Health Information Compliance Alert

Take A Peek Inside Health Insurers' Cyber Security Practices

Despite lackluster efforts in key security areas, insurers' confidence is strong.

If the massive breach of **Anthem, Inc**. isn't a good reason to take a closer look at health insurers' HIPAA compliance, then what is? In an instance of good timing, a new report came out examining just that.

On Feb. 8 (just days after Anthem reported its major breach of 80 million patient records), the **New York State Department of Financial Services** (NYSDFS) released a report that illustrates the current cyber security landscape in the insurance industry, according to a Feb. 12 analysis by attorneys **Dianne Bourque** and **Jordan Cohen** with the law firm Mintz Levin Cohn **Ferris Glovsky and Popeo PC.**

The "Report on Cyber Security in the Insurance Sector" analyzed data collected from 43 insurance entities, 21 of which are health insurers and the rest comprised of life insurance providers and property and casualty insurers. The report addressed six major topics:

1. The insurer's information security framework;

2. The use and frequency of penetration testing and results;

3. The budget and costs associated with cyber security;

4. Corporate governance around cyber security;

5. The frequency, nature, cost of, and response to cyber security breaches; and

6. The insurer's future plans for cyber security.

The NYSDFS provided a handful of valuable insights on the state of cyber security in the health insurance industry in its report, especially in light of the recent Anthem breach. The report highlighted the following findings:

- **Cyber security sophistication is all over the map:** The report found that the size of an insurer's assets doesn't necessarily dictate the sophistication of its cyber security program. "The breach of Anthem, one of the largest health insurers in the country, may be viewed as leading credence to this finding," Bourque and Cohen wrote. The insurer's transactional frequency, variety of business lines written, and sales and marketing technologies also impact the sophistication of the cyber security program.
- **Confidence is high:** More than half of surveyed insurers reported that their current information security strategy adequately addresses new and emerging cyber risks. Approximately 95 percent of insurers said that they have adequate staffing levels for information security, but only 51 percent reported having a budget specifically for cyber security events.
- **In-house IT management dominates:** Nearly 60 percent of surveyed insurers relied entirely on in-house IT system management. "The Anthem hack will certainly raise questions about the capabilities of in-house IT management," Bourque and Cohen cautioned. Health insurers were also the least likely to implement intrusion detection systems.
- **Cloud policies are scant:** "Of the three insurance sectors surveyed, health insurers were the least likely to have policies and procedures in place to mitigate the information security risks associated with cloud computing," according to Bourque and Cohen.

The NYSDFS also highlighted three areas of improvement to help foster better cyber security in the health insurance industry:

1. Management of third-party service providers that handle sensitive information, with a focus on obtaining the appropriate representations and warranties from the third-party service providers;

2. The potential use of new security technologies, such as multi-factor authentication, to prevent breaches; and

3. The potential industry benefit that could result from a larger cyber insurance market.

Resource: To read the NYSDFS report, go to www.dfs.ny.gov/reportpub/dfs_cyber_insurance_report_022015.pdf.