

Another Huge Medical Data Breach is Mishandled

by dugan November 7, 2008 4:00 PM PST

Both president-elect Barack Obama and Sen. John McCain backed electronic medical records during their campaign. Computerizing patient data, which could increase efficiency and cut costs, is part of every major federal health reform proposal. But what are the rules for this data? [An extortion threat reported today](#), and involving up to 50 million patients' prescription drug records, shows the huge risks in letting unregulated for-profit companies take charge of Americans' medical records.

The company, called Express Scripts, not only had a serious hole in its data security, it also isn't doing nearly enough to help its clients.

Express Scripts is a pharmacy benefit manager, handling prescription drug plans for clients including insurance companies, employers and union health plans. It covers about 50 million people. Yes, 50 million. It's a very profitable middleman job in the health industry.

Here's what happened, according to the NY Times story:

The company said Thursday that it had been investigating the threat since early October, when it received a letter that contained personal information on about 75 of its members including names, dates of birth, Social Security numbers and, in some cases, prescription information.

Wouldn't you want to know if your information may have been stolen? Don't look to Express Scripts for much help. The company has called in the FBI, but it hasn't personally notified any of its patients, except for the 75 people named in the extortion letter. So the company waited a month before going public. Its stated reason, [according the Wall Street Journal](#), is that it wanted to "get the investigation up and running" first. Pardon my suspicion, but I think Express Scripts was waiting to see if it got reports of identity theft. It says it hasn't, but how would most of us even know that a credit problem was linked to a huge but nearly anonymous "pharmacy benefits manager?"

Even people who order their drugs online don't see the company mailing back their Lipitor as a brand like MasterCard or Visa (and credit card companies at least have to follow strict rules about disclosing data breaches). Patients who get their prescriptions at a drugstore wouldn't have any direct contact at all with Express Scripts.

Here are other ways that Express Scripts is failing its duty:

- Instead of notifying all patients, it is depending on the news media to get the word out and guide patients (if they even know they're "clients" of Express Scripts) to a [special "support" website](#) about the extortion threat.
- People who hear about Express Scripts in passing, for instance on radio news, won't find a word about possible theft of their data on [Express Script's main corporate website](#). As of today, it has a small-type link for people with "questions about safeguarding your personal privacy." Most of us would take this to be something about the corporate privacy policy.
- I put "support" in quotes in discussing the client web site because it offers precious little support. It links to credit bureaus like Experian, and some government agencies. It just tells folks to go check their credit reports for themselves.. No advice is offered regarding possible release or misuse of their private medical information, except to be "alert" to any irregularities in their pharmacy benefit statements
- The support site suggests that individuals "consider placing a security/fraud alert or extended security/fraud alert through the credit bureaus," which, depending on whether you opt for a "security freeze," can cost money and freeze up individual's ability to get credit unless they pay for a temporary lifting of the alert. In any case, it's a thrash to contact all three major credit bureaus.
- In similar data theft instances involving [financial companies](#) and the [Veterans Administration](#), possible victims were offered free credit monitoring for a year or more, even if no instances of fraud were detected. In the case of a stolen laptop at the VA, it was recovered two months later with the files unopened.

Express Scripts says it was able to identify the location on their system from which the data was lifted, and says it has plug whatever security loophole might have been found. Unfortunately, there is no regulation of how secure such data must be, no impetus in the for-profit world to put top-notch data security at the top of the corporate list.

Drug companies increasingly seek to use pharmacy databases for commercial purposes, including direct advertising of their own drugs for a patient's condition. This offers another opportunity for hacking or theft, as well as inappropriate interference in doctor-patient relationships. Read [here](#) and [here](#) about how Consumer Watchdog fought off an attempt to make this use legal in California.

Google, the search giant, is offering Google Health," where consumers can store their own health data. Google, however, keeps the data. It says it will only use your data in aggregated ways, without personal information. But it does [allow third parties](#) to ask you for access, even for advertising and promotional uses. Google reserves the right to change its policies in the future, and theft is always a threat.

President-elect Obama has signaled that broad health care reform may have to be delayed because of the financial meltdown, but that he is open to faster partial reforms. Here's one that he can take on at no cost to taxpayers:

- Oversee and regulate all of these huge patient databases held by for-profit companies.
- Make sure that intense security comes before, not after, profit. Ban any third-party commercial use of patient information.
- Put simply, ensure that patient privacy is the first thing that a CEO thinks about in the morning--or else.