records Mailed Anonymously,” *The Washington Post*, August 26, 2000, p. V1)

A patient at Brigham and Women’s Hospital in Boston learned that employees had accessed her medical record more than 200 times. (R. Mishra, “Confidential Medical Records Are Not Always Private,” *The Boston Globe*, August 1, 2000, p. D1)

A South Carolina resident was suspended from work for refusing to release her medical records to her employer. (S. Crowley, “Invading Your Medical Privacy,” *AARP Bulletin*, March 2000)

An Atlanta truck driver lost his job in early 1998 after his employer learned from his insurance company that he had sought treatment for a drinking problem. (J. Appleby, “File safe? Health Records May Not Be Confidential,” *USA Today*, March 23, 2000, p. A1)

After suffering a work-related injury to her wrist, Roni Breite authorized her insurance company to release information pertaining to her wrist ailment to her employer. The file that the company released contained her *entire* medical history, including records on recent fertility treatment and pregnancy loss. (E. McCarthy, “Patients Voice Growing Concerns about Privacy,” *Sacramento Business Journal*, April 5, 1999)

Joan Kelly was automatically enrolled in a “depression program” by her employer, Motorola, after her prescription drug management company reported that she was taking anti-depressants. (R. O’Harrow, “Plans’ Access to Pharmacy Data Raises Privacy Issue,” *The Washington Post*, September 27, 1998, p. A1)

New York Congresswoman Nydia Velasquez’s confidential medical records – including details of a bout with depression and a suicide attempt – were faxed from a New York hospital to a local newspaper and television station on the eve of her 1992 primary. After overcoming the fallout from this disclosure and winning the election, Rep. Velasquez testified eloquently about her experiences before the Senate Judiciary Committee as it was considering a health privacy proposal. (A. Rubin, “Records No Longer for Doctors’ Eye Only,” *Los Angeles Times*, September 1, 1998, p. A1)

Just months before tennis star Arthur Ashe died of complications of AIDS, he was coerced into disclosing his HIV status in 1992 when he learned the newspaper USA Today was about to publish a story about his condition.

Unauthorized Access

New York City's public hospital system will suspend 39 employees without pay for peeking at the private medical records of Nixzmary Brown. The case of the 7-year-old girl, who died in Brooklyn in January from beatings and torture, become a tabloid and TV news sensation, and dozens of workers at the Woodfull Medical and Mental Health Center apparently couldn't resist looking at the child's computerized medical file. The suspensions will last from 30 to 60 days, and each of the sanctioned employees will be required to undergo training in patient privacy rules before they return to work. (Caruso, D., Prying N.Y. hospital workers suspended, *Washington Post*, September 25, 2006)

A former Randolph County, NC nurse who stole the identity of 12 patients and ran up credit card bills in their names was sentenced to a prison term of almost three years. Having obtained patient names and Social Security numbers, Susan Pugh White used the information to create fake documents in order to obtain credit cards in the patients' names. Law enforcement discovered personal information on another dozen patients in White's possession. (E. Collins, "Nurse sentenced for identity theft," *News-Record.com,* June 16, 2006)

The names, birth dates, Social Security numbers and medical information for 60,000 students, faculty and staff at Ohio University were stolen in the third electronic security breach in three weeks. The university learned on May 4 that an unauthorized person gained access into a computer server that supports the Hudson Health Center. (J. Gonzalez, Third computer breach at Ohio University; Records involve 60,000 who used health center, *Plain Dealer (Cleveland)*, May 12, 2006)

A new report by World Privacy Forum has found more than 19,000 complaints of medical ID theft on file with the federal government. (D. Harris, Medical ID theft can wreck victims' health and finances, *ABC News*, May 3, 2006)

A Nassau County (NY) District Attorney's office uncovered an insurance scam in which hospital employees were paid to disclose the medical information of Hispanic emergency room patients who were involved in automobile accidents. (Office of the District Attorney, Press Release: Numerous Arrests in Connection to Sale of Confidential Patient Information, November 23, 2004)

In the first criminal conviction under the HIPAA Privacy Rule, a Washington state man was convicted of wrongfully accessing a patient's protected health information. Richard Gibson, an employee at a Seattle provider of cancer treatment, admitted that he obtained a cancer patient's name, date of birth and Social Security number. Mr. Gibson admitted to using the information to get four credit cards in the patient's name. ("First Criminal Guilty Plea Offered," www.thompson.com, August 20, 2004.)

A New York City emergency medical technician was suspended after sharing a patient's medical record with friends as a joke. The FDNY medical technician found the patient's medical circumstance funny, and stole the medical record from the ambulance, scanned it, and e-mailed it to friends and colleagues. In addition to medical information, the record contained the patient's name, address, and Social Security number. (Fernanda Santos, "Joke Bad Ca-Rear Move for City EMT," New York Daily News, October 29, 2004.)

Medical records from the University of California – San Francisco Medical Center that had been sent to Pakistan for transcription were nearly made public when a Pakistani transcriber threatened to post them on the Internet. Although the transcriber ultimately agreed not to post the records, UCSF could not confirm that she had destroyed them. The American Association for Medical Transcription, an industry group, estimates that about 10 percent of U.S. medical transcription is done abroad, where U.S. privacy laws are virtually unenforceable (D. Lazurus, "A Tough Lesson on Medical Privacy: Pakistani Transcriber Threatens UCSF over Back Pay," San Francisco Chronicle, October 22, 2003, p. A1).

A hospital clerk at Jackson Memorial Hospital in Miami, Florida stole the social security numbers of sixteen patients named Theresa when they registered at the hospital. The hospital clerk then provided the social security numbers and medical record information to a friend, also named Theresa, who opened up over 200 bank and credit card accounts and buy six new cars. (D. Sherman, "Stealing From The Sick," NBC6.net, May 21, 2002)

A temporary employee of the Dana-Farber Cancer Institute stole patients' personal information. The employee allegedly used one patient's name and data to obtain $2,500 in long distance and other phone service. (J. Ellement, "Dana-Farber Says Patient Data Stolen," *The Boston Globe*, August 8, 2000, p. A1)

A state health department employee compiled a list of 4,000 Pinellas County, Florida individuals diagnosed with HIV and then offered the information to friends to to screen potential dates. (C. Pittman, Ruling propels AIDS-list case toward trial, *St. Petersburg Times*, July 31, 1997)

In Tampa, a public health worker walked away with a computer disk containing the names of 4,000 people who tested positive for HIV. The disk was sent to two newspapers. (J. Bacon, "AIDS Confidentiality," *USA Today*, October 10, 1996, p. A1)

The Harvard Community Health Plan, a Boston-based HMO, admitted to maintaining detailed notes of psychotherapy sessions in computer records that were available to all clinical employees. Following a series of press reports describing the system, the HMO revamped its computer security practices. (A. Bass, “HMO Puts Confidential Records On-Line; Critics Say Computer File-Keeping Breaches Privacy of Mental Health Patients,” *The Boston Globe*, March 7, 1995, p. 1)

