Are You at Risk for Medical ID Theft?

Cyber criminals hacked into the computers at a major Washington, D.C., hospital chain this week, forcing the outfit's medical records systems offline for thousands of patients and doctors, federal law enforcement officials said.

MedStar Health Inc. officials confirmed that a computer virus crippled operations at the chain's Washington-area hospitals and doctors' offices, leaving patients unable to book appointments and staff locked out of their email accounts.

Computer security experts said the case was the just latest in a series to highlight the vulnerability of digital medical systems, including electronic medical records pushed and underwritten by Obamacare in recent years. It also spotlights the importance of taking active steps to protect the security of your health information, in the same way consumers advise keeping bank and credit card records safe.

Twila Brase, president of the Citizens' Council for Health Freedom—a Minnesota-based organization dedicated to protecting patient privacy rights—tells Newsmax Health that medical ID theft is a growing national problem.

"I do see it growing," she says. "It's one of the problems with a push toward a National Medical Records System because now we have created, or will create, a bigger and bigger target as our medical records get connected without our consent, mind you."

A law enforcement official said the FBI was assessing whether the MedStar virus was so-called "ransomware," in which hackers extort money in exchange for returning a victim's systems to normal, ***CBS News*** reports.

MedStar operates 10 hospitals in Maryland and Washington, including the MedStar Georgetown University Hospital, along with other facilities. It employs 30,000 staff and has 6,000 affiliated physicians.

The Medstar incident was the latest against a U.S. medical provider. Last month, a Los Angeles hospital paid hackers $17,000 to regain control of its computer system, which cyber attackers had seized with ransomware.

In other recent data breaches, America's second-largest health insurer, Anthem, was targeted by hackers who accessed the records of 80 million people, and Premera Blue Cross, based in Washington State, reported a cyber attack that affected 11 million policyholders.

In both cases, thieves gained access to claims data, including clinical records, banking account numbers, Social Security numbers, birth dates and other personal information.

Experts say computer security of the hospital industry is generally poor, and the federal Health and Human Services Department regularly updates a list of health care providers that have been hacked and patient information stolen.

Between 2010 and 2013, nearly 950 data breaches of protected health information were reported by entities covered by the Health Insurance Portability and Accountability Act (HIPAA)—involving approximately 29 million records, according to a study published in the *Journal of the American Medical Association*.

The increase in recent cyber attacks has paralleled a major shift to digital medicine and electronic health records (EHRs) in the United States, largely pushed and underwritten by Obamacare.

Advocates of EHRs note that going digital has numerous benefits for patients and doctors. EHRs are easier to track

than paper records, giving doctors access to patient info in an instant. They have also been shown to reduce prescription error risks and have led to the creation of create large health databases that offer clues to the best care practices for the diagnosis, treatment, and management of cancer, diabetes, heart disease, and other health conditions.

But as the MedStar case shows, there are also significant downsides to EHRs, which give hackers the ability to cripple health care systems with viruses and hand ID thieves easier access to sensitive patient health information.

“When you have these kinds of systems that connect all of this information together, it just becomes a very valuable target to those who see how much money that they can make off of our medical IDs,” Brase says.

The Medical Identity Fraud Alliance estimates that 2.3 million Americans are victimized annually by such breaches, with total damages adding up to $20 billion a year. About a fifth of medical ID theft victims have suffered a decrease in their credit scores, a third lost their health insurance, and two-thirds have paid an average of $13,500 to resolve the crime, according to MIFA.

Records acquired through medical ID theft are 20 times more valuable than financial information on the black market, MIFA says. Thieves who steal a patient’s name, medical records and insurance numbers can use them to get drugs or file fraudulent insurance claims or get health care.

But there are some steps you can take to reduce your chances of falling prey to ID thieves:

- Check your credit reports regularly for unpaid bills. Don’t give out your personal information to friends or family members.
- You’re entitled to one free copy of your credit report each year from each of the three main reporting bureaus

(access them at).

- Protect your health records like would bank and credit card information.
- Ask your doctor to see your medical records to check for errors.
- Read your explanation-of-benefits statements from providers to check for fraudulent charges.
- Ask your health insurer and medical providers for what’s called an “accounting of disclosures,” a listing of who has received your records and what info received.
- Be on the lookout for scams, such as if someone claims to work for a health care company and offers you some services for free or for a too-good-to-be-true price.
- If you find that you’ve been victimized, report it to your insurance provider, doctor, as well as to local police, and federal or state authorities.

For the original article, visit .