BURR ARTICLE

Cyber Threats Equal Serious Threats

By Kelli Carpenter Fleming

Reprinted with Permission from the Birmingham Medical News

Every where you look these days, there seems to be another report of a cyber attack--attacks which do not discriminate based on industry type, size of business, or impact. In other words, everyone is vulnerable. In fact, the phrase, "it is not **if** it happens, it is **when** it happens" has become commonplace when discussing security incidents.

Given the number of incidents occurring within the healthcare industry, over the past few months, the Office of Civil Rights ("OCR"), the entity overseeing compliance with the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and its implementing regulations, has issued extensive guidance on monitoring cyber threats and responding to cyber attacks. One theme throughout the OCR guidance is reporting the incident to various governmental authorities. However, while governmental reporting can have significant benefits, any disclosure of a cyber-incident needs to be carefully considered and analyzed.

In February, OCR issued guidance on reporting and monitoring cyber threats. In the February guidance, OCR encourages covered entities and business associates to report cyber security incidents, cyber threat indicators, and phishing incidents to the United States Computer Emergency Readiness Team ("US-CERT"), a branch within the Department of Homeland Security. US-CERT develops information on cyber security incidents, responds to incidents, and analyzes data regarding incidents. In addition, the February guidance encourages covered entities and business associates to sign up to receive e-mail alerts from US-CERT regarding known patches and mitigations.

In June, OCR issued a checklist for steps that covered entities and business associates experiencing a security incident should take. Similar to the February guidance, the June checklist includes various reporting recommendations. Specifically, the June guidance states that in the event of a cyber incident, entities should take the following steps:

- Execute response and mitigation procedures and contingency plans.
- Report the incident to law enforcement agencies, including state and local law enforcement, FBI, and the Secret Service.
- Report the incident to appropriate federal information-sharing and analysis organizations, such as the Department of Homeland Security and the HHS Secretary for Preparedness and Response.
- Report the incident to OCR through the breach reporting process, if such breach reporting is required.

While OCR has repeatedly indicated that cyber incidents should be reported to various federal agencies, as evidenced above, covered entities and business associates should first analyze the advantages and

disadvantages of making such reports. While getting federal agencies involved may be helpful in terms of mitigating and stopping the threat or preventing it from happening again, as the agencies may have seen this type of incident before, one can only wonder what type of exposure such report will correspondingly bring. Will the report be shared with OCR? If so, what if an internal determination is made that the incident is not a reportable HIPAA breach? Will OCR investigate that internal determination now that it is aware of the incident? Will response and mitigation efforts be analyzed and scrutinized? Do you open yourself up to additional penalties and exposure?

Please keep in mind that anytime a report is made to any authority regarding a cyber incident, protected health information shall only be included when absolutely necessary, and even then, only in accordance with the disclosure requirements of HIPAA.

Cyber incidents are here to stay, and I can almost guarantee that we will continue to see more and more guidance from OCR on how to prevent them and how to respond to them when they do occur. Reviewing such guidance may not only help strengthen Security Rule compliance, but may also help avoid a widespread reportable HIPAA breach.

For more information, please contact:

Kelli Carpenter Fleming
Partner, Birmingham Office
Phone (205) 458-5429
E-Mail kfleming@burr.com

Kelli Fleming is a partner at Burr & Forman LLP who works exclusively within the firm's Health Care Practice Group.