The 13-year-old daughter of a hospital employee took a list of patients’ names and phone numbers from the hospital when visiting her mother at work. As a joke, she contacted patients and told them that they had been diagnosed with HIV. (“Hospital Clerk’s Child Allegedly Told Patients That They Had AIDS,” *The Washington Post*, March 1, 1995, p. A17)

A banker who also served on his county’s health board cross-referenced customer accounts with patient information. He then called due the mortgages of anyone suffering from cancer. (M. Lavelle, “Health Plan Debate Turning to Privacy: Some Call For Safeguards on Medical Disclosure. Is a Federal Law Necessary?” *The National Law Journal*, May 30, 1994, p. A1)

Poor Security

Kaiser Permanente announced this week that a laptop computer containing names, membership identification numbers, dates of birth, gender, and physician information on 38,000 Kaiser Permanente members was stolen in the Denver area in early October from a car belonging to a Kaiser Permanente employee in California. (Laptop with patient info stolen, *Rocky Mountain News*, November 29, 2006)

Two computers containing health records on participants in Indiana's Breast and Cervical Cancer Program were stolen from a Jeffersonville health clinic, leaving more than 7,500 Indiana women at risk of identity theft, according to the Indiana Department of Health. Data stored on the computers may include names, addresses, Social Security numbers, medical information or other data. (Women alerted to possible identity theft, Associated Press, November 27, 2006)

The Department of Veterans Administration confirmed on November 2 that a computer containing the personal data of former military servicemen and women was stolen from the agency's Manhattan hospital. VA spokeswoman Jo Schuda said the laptop computer, used to measure pulmonary function, was stolen from a locked room in a locked hallway at the VA hospital on East 23rd Street. The theft took place September 6, but VA officials sent out a letter to the 1,600 affected veterans only within the past two weeks. Their personal data was on the computer's hard drive. (Raymon, G., Data on veterans missing, *Newsday*, November 3, 2006)

The Sisters of St. Francis Health Services Inc. began contacting customers on October 9 regarding a July 28 incident with a contracted employee that representatives say left sensitive data of at least 260,000 Indiana and Illinois residents "out of hospital hands" for several days. An employee of Perot Systems, a company contracted to perform medical billing, copied the data onto several CDs to work on it from home. The contracted employee left the CDs in a store inside a bag she returned there. The CDs were recovered when another customer noticed them. Lisa Decker, director of public relations for Greater Lafayette Health Services clients, a subsidiary of the Sisters, said the companies are examining procedures and best practices involving patient information in hopes of preventing future mistakes. She said it was unclear as yet whether a single employee would have the freedom to transport such a volume of data in the future. (Brown, T., 260,000 told of data breach, *Journalandcourier.com* (Lafayette, IN), October 24, 2006)

A laptop computer containing the names and Social Security numbers of about 14,000 of Allina Hospitals and Clinics obstetrics patients was stolen from a nurse's car on October 8. Although two passwords are needed to access the information on the laptop, Allina acknowledged the potential for identity theft, according to a letter sent patients this week. The nurse whose computer was stolen said she had left the laptop in her car when she went in to a Minneapolis lab to drop off a specimen. The nurse believes she locked the vehicle, he added.In the future, Kanihan said, the laptops no longer will contain Social Security numbers. (Lonetree, A., Stolen laptop held personal data of thousands of Allina patients, Minneapolis-St. Paul Star Tribune, October 20, 2006)

Security weaknesses have left millions of elderly, disabled and poor Americans vulnerable to unauthorized disclosure of their medical and personal records, federal investigators said Tuesday. The Government Accountability Office said it discovered 47 weaknesses in the computer system used by the Centers for Medicare and Medicaid Services to send and receive bills and to communicate with health care providers. The agency oversees health care programs that benefit one in every four Americans. Its massive amount of data is transmitted through a computer network that is privately owned and operated. However, CMS did not always ensure that its contractor followed the agency's security policies and standards, according to the GAO report. "As a result, sensitive, personally identifiable medical data traversing this network are vulnerable to unauthorized disclosure," the federal investigators said. The network handling Medicare claims transmits extremely personal information, such as a patient's diagnosis, the types of drugs the patient takes, plus the type of treatment facility they visited, including treatment centers for substance abuse or mental illness. (Freking, K., Auditors: health records at risk, *Associated Press*, October 3, 2006)

The husband of a federal prosecutor in Seattle was one of 42 people whose personal information was stolen by a sophisticated identity-theft ring that stole patient data from Virginia Mason Medical Center between May 2005 and September 17. Susan Harrison discovered she and her husband were the victims of identity theft after thousands of dollars suddenly disappeared from their checking account in December. Two former medical center employees allegedly used fake ID badges to enter Virginia Mason facilities at night and lift data from the files of patients who had appointments the next day. (Bowermaster, D., Identity theft: it could happen to anyone, *Seattle Times*, September 28,2006)

Providence Health Systems agreed to reimburse the state of Oregon more than $95,000 in costs as part of a deal to settle a nine-month invetigation into the largest data breach ever reported in Oregon. Medical records of 365,000 patients, stored on computer disks and digital tape, were in a car stolen from a Providence home services employee. The data was not encrypted. The theft revived efforts to enact stronger privacy protections in Oregon and spurred some patients to back a class-action lawsuit seeking damages from Providence. (Rojas-Burke, J., Providence settles data breach, *The Oregonian*, September 27, 2006)

A retired school teacher -- with two feet -- was stunned when hospital bill collectors demanded she pay for the amputation of her right foot. The victim of medical identity theft, Lind Weaver says trying to catch errors in her medical records and clear up hospital bills fraudulently run up in her name has "become a 40-hour-a-week job." Meanwhile, Anndorie Sachs received a call from a Utah state social worker that her hospitalized infant had tested positive for methampehtamine, yet Sachs hadn't delivered a baby in two years. A woman had used Sachs' stolen drivers license to check into the hospital to give birth. Weaver and Sachs join at least 200,000 Americans who have become victims of medical identify theft, according to a 2003 federal report. (Menn, J., ID theft infects medical records, *Los Angeles Times*, September 25, 2006)

A Washington state mental health care provider, Compass Health, has notified authorities that a laptop computer containing data on an undisclosed number of patients was stolen more than a month ago. According to a media alert issued by Compass Health, the laptop contained information on clients of the clinic and its partners since October 1st, 2005. The information included Social Security numbers, "along with other clinical and demographic information." The theft occurred June 28. Compass did not say why it waited so long to issue the alert. (Bosworth, M., "Mental health clinic loses laptop bearing patient data," *ConsumerAffairs.com*, August 30, 2006)

Pediatric Services of America, Norcross, Ga., doing business as PSA HealthCare, has announced it will sell a business unit but has no new information about a stolen laptop computer with the personal information of 51,000 patients. The laptop contained the personal information of current and former patients, including their names, Social

