Health Information Compliance Alert

Case Study: Watch Out: Hackers Want Your Patient Databases

How cyberattackers are gaining easy access to your data.

This hasn't been a good HIPAA year for health plans. Yet another health insurer is facing costly and harsh consequences after a breach went undetected for years and revealed the protected health information (PHI) of a whopping 10 million individuals.

And this latest breach follows a string of significant health plan data breaches in 2015, including the **Anthem Inc.** breach affecting 80 million members, the **Premera Blue Cross** breach affecting 11 million members, and the **CareFirst** breach affecting more than 1 million members, according to a Sept. 11 blog posting by attorney **Dianne Bourque** for the law firm **Mintz Levin P.C.**

(See "How 'Phishing' Netted A Monster Of A HIPAA Breach," HICA Vol. 15, No. 3, page 17 for more on the Anthem breach; "Beware: HIPAA Compliance Won't Always Ensure Protection From Breaches," HICA Vol. 15, No. 4, page 25 for more on the Premera breach; and "Keep Your Eye On 'Look-Alike' Domain Names To Prevent Cyberattacks," HIC Vol. 15, No. 6, page 41 for more on the CareFirst breach.)

Big Breach Equals Big Problems

Background: On Aug. 5, **Excellus BlueCross Blue Shield** (BCBS) learned that cyberattackers had gained unauthorized access to their information technology (IT) systems, accessing individuals' names, birthdates, Social Security numbers, mailing addresses, telephone numbers, member identification numbers, and financial account and claims information.

The unauthorized access affects more than 10 million members, including other BCBS plans for members who sought healthcare services in 31 counties comprising Excellus' upstate New York service area. Also affected are BCBS affiliates **Lifetime Benefit Solutions, Lifetime Care, Lifetime Health Medical Group, Univera Healthcare,** and **The MedAmerica Companies**.

Excellus discovered the hacking incident while cybersecurity experts were performing a "digital forensics assessment" of the company's network security. Excellus notified the **FBI** of the cyberattacks, the first of which occurred back in December 2013, and is working with leading cybersecurity firm **Mandiant**.

On Sept. 9, Excellus mailed letters to affected individuals and is providing two years of free identity theft protection services through **Kroll**, as well as credit monitoring through **TransUnion**. So far, the investigation has not shown that the attackers removed data from Excellus' systems, nor have they used the data inappropriately.

Class-Action Lawsuits are Inevitable

Devastating fallout: Despite the two years of free identity theft protection services, the sensitive information that the hackers obtained "may continue to pose problems for the victims, especially children, well into the future," noted the law firm **Faraci Lange Attorneys**, which has filed a class-action lawsuit against Excellus seeking damages for individuals affected by the breach.

The law firm **Weitz & Luxenberg P.C.** has also filed a class-action lawsuit. Several other law firms are investigating the breach, in expectation of filing class-action lawsuits, including **Keller Rohrback LLP, Berger & Montague P.C.**, and **Goldman Scarlato & Penny P.C.** (GSP), among others.

"These remedial actions come too late," GSP said of the free credit monitoring and identity theft protection that Excellus is offering to its members. "Once the sensitive personal data of customers has been stolen, it is usually only a matter of time before the repercussions will be seen. In many cases, fraud stemming from the hack will continue long after the two years of credit monitoring has passed."

Case in point: Coinciding with the Premera Blue Cross and Anthem breaches, "were an alarming number of reports of stolen Social Security numbers being used to file false tax returns and claim refunds in the names of persons whose identity was stolen," GSP noted. "Potential fraudulent activity could also include healthcare fraud and obtaining credit cards in someone else's name."

What's more: Lawmakers are also using this latest HIPAA breach as a testament to toughening up cybersecurity legislation. Senate Banking Committee member Sen. **Charles Schumer** (D-N.Y.) referenced the huge Excellus cyberattack when recently calling for action on cybersecurity legislation:

"The fact that this data breach was not discovered for 19 months just goes to show how sophisticated online hackers are and how much work we have to do when it comes to protecting our personal information," Sen. Schumer said. "So I am urging my colleagues in Congress to strengthen consumer cyber protections and require companies to notify their customers if there has been a breach of their personal information in a timely manner so they can take action to ensure they are not the victim of identity theft."

Beware of Hackers Targeting Your Databases

So what can you learn from this latest big healthcare data breach? First, "it seems healthcare hacks won't be slowing down any time soon," **IdentityForce** president **Judy Leary** warned in a Sept. 16 company blog posting. And the question experts are asking is: Who's next?

Danger: And as hackers are getting cleverer, healthcare providers are taking longer to notice hacking incidents and unauthorized access. The delay in discovering the hacking incidents in the Excellus case isn't out of the norm the recent CareFirst breach involved hackers gaining access to a member database a year before the health plan detected the breach, Leary noted. Like the Excellus case, "CareFirst only discovered the hack because it was updating its security in the wake of breaches at other companies."

In addition to the dangers of long delays in detecting breaches, keep in mind that medical records are lucrative. "With healthcare information becoming increasingly digitized and tied to financial data an insurer can link to bank accounts for automatic withdrawal, for example these records are soaring in value on the black market," Leary said.

Value: "Some security experts have estimated that medical information and insurer data are worth 10 times more than your credit card number," Leary cautioned. And this is, in part, because medical records can include data not just on the individual, but on the entire family.

And according to **SurfWatch Labs**' 2015 Mid-Year Cyber Risk Report, cyber criminals are targeting access to databases. Why? "Database information has a long 'shelf life,'" noted **Mary Beth Gettins** of **Gettins' Law** in a Sept. 10 blog posting. "Databases may have information dating back days, months, years. Databases have large amounts of information in one place that can be sold on the black market, used for identity theft or in future phishing efforts."

Watch for: According to the SurfWatch report, hackers are targeting the healthcare industry specifically, including health plans, healthcare providers, healthcare facilities, "or just about anybody in healthcare," Gettins noted. Hackers are gaining access in countless ways, but most of the ways are related to employees, such as:

- Devices (laptops, USB drives, etc.) and physical files stolen after being left at inappropriate/unsecured places;
- Devices taken after improper disposal or storage;
- Disgruntled employees selling information to criminals;
- Employees intentionally or unintentionally accessing information illegally; and
- Employees unwittingly given access to criminals directly or indirectly.

Link: For more on the Excellus data breach case, visit www.excellusfacts.com or

https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf. To read the SurfWatch report, go to http://info.surfwatchlabs.com/2015-mid-year-cyber-risk-report.