Codify
BY AAPC

# Health Information Compliance Alert

## Case Study: Keep Your Eye On 'Look-Alike' Domain Names To Prevent Cyberattacks

**How latest HIPAA breach could involve hackers in China.**

Health insurance companies seem to be bearing the brunt of the latest large-scale HIPAA security breaches, and this latest breach affecting 1.1 million individuals is only furthering this trend. But these recent breaches may have far more in common with one another than just the fact that they involve insurers.

**Watch Out: Yet Another Attack on a Health Insurer**

Background: On May 20, the Maryland-based insurance provider **CareFirst Blue Cross Blue Shield** announced that one of its databases was accessed in a cyberattack back in June 2014. The cyber-attackers gained limited, unauthorized access to approximately 1.1 million CareFirst members' information.

Although CareFirst claims that only "limited personal information was involved in this attack," the insurer is nevertheless offering affected members two years of free credit monitoring and identity theft protection services, according to www.carefirstanswers.com, a consumer-focused website that CareFirst established following the discovery of the breach. The **FBI** is also investigating the breach.

Although the hackers appeared not to have accessed any members' Social Security numbers, medical claims information or financial information, they may have acquired member-created user names for CareFirst's website, as well as members' names, birthdates, email addresses and subscriber identification numbers, according to a May 22 blog posting by Rochester, N.Y.-based associate attorney **Kate Martinez** for the law firm **Nixon Peabody LLP**.

**How CareFirst Discovered the Breach**

CareFirst actually discovered the cyberattack during ongoing IT security review efforts following the recent cyberattacks on other health insurers, namely **Premera** and **Anthem.** CareFirst hired leading cybersecurity firm **Mandiant** to conduct an end-to-end examination of the insurer's IT environment, including multiple comprehensive scans of its IT systems to search for any evidence of a cyberattack.

Mandiant's security review revealed that cyber-attackers accessed one of CareFirst's databases in June 2014. Specifically, the database stores data that members and other individuals enter to access CareFirst's websites and online services. Mandiant found no other prior or subsequent attach and no evidence that hackers accessed any other personal information.

(For more on the Anthem breach, see "How 'Phishing' Netted A Monster Of A HIPAA Breach," HICA Vol. 15, No. 3, page 17. For more on the Premera breach, see "Beware: HIPAA Compliance Won't Always Ensure Protection From Breaches," HICA Vol. 15, No. 4, page 25.)

**Trend Emerges: Evidence Points to Bigger Hacking Operation**

What's most disturbing about the CareFirst breach is the not-so-subtle evidence that points to a larger trend in cyberattacks on insurers  possibly by the same overseas attackers.

In particular, "there are indications that the same attack methods may have been used in this intrusion as with breaches at Anthem and Premera, incidents that collectively involved data on more than 90 million Americans," pointed out computer security expert **Brian Krebs** in a May 21 Krebs on **Security LLC** blog posting.

Although "nobody is officially pointing fingers," Krebs said that "there are clues implicating the same state-sponsored actors from China thought to be involved in the Anthem and Premera attacks." Security researchers at the cybersecurity firm **ThreatConnect Inc.** found that in both the Anthem and Premera attacks, hackers registered false domains and subdomains in the insurers' names and that the hackers used the domains in conjunction with malware designed to mimic a software tool that many organizations commonly use to allow employees remote access to internal networks.

"Turns out, the same bulk registrant in China that registered the phony Premera and Anthem domains in April 2014 also registered two CareFirst look-alike domains," Krebs noted. ThreatConnect also discovered evidence that hackers used the same tactics on **Empire Blue Cross Blue Shield,** which was one of the organizations impacted by the Anthem breach.

**Lesson learned: "**This incident again highlights the ongoing efforts that companies, particularly those in the health industry, must take to protect against and respond to cyberattacks," cautioned Washington, D.C.-based associate attorney **Stephanie Carson** in a May 25 blog posting for the law firm **Cooley LLP.**

"It is no secret that the healthcare industry is a top target for cyberattacks," Martinez warned. "And the attack against CareFirst is just one in a string of attacks against health insurers and other entities that collect and use sensitive information."