Security numbers and, "in a limited number of cases, personal healthcare information," according to a company news release. (Conn, J., "Stolen laptop delays company's financial forecast," *Modern Healthcare*, August 29, 2006)

The homecare division of William Beaumont Hospital, Royal Oak, Mich., asked the public to help it recover a laptop filled with three years of personal information on home-health patients, including names, Social Security numbers, medical data and insurance information. The laptop was stolen with an employee's car. The system said the information was encrypted and password-protected, but the laptop belonged to a new employee who had stored the ID access code and password with the computer. ("Mich. system says stolen laptop holds patient data," *Crain's Detroit Business*, August 23, 2006)

HCA, the Nashville-based group of hospitals, late last week said burglars broke into a regional office and stole ten computers containing names and Social Security numbers for thousands of patients treated at its facilities from 1996 until this year. The computers contain 15,000 to 18,000 files with information on Medicare and Medicaid patients who have uncollected copayments and deductibles. (Galloro, V., "10 PCs stolen at HCA office," *HIT Strategist*, August 14, 2006)

Madrona Medical Group, a is asking its patients to watch their credit reports after a former employee was charged with illegally downloading 6,000 patient files onto his personal laptop computer. (Gallagher, M., "Madrona patients may face ID theft," *The Bellingham Herald*, August 11, 2006)

A desktop computer containing personal information for up to 38,000 patients treated at Veterans Affairs Department medical centers in Pittsburgh and Philadelphia over the past four years was reported missing from the Reston, VA offices of VA contractor Unisys Corp. The VA and Unisys says the computer contained names, addresses, Social Security numbers and dates of birth. It may also have included insurance carrier and billing information, claims data and medical information. (Robeznieks, A., "Another computer with VA data goes missing," *HIT Strategist*, August 8, 2006)

The personal information of about 160,000 Northern California Kaiser Permanente members who receive hearing aid services was stolen with a computer from a secure office in Oakland. The information stolen included names, addresses, phone numbers, ages or dates of birth, appointment type and dates of service. (Raskin-Zrihen, R., "Patient data stolen from Kaiser," *Vallejo Times Herald,* August 7, 2006)

A laptop containing personal information about 257,800 patients of Poughkeepsie's Vassar Brothers Medical Center was stolen in late June, but some patients did not receive a letter of notification of breach until this week. The information in the laptop covers about 20 years of patient activity. ("Patient information stolen from N.Y. medical center," *Associated Press*, August 4, 2006)

A state government computer was stolen during a July Fourth break-in at the offices of a drug dependency program, and officials were trying to determine Friday whether it contained sensitive information. Many top officials in state government were unaware Friday morning that a Public Health and Human Services computer had been stolen from a state office building on Tuesday. The agency later said it took a few days for the information to filter to top officials. ("*Computer taken from Montana office*," Bismarck Tribune, July 8, 2006

Three laptops, one of them containing personal information on thousands of blood donors -- including Social Security numbers and medical histories -- were stolen from a locked closet in the Farmers Branch office of the American Red Cross during two separate incidents in May. Donors were not notified of the theft. Red Cross officials say they aren't overly concerned because the information was encrypted. The computers were recovered by officials on June 28, who report it appears that personal information had not been compromised. (Schreier, L., "Donor data stolen at local Red Cross," *Dallas Morning News*, July 1, 2006)

A backup tape containing the dates of birth, medical records and Social Security numbers of more than 16,000 held by the Department of Veterans Affairs Regional Counsel Office in Indianapolis. The VA might offer credit monitoring for anyone who could have been impacted by the security breach. The incident occurred two days after a laptop containing the personal information of more than 26 million veterans was reported stolen in Maryland. ("Veterans records tape missing from Indy office," *TheIndyChannel.com*, June 29, 2006)

A laptop containing personal information about 24,000 Cumberland County, N.C. emergency medical patients cannot be located by its owner, the local health department. Local police are investigating whether the computer was stolen, and the health department is reviewing its policies and procedures. ("Fayetteville police look for laptop containing patients' info," *wral.com*, June 21, 2006)

The University of Alabama in Birmingham earlier this month reported a laptop computer containing confidential information about 9,800 kidney donors, organ recipients, and potential recipients was stolen in February from its kidney transplant program offices. UAB said it took months for officials to reconstruct the information stolen in order to contact those affected. ("Data on 9,800 people missing after theft of computer," *Associated Press*, June 21, 2006)

One of the world's largest insurers, American International Group, said yesterday a burglar stole computer equipment in March from one of its Midwest offices that contained personal information about 930,000 people. A company spokesperson said the data consisted of names, Social Security numbers and "fragments of medical information." The information was provided to AIG by insurance brokers seeking quotes for coverage on high levels of health insurance for employees of companies around the country. AIG declined to name these companies. (J. Treaster, "Insurer reports theft of data on 930,000," *New York Times*, June 15, 2006)

The Veterans Affairs Department announced it has been investigating allegations that an offshore medical transcription subcontractor threatened to expose 30,000 veterans' electronic health records on the Internet in a payment dispute with a VA contractor. According to testimony of VA's assistant inspector general for auditing, Michael Staley, at a House Veterans Affairs Committee hearing, "Contracts do not specify criteria for how to protect information." Staley also reported that a 2005 audit of information management security found instances where out-based employees send veterans' medical information to the VA regional office through unencrypted email, monitoring remote network access and usage does not routinely occur, and off-duty users' access to VA computer systems and sensitive informaton is not restricted. (M. Mosquera, "Rep. Buyer: Department CIO needs IT security enforcement authority," *Government Computer News*, June 14, 2006)

Federal Centers for Medicare and Medicaid Administrator Mark McClellan reported that 17,000 beneficiaries covered by Humana, Inc. health care plans are at risk from unsecured computer data containing their personal information. McClellan says Humana's lapse violates Medicare's privacy and information security policies. The news follows reports of the theft of about 250 Humana plan applications last month in Minnesota. (U.S. Medicare official says Humana data not secured," *Reuters*, June 5, 2006)

A computer file containing the data of 17,000 Medicare beneficiaries enrolled in Humana health care plans is not secure, according to a finding by the HHS inspector general. Applications with personal data for 250 people applying for Humana plans were stolen last month from an insurance agent's car. ("Humana computer data not secure," *Reuters*, June 5, 2006)

Laptop computers with personal information on 72,000 Ohio low-income, disabled, and elderly Medicaid recipients stored on four computers were stolen from a private managed-care agency. Although the computers themselves were password protected, the files themselves were not. Data on the files included names, Social Security numbers, and addresses. ("Laptops stolen with Medicaid, Buckeye health member data," *The Toledo Blade*, June 3, 2006)

