# What the Cybersecurity Information Sharing Act of 2015 means for your organization

| Tuesday, February 9, 2016

Many people missed that, before the clock struck midnight on January 31, 2015, the Cybersecurity Information Sharing Act of 2015 (CISA), a bill that was years in the making, passed. How did so many people miss it? Well, CISA was packaged in a 2,000+ page spending bill that was not the most exciting thing to read as you can imagine.

CISA, which was part of the Cybersecurity Act of 2015, became law on December 18, 2015. So what does it mean for privacy professionals and organizations?

#### What you need to know about CISA

CISA attempts to encourage organizations to share cyber threat indicators they experience with the government to promote the spread of this information to other organizations so they can look out for similar threats and improve their cyber defenses. The goal is to help organizations prepare for and respond more