The Medicare prescription drug benefit applications for 268 people from North Dakota and Minnesota were stolen in a Minnesota car burglary. The applications for coverage by Humana's health insurance company included applicants' names, addresses, Social Security numbers, and bank routing information and were left in a briefcase in the car. North Dakota Insurance Commissioner Jim Poolman said he did not believe the company was being forthcoming about the extent of the data loss. He suspects customer information was also stored on a stolen computer inside the case. (Wetzel, D., "Medicare data at risk of theft of forms," *St. Paul Pioneer Press*, June 2, 2006)

The names, birth dates, Social Security numbers, and, in some cases, disability ratings of as many as 26.5 million veterans were stolen recently from the home of a Department of Veterans Affairs employee on May 3rd in suburban Maryland. While police believe that the burglary was a random occurrence, the VA Inspector General is very critical of the Veterans Affairs department for its lax information security and emphasizes that the employee was not authorized to remove such sensitive material. This theft represents the biggest unauthorized disclosure of Social Security data ever. (C. Lee and S. Vogel "Personal Data on Veterans is Stolen," *The Washington Post*, May 23, 2006, Page A01)

Twenty-five laptop computers that were stolen from Iowa Methodist Medical Center in DesMoines throughout May 2006 turned up on eBay near the end of that month. Although the computers did not contain sensitive information, they were most likely taken by a hospital employee as they had been stored in a locked room. No arrests have been made. (*The Associated Press*, May 18, 2006)

The Pentagon has sent letters to more than 14,000 people who registered for a 2001 Defense Department conference on health care fraud whose names, Social Security numbers, credit card information and other personal information may have been stolen due to a breach of security of the computer system of Tricare Management System, a government health-care contractor. (S. Barr, Conference attendees' personal data may be at risk, *Washington Post*, May 10, 2006)

The University of Texas Southwestern Medical Center sent letters to 1,447 patients in late April telling them of the theft on or about January 1 a computer hard drive containing their names, Social Security numbers and medical diagnoses patients from the center's ophthalmology department. The university's privacy officer delayed informing patients to allow to investigate its own employees, relying on data showing three quarters of such incidents are "inside jobs." (M. Stewart, North Texas patients may be ID theft victims, *CBS 11 News (Dallas),* May 8, 2006)

An annual survey conducted by the American Health Information Management Association reports fewer health plans and providers consider themselves to be "mostly compliant" with the Health Insurance Portability and Accountabilty Act's privacy regulations than a year before. Although 91 percent said in 2005 that they were mostly compliant, that number dropped to 85 percent this year. HIPAA gives patients a right to know who has seen their records other than the people involved in their treatment, payment or health care operations. More than half of the respondents cited some difficulties in complying with this provision. (N. Ferris, Privacy compliance has declined, FCW.com, April 24, 2006)

The Georgia Division of Public Health has shut down a clinic in Carrollton which provided care to about 75 people living with HIV due to "[c]lient confidentiality required for the privacy of clinical services was not being observed," according to a statement by health officials. (Z. Hudson, Carrollton HIV clinic shut down, *Southern Voice*, April 21, 2006)

The Ohio State University Medical Center in Columbus, OH mistakenly posted online the personal health information—including names, addresses, social security numbers, and treatment information—of approximately 2,800 patients. (Associated Press, “Patients’ Personal Health Information Mistakenly Posted Online,” November 4, 2005)

Information about 5,000 patients—including birth dates, Social Security numbers, and diagnostic and financial information—was stolen from the Children’s Health Council, a treatment center in Palo Alto California that treats emotionally troubled and developmentally challenged children. (Ihealthbeat.org, "Medical Records Stolen From California Children's Clinic," 9/21/05 and Webby, San Jose Mercury News, September 20, 2005)

Sensitive information about 57,000 Blue Cross Blue Shield of Arizona patients—including addresses, phone numbers, Social Security numbers, birth dates, and treatment histories—was stolen from Arizona Biodyne, a Phoenix-based managed care company that coordinates behavioral health for Blue Cross of Arizona. (Matt Hanson, "Medical Firm's Files with Personal Data Stolen," The Arizona Republic, July 13, 2005)

Kaiser Permanente Northern California left the names, addresses, phone numbers and lab results of approximately 150 patients posted on a publicly accessible website for up to four years. In violation of both state law and Kaiser's policy, the site was developed without patient consent. It was not until a disgruntled employee linked the website to her online blog that the breach became public. Still, Kaiser did not remove the site until federal civil-rights authorities learned about it in January. Further, Kaiser did not inform state regulators or patients about the breach until March—when it was reported in the media. The state Department of Managed Health Care levied the largest fine for a privacy violation to Kaiser in the amount of $200,000. ("Privacy Breach Costs Kaiser," *San Jose Mercury News*, June 21,2005)

The University of Pittsburgh Medical Center was using an insecure online form to collect patient information, including name, Social Security number, and prescription information. After the form was brought to UPMC's attention, they removed it from their site. More than 100 patients were believed to have used the form. (Christopher Snowbeck, "UPMC Pulls Online Drug Form," Pittsburgh Post-Gazette, May 27, 2005)

About 16,000 patients were notified by Christus St. Joseph Hospital of Houston, TX that a computer was stolen that contained files including their names, social security numbers, and health information. The computer was taken from Gateway File Systems, Inc., which was in the process of converting paper-based medical records to electronic records for St. Joseph. (ROBERT CROWE, "Patients warned that stolen data could be theirs; Letters are sent to 16,000 whose records were on computers taken from St. Joseph," *The Houston Chronicle*, April 26, 2005*)*

The Northwestern Memorial Physicians Group belatedly notified patients of a local health clinic that their blood and stool samples had been stolen weeks previously, along with their Social Security numbers, names, and other identifying information. (Jeremy Manier and Carlos Sadovi "Clinic red-faced about blood theft; Patients angered by delay in reporting theft of specimens," *Chicago Tribune*, April 22, 2005)

Two computers that contained the names, addresses, Social Security numbers, and medical information of 185,000 people were stolen from the San Jose Medical Group in California. (Glennda Chui, "Medical Data Thefts Spur Worry," San Jose Mercury News, 4/12/05)

A Palm Beach County Health Department statistician and epidemiologist mistakenly attached a list containing more than 6,000 names of HIV/AIDS patients to an e-mail sent out to 800 of the department's 900 employees (Mary McLachlin, "HIV E-mail Leads to Changes," *Palm Beach Post,* February 23, 2005).

In the first criminal conviction under the HIPAA Privacy Rule, a Washington state man was convicted of wrongfully accessing a patient's protected health information. Richard Gibson, an employee at a Seattle provider of cancer treatment, admitted that he obtained a cancer patient's name, date of birth and Social Security number. Mr. Gibson admitted to using the information to get four credit cards in the patient's name. ("First Criminal Guilty Plea Offered," www.thompson.com, August 20, 2004)

Medical records from the University of California – San Francisco Medical Center that had been sent to Pakistan for transcription were nearly made public when a Pakistani transcriber threatened to post them on the Internet. Although the transcriber ultimately agreed not to post the records, UCSF could not confirm that she had destroyed them. The American Association for Medical Transcription, an industry group, estimates that about 10 percent of U.S. medical transcription is done abroad, where U.S. privacy laws are virtually unenforceable (D. Lazurus, "A Tough Lesson on

Medical Privacy: Pakistani Transcriber Threatens UCSF over Back Pay," *San Francisco Chronicle*, October 22, 2003, p. A1).

Software developed by Hospice Systems, Inc., the for-profit subsidiary of Hospice of the Florida Suncoast, disclosed the medical records of patients treated at the Hospice. The software, which contains patient names, address, social security numbers and diagnoses, is currently used by approximately 100 hospices. Patients whose privacy was allegedly violated filed a lawsuit in Pinellas-Pasco circuit court in May 2003. ("Lawsuit alleges that hospice released private information," *St. Petersburg Times*, May 2, 2003)

A hacker found a webpage used by the Drexel University College of Medicine in Pennsylvania that linked to a database of 5,500 records of neurosurgical patients. The records included patient addresses, telephone numbers, and detailed information about diseases and treatments. After finding the database through the search engine Google, the hacker was able to access the information by typing in identical usernames and passwords. Drexel University shut down its database upon learning of the vulnerability and a university spokeswoman stated that officials had been unaware that the database was available online, as it was not a sanctioned university site. (C. Null, "Google: Net Hacker Tool du Jour," Wired News, March 4, 2003)

A Kentucky state computer that was put up for sale for $25 contained files naming thousands of people with AIDS and other sexually transmitted diseases. The state auditor's office purchased the computer and, upon taking it back to the office for testing, discovered the confidential information. The auditor's office issued an alert that all surplus computers must be wiped clean with special software. (C. Wolfe, "Discarded Computer had Confidential Medical Information," Associated Press, February 6, 2003)

Thieves broke into TriWest Healthcare Alliance in Phoenix, Arizona and stole computers that contained medical and social security records of over 500,000 retired and current military personnel. TriWest is a contractor that stores information for the Department of Defense. The FBI and other law enforcement agencies are investigating the security breach, and TriWest has offered a reward of $100,000 for information leading to an arrest. It is unknown if any of the personal information obtained in the theft has been misused. (A. Clymer, "Threats and Responses: Privacy," The New York Times, January 11, 2003)

Police in Wilson, Pennsylvania are investigating why medical records from Easton Hospital, including lab reports, drug reports, and doctors' examinations notes, were found on the streets of Allentown, PA. All of the records included patient names and many included addressed and phone numbers. A hospital official stated that an internal investigation had revealed a suspect. The results of this investigation are being made available to the police in Wilson, PA. (D. Nerl and A. Wlazelek, "Patients' Privacy Breached," T*he Morning Call*, August 8, 2002)

Eli Lilly and Co. inadvertently revealed over 600 patient e-mail addresses when it sent a message to every individual registered to receive reminders about taking Prozac. In the past, the e-mail messages were addressed to individuals. The message announcing the end of the reminder service, however, was addressed to all of the participants. (R. O'Harrow, "Prozac Maker Reveals Patient E-Mail Addresses," *The Washington Post*, July 4, 2001, p. E1) The FTC filed a complaint against Eli Lilly alleging that the unauthorized disclosure of personal information by the company was an "unfair or deceptive" act or practice in violation of Section 5(a) of the Federal Trade Commission Act. In January 2002, Eli Lilly settled the FTC charges against the company. It agreed to increase existing security and to create an internal program to prevent future privacy violations. No fine was involved in the settlement because the incident was unintentional. ("Lilly Privacy Violation Charges Are Settled," *The New York Times*, January 19, 2002, p. C3)

About 400 pages of detailed psychological records concerning visits and diagnoses of at least 62 children and teenagers were accidentally posted on the University of Montana Web site for eight days. The information included names, dates of birth and, in come cases, home addresses and schools attended, along with psychological test results. (C. Piller, "Web Mishap: Kids' Psychological Files Posted," *Los Angeles Times*, November 7, 2001, p. A1)

Due to a software flaw, thousands of consumers who requested pamphlets and brochures about drug and alcohol addiction had their names, addresses, telephone numbers and e-mail addresses exposed on Health.org, a government health information Web site. (B. Sullivan, “Health Site Exposed Customer Info,” MSNBC, May 25, 2001)

A hacker downloaded medical records, health information, and social security numbers of more than 5,000 patients at the University of Washington Medical Center. The hacker claimed to be motivated by a desire to expose the vulnerability of electronic medical records. (R. O’Harrow, “Hacker Accesses Patients Records,” *The Washington Post*, December 9, 2000, p. E1)

A doctor’s laptop was stolen at a medical conference. The computer contained the names and medical histories of his patients in North Carolina. (A. Santana, “Thieves Take More than Laptops,” *The Washington Post*, November 5, 2000, p. A1)

Kaiser Permanente mistakenly sent responses to member e-mails to the wrong recipients. The e-mails, some of which contained sensitive patient information, affected 858 members who use their online services. (B. Brubaker, “Sensitive Kaiser Emails Go Astray,” *The Washington Post*, August 10, 2000, p. E1)

Two health care organizations in Washington State were found discarding medical reports in unlocked dumpsters. Among the information found by reporters were patient names, addresses, social security numbers, and detailed descriptions of sensitive medical procedures. (S. Salyer, “Patients’ Records Found in Unsecured Dumpsters,” *The Daily Herald*, June 18, 2000)

The medical records of about 20 patients of Providence Alaska Medical Center were accidentally posted on a Web site. (P. Porco, “Patients’ Privacy Breached; Alaskans’ Medical Records Put on Net,” *Anchorage Daily News*, June 4, 2000)

Thousands of medical records fell out of a vehicle and were blown throughout Mesa, Arizona. The records were being transported to be destroyed. (“Medical Records Fall Out of Vehicle, Blown Through Street,” *Associated Press*, May 26, 2000)

SelectQuote Insurance Services exposed many customers’ personal health information on their Web site. Information submitted by users to receive a life insurance quote was not “cleared” and thus remained on the site where it could be viewed by subsequent users. (M. Brunker, “Insurance Site Exposes Personal Data,” MSNBC, March 22, 2000)

GlobalHealthtrax, which sells health products online, inadvertently revealed the names, home phone numbers, and bank account and credit card information of thousands of customers on their Web site. (B. Sullivan, “Bank Information Exposed Online,” MSNBC, January 19, 2000. Accessed at www.zdnet.com on January 19, 2000)

Several thousand patient records at the University of Michigan Medical Center were left inadvertently on public Internet sites for two months. A student searching for information about a doctor discovered the problem when he came across a link to files containing private patient records with numbers, job status, treatment for medical conditions, and other data. (“Black Eye at the Medical Center,” *The Washington Post*, February 22, 1999, p. F5)

Poor Disposal

The personal health information of more than 200 people was discovered by KPRC Local 2 TV investigators in unlocked garbage Dumpsters outside Houston area Walgreens, CVS and other pharmacies. Investigators found prescription labels, pill bottles and computer printouts disclosing detailed personal medical information. The Texas

State Board of Pharmacy is expected to take immediate action. (Pharmacies dump medical information in trash, *KPRC Local 2 (Houston)*, November 15, 2006)

According to a November 2005 Gartner Inc. survey, nearly 80% of companies said that "managing data security and privacy risks' were very important or most important when disposing of obsolete hardware." Yet 30% admitted they had no policy for ensuring the security of equipment, including hard drives, sold to others. (S. Hildreth, Where hard drives go to die, or do they?, *Searchsecurity.techtarget.com*, May 4, 2006)

A local Michigan news team discovered patient records in dumpsters outside of physicians' offices and other medical facilities. The news team found personal information in one half of the 20 dumpsters they surveyed. The information included patients' names, social security numbers, work addresses, and treatment information; for one patient, information about a hysterectomy and history of depression was included. (WZZM13, Grand Rapids Michigan, November 9, 2005)

Confidential Medicaid records were disclosed during the sale of surplus equipment by the Arkansas Department of Human Services twice in six months. In October 2001, the state stopped the sale of the department's surplus computer drives when it discovered that Medical records that should have been erased were found on the computers. In April 2002, a man who bought a file cabinet from the department found the files of Medicaid clients in one of the cabinet's drawers. The files include Social Security numbers and birth dates. ("DHS Surplus Sales Again Reveal Confidential Information," *Associated Press*, April 3, 2002)

Documents referring to over 125 psychiatric patients of Rapid City Regional Hospital were found in a convenience store trashcan by an editor of the Milwaukee *Journal Sentinel*. A University of South Dakota fourth year medical student had taken the papers outside of the hospital and dumped them in the trash. The documents included lists of patients in the psychiatric unit and their diagnoses, along with the student's handwritten notes about some of the patients. The University's faculty committee will be recommending discipline for the student. (C. Brokaw, "S. Dakota Investigates Psych Records," Associated Press, December 30, 2001)

Aetna health insurance claim forms blew out of a truck on the way to a recycling center and scattered on I-84 in East Hartford during the evening rush hour. Aetna, the nation's largest health insurer, quickly dispatched employees – some of them on the way home from work – to scoop up forms containing names and personal health information. The papers should have been shredded under company policy. ("Careless Disposal of Records Imperils Privacy," *The Hartford Courant*, May 14, 1999)

Intermountain Healthcare, a Utah-based health plan, recently took steps to recover misplaced patient medical files. IHC said that its Salt Lake Clinic had donated a file cabinet to Deseret Industries and did not know that some records and laboratory reports had accidentally slipped behind the drawers. (J. Constanzo, "IHC Sues over Misplaced Records," *The Deseret News*, December 2, 1998)

Hundreds of patient records were found in the parking lot outside Scripps Clinic in California. Information included diagnosis, credit card information and test results. The records appeared to be from multiple health care sites. ("Patient Privacy Dumped in Trash," *San Diego Union-Tribune*, May 18, 1998)

Medical Information Used for Marketing

The Florida Attorney General's office investigated the marketing practices of Eckerd Drug Company to determine whether or not the company is violating customers' privacy. When customers of Eckerd Drug had picked up their prescriptions, Eckerd's had them sign a form not only acknowledging receipt of a prescription but also authorizing the store to release their prescription information to Eckerd Co. for future marketing purposes. The form apparently did not adequately inform customers that they were authorizing the commercial use of their medical information. According to the Attorney General's investigation, no customer or store employee interviewed was aware if the fact that the customer had actually signed an authorization for marketing purposes. In a settlement with the attorney general, Eckerd agreed to change its policies to better protect patient privacy, including restriction of direct marketing of prescription drugs to customers who have given written consent to use their medical information for such purposes. The company also agreed to fund a $1 million ethics chair at the Florida A & M School of Pharmacy. (M. Albright, "More Eckerd Questions," *St. Petersburg Times*, March 5, 2002, p. 1E; J. Dorschner, "Eckerd Endows FAMU Ethics Chair," *The Miami Herald*, July 11, 2002)

An Orlando woman had her doctor perform some routine tests and received a letter weeks later from a drug company touting a treatment for her high cholesterol. ("Many Can Hear What You Tell Your Doctors: Records of Patients Are Not Kept Private," *Orlando Sentinel*, November 1997, p. A1)

The chain drug stores CVS and Giant Food admitted to making patient prescription records available for use by a direct mail and pharmaceutical company. Their stated intent was to track customers who do not refill prescriptions and send letters encouraging them to refill and consider alternative treatments. However, in response to the outrage and worry expressed by their customers, both companies advised their plans to abandon their marketing and direct mail campaigns. (R. O'Harrow, "Prescription Fear, Privacy Sales," *The Washington Post*, February 15, 1998, p. A1)

RxAmerica, a Utah-based pharmaceutical benefits manager, used patient data to solicit business for its owner, American Drug Stores. Patients were asked to switch drug stores and start filling their prescriptions at Sav-on, a chain owned by American Drug Stores. (S. Gallagher, "In the Public Eye," *Kiplingers*, February 2000, p. 78)

On July 9, 2002, the Florida Attorney General issued investigative subpoenas to Eli Lilly & Co., Walgreen Co. and a number of health care providers to determine whether state laws were violated when Prozac tablets were mailed unsolicited to Florida residents. Individuals received an envelope from Walgreens with a letter encouraging them to switch to Prozac Weekly along with a free one-month trial of the drug. The Attorney General's office is concerned not only with the unsolicited delivery of a prescription drug but also with the possibility that privacy rights were violated by the misuse of medical information to target likely candidates for a particular drug. A woman who received the unsolicited Prozac also filed an invasion of privacy lawsuit against Eli Lilly, Walgreens, and her doctor for sending her a drug that she did not request. ("Fla. AG Issues Subpoenas Over Prozac," *Associated Press*, July 10, 2002; B. Japsen, "Florida Prozac Case Raises Issues of Privacy, Health," *Chicago Tribune*, July 11, 2002)

Government Use of Records

The California state Department of Health Services inadvertently revealed the names and addresses of up to 53 people living with enrolled in an AIDS drug assistance program to other enrollees by putting benefit notification letters in the wrong envelopes, officials said Friday. The department learned about the mix-up after 12 people in the drug assistance program phoned to say they had received letters addressed to someone else. The department on Friday mailed certified letters to the 54 enrollees, explaining the mix-up and asking that anyone who received a wrongly addressed letter destroy it. It also notified the California Highway Patrol, as is required by a state law on security breaches. The department is looking into ways to make the system more foolproof, such as using envelopes with window addresses, said health services Director Sandra Shewry. HIV/AIDS services and advocacy groups said this was the first known breach of that database. "I would hope this is an anomaly," said Jeff Bailey, director of client services for AIDS Project Los Angeles. (Engel, M., Mix-up breaches confidentiality of dozens in state AIDS program, *Los Angeles Times*, March 3, 2007)

A Palm Desert medical marijuana dispensary is being required to turn clients' names over to authorities, and client advocates say that violates their privacy rights. Palm Desert city attorney David Erwin said the deal between the city and the CannaHelp dispensary on El Paseo, is merely meant to ensure that the dispensary is obeying state law. Lanny Swerdlow of Palm Springs, head of the Marijuana Anti-Prohibition Project, a patient support group, believes the data sharing to be a violation of the federal Health Insurance Portability and Accountability Act which ensures the confidentiality of patients' medical records. (K. Kaufmann, Dispensary must turn over names, *The Desert Sun*, April 22, 2006)

A Palm Beach [FL] County Health Department statistician and epidemiologist mistakenly attached a list containing more than 6,000 names of HIV/AIDS patients to an email sent out to 800 department employees. (M. McLachlin, HIV email leads to changes, *Palm Beach Post*, February 23, 2005)

In New York City, the Guiliani administration planned to use Medicaid billing records to force individuals into drug and alcohol treatment. The same department maintains both the Medicaid and welfare lists. Participating in substance abuse treatment would have been a requirement for maintaining benefits. The plan was abandoned after significant media coverage. ("Misuse of Drug Treatment Records," *The New York Times*, September 28, 1999, p. A24)

An anti-fraud program came under fire when the California Department of Human Services was accused of providing the Immigration and Naturalization Services with information about immigrants' lawful use of Medi-Cal services. (*California HealthLine*, August 8, 1998)

Federal officials filed a complaint in Federal District Court in Boston seeking an injunction blocking the Federal Inspector General's office from obtaining the names and Social Security numbers of people with AIDS. The IG claims the information is needed to audit eligibility for federally-funded HIV care services programs, but the head of the Federal government's division of HIV services attacked the attempt as "an egregious breach of confidentiality." (T. Lewin, Lawsuit seeks to bar U.S. from access to AIDS files, *New York Times*, April 3, 1996)

Public health workers in Dade County (Fl) lost a confidential log in 1992 they kept of people with AIDS. The log turned up a week later behind a file cabinet. The health department employee who reported the incident was told to destroy her records of the security lapse; a public health investigator later found some workers were not following security protocols. The cover-up is believed to be in response to an earlier incident where a health department employee disclosed the HIV status of an individual to his coworkers. (S. Kestin, Workers say there were told to destroy report on AIDS records, *Tampa Tribune*, November 7, 1996)

Researchers

University of Minnesota researchers violated the confidentiality of organ donors when it mailed a survey to 1,200 transplant recipients participating in a long-term research study and mistakenly revealed the names of those who had donated their kidney to the recipients. Although many recipients already knew the identity of their organ donors, more than 400 learned the name of their donor for the first time. A software upgrade was cited as the reason for the breach, apparently because it altered a feature that was supposed to suppress the donors' names. This is the second time within three months that computer problems at the University have led to the violation of patient confidentiality. In November 2001, a psychologist mistakenly posted the mental health records of 20 children on a public Web site. That breach is still being investigated. (J. Marcotty, "Names of Donors Are Accidentally Included in Letter to Kidney Patients," *Minneapolis Star Tribune,* January 15, 2002, p. 1A)

Boston University created a private company, Framingham Genomic Medicine, to sell the data collected for more than 50 years as part of the "Framingham Heart Study." Anonymous data collected on more than 12,000 people – including medical records and genetic samples – would be sold to researchers. The company was criticized for commercializing what began as an altruistic act on the part of a community. (G. Kolata, "Boston U. Found Company To Sift Leading Heart Data," *The New York Times*, June 17, 2000, p. A10). The company has since been disbanded, but Boston University is appealing the decision to shut down Framingham Genomic. (R. Rosenberg, “Questions Still Linger on Heart Study Access,” *The Boston Globe*, February 21, 2001, p. D4)

The federal Office for Protection from Research Risks suspended more than 1,000 studies at Virginia Commonwealth University, in part for violating privacy by failing to gain the consent of research subjects and failing to adequately safeguard data. (J. Matthews, “Father’s Complaints Shut Down Research,” *The Washington Post*, January 12, 2000, p. B7)

Robin Kaigh of New Jersey reported that her father, a physician, agreed to allow slides of his cancer cells to be used in research. He was promised anonymity, but his name was entered into a computer associated with the slides, and colleagues quickly began calling to offer condolences. (M. Serafini, “Medical Privacy in the Information Age,” *National Journal*, April 18, 1998)

Law Enforcement

A “Persons at Risk” program in New Jersey allows the Burlington Sheriff’s Department to maintain a list of residents with severe mental health problems. The list is intended to be used to help identify and locate people who may be lost or disoriented, but advocates are worried that the information could fall into “the wrong hands” or be used against people. (“New Jersey: Advocates Angry Over ‘Persons-at-Risk’ List,” *American HealthLine*, May 30, 2000)

Two hundred and seventy-four patients were listed by name in a legal brief submitted by the U.S. attorney for Kansas in a fraud investigation. The patients’ names and associated medical procedures and billing records were made public, even though they were not involved in any criminal activity. (J. Duncan Moore, Jr., “Confidentiality Casualty: Patient Billing Printouts Released in Kansas Fraud Case,” *Modern Healthcare*, September 14, 1998, p.3)

Police in Fairfax, Virginia, seized records from a local drug treatment clinic when a car was stolen nearby. The police argued that the records were necessary to identify potential culprits, but returned the records after legal complaints were filed. (B. Masters, “Fairfax Police Concede Seizure Was Wrong,” *The Washington Post*, September 1, 1998, p. D1)

Ben Walker, an employee of the FBI for 30 years, was forced into early retirement after his employer learned that he sought mental health treatment. When Walker’s therapist was under investigation for fraud, the FBI obtained Walker’s prescription records. The FBI then targeted Walker as an unfit employee and stripped him of many of his duties, even though he was later found fit for employment. (A. Rubin, “Records No Longer for Doctor’s Eyes Only,” *Los Angeles Times*, September 1, 1998, p. A1)

Lawsuits

A jury in Waukesha, Wisconsin found that an emergency medical technician (EMT) invaded the privacy of an overdose patient when she told the patient’s co-worker about the overdose. The co-worker than told nurses at West Allis Memorial Hospital, where both she and the patient were nurses. The EMT claimed that she called the patient’s co-workers out of concern for the patient. The jury, however, found that regardless of her intentions, the EMT had not right to disclose confidential and sensitive medical information, and directed the EMT and her employer to pay $3,000 for the invasion of privacy. (L. Sink, “Jurors Decide Patient Privacy Was Invaded,” *Milwaukee Journal Sentinel*, May 9, 2002)

In 2001, a former patient of Johns Hopkins Hospital sued the hospital for $12 million, alleging that the hospital had released his medical records in April 997 to Dorinda Mae Hughes, his former friend and business partner. Hughes gave information about the patient’s former drug abuse problems to his friends, family, business associates, and clients. The court ruled that the hospital did not knowingly give information about the patient's psychiatric troubles to a disgruntled former friend. The patient filed an appeal on December 27, 2001. (S. Graham, "'John Doe' To Appeal Hopkins Privacy Case," *Baltimore Business Journal*, January 14, 2002)

A man diagnosed with AIDS had his prescriptions filled by Trio Drugs, a local pharmacy, to avoid storage of his medical information in a chain store database that could be accessed by health plans. Trio Drugs closed and sold its records to CVS Corp. The man sued, claiming that his privacy was violated when his records were sold without his consent. CVS and Trio Drugs filed a motion to dismiss the case. A New York Supreme Court judge allowed the lawsuit to go forward and stated in his opinion, "Because pharmacists have a certain amount of discretion, and an obligation to collect otherwise confidential medical information, the court must find that customers can reasonably expect that the information will remain confidential." (T. Albert, "Records Privacy Extended to Pharmacies," *American Medical News*, April 2, 2001)

In *Ferguson v. City of Charleston*, the Supreme Court found that a state hospital's drug testing policy constituted an unreasonable search under the Fourth Amendment. In an effort to deter the use of cocaine by pregnant women, the Medical University of South Carolina (MUSC) had cooperated with law enforcement officials to develop a program for identifying and testing pregnant patients suspected of drug use. MUSC used the threat of arrest and prosecution to coerce patients into substance abuse treatment. Positive drug tests were shared with police, and law enforcement officials had access to the medical files of patients who tested positive. Ten obstetrical patients who were arrested after testing positive for cocaine filed a suit challenging the constitutionality of the MUSC policy. (2001 U.S. LEXIS 2460)

On February 15, 2001, Massachusetts' highest court upheld the state's HIV privacy law, ruling that a man whose blood was splattered on law enforcement officials during an arrest is protected from having to reveal his HIV status. (K. Burge, "Suspect's HIV Test Privacy Upheld," *The Boston Globe*, February 16, 2001, p. B3)

Captain Edward Deveau, the acting police chief of Watertown, Massachusetts, is being sued for violating Lieutenant James Conley's privacy by altering a medical release to gain access to Conley's medical information. Conley had given the police department permission to obtain his medical information from a specific doctor, but the release was altered to allow the department to obtain Conley's medical history from two other doctors. The Watertown Police Department claims that it had the right to the information because the department paid for the health services Conley received for an injury sustained while on duty. (L. Kocian, "Acting Chief Sued Over Release," *The Boston Globe*, January 18, 2001, Globe West, p. 1)

After separating from her husband, Annette Wise instructed her local pharmacy, Thrifty Payless in California, not to disclose any of her prescription information to her husband. The day after she made the request, however, her husband asked for, and received, a copy of all of her prescription records from the pharmacy. He claimed that he needed them for tax purposes. Mr. Wise subsequently disclosed the information to family, friends, the Department of Motor Vehicles, and others, alleging that she was a drug addict and a danger to their children. (*Annette Wise v. Thrifty Payless*, 2000 Cal. App. LEXIS 765)

As part of a workers' compensation claims case, a California man authorized that his medical records be released. His HIV status was revealed in the process, even though it was not relevant to the case. Despite the existence of a strong HIV confidentiality law in California, the court ruled that there was no obligation to exclude the information. ("CA App. Ct. Says Plaintiff's Signed Release Bars HIV Privacy Suit," *AIDS Litigation Reporter*, February 22, 2000)

A Washington, D.C. jury ordered a local hospital to pay $25,000 for failing to keep a patient's medical records confidential. Coworkers learned of the victim's HIV status after an employee at the Washington Hospital Center revealed information from his medical record. (P. Slevin, "Man Wins Suit Over Disclosure of HIV Status," *The Washington Post*, December 30, 1999, p. B4)

In a case pending in Georgia, a nurse claims that her immediate supervisor accessed her medical records without permission. The supervisor, Dr. Thomas Boyer of the Emory School of Medicine, accessed her electronic medical records by posing as her treating physician. He claims that he did so out of concern that she had contracted an illness on the job. (B. Schmitt, "Suit Alleges University Tapped into Nurse's Medical Records," *Fulton County Daily Report*, October 26, 1999)

A psychiatrist from New Hampshire was fined $1,000 for repeatedly looking at the medical records of an acquaintance without permission. Because there was no state law making it a crime to breach the confidentiality of medical records, the case was brought under a law against misusing a computer. ("Psychiatrist Convicted of Snooping in Records," *The Associated Press State & Local Wire*, May 5, 1999)

Renee McIntosh is suing a San Francisco law firm that represents her employer, Safeway. McIntosh claims that the firm shared information – including a psychiatric evaluation – about her workers' compensation claim with one of her coworkers. (K. Flaherty, "Litigation Privilege vs. Privacy Is Issue in Suit," *American Lawyer Media*, April 9, 1999, p. 2)

In 1998, Longs Drugs in California settled a lawsuit filed by an HIV positive man. After a pharmacist inappropriately disclosed the man's condition to his ex-wife, the woman was able to use that information in a custody dispute. However, rather than pursue the suit against the pharmacy, the man chose to settle in order to avoid a court trial that could result in news coverage – and further disclosure – of his illness. ("Longs Drugs Settles HIV Suit," *San Diego Union-Tribune*, September 10, 1998, p. A3)

A man with AIDS won an out-of-court settlement with a Michigan pharmacy in 1998 after a pharmacy clerk told Stanley Grzadzinski's children that he had AIDS. ("Settlement in Privacy Suit Against Drug Store; Children Allegedly Learned of Dad's AIDS from Son of a Pharmacy Clerk," *Chicago Tribune*, January 9, 1998, p. 10)

A Minnesota man filed a lawsuit against Northwestern Mutual Life Insurance Co. for allegedly signing his name on an authorization form to release his mental health records without his knowledge. (J. Gaw, "Insurance Firm Sued Over Mental Health Records," *Star Tribune*, August 7, 1997, p. D3)

In *Doe v. SEPTA*, Rite-Aid drug store in Pennsylvania provided to the state's transportation authority (SEPTA) information about the prescription drugs being taken by SEPTA's employees. In disclosing to SEPTA authorities that one of its employees was receiving AZT, Rite-Aid in effect disclosed the employee's HIV status. Prior to the disclosure, Doe's employers had assured him that although they were self-insured, no information regarding his prescription drugs or HIV status would be disclosed outside of the Medical Department. The court found no privacy violation stemming from this disclosure since Doe could not prove actual damages, and the employer was deemed to have legitimate interest in knowing the details of how its employees used the health plan. (*Doe v. SEPTA*, WL 76, 2891. (3d Cir. 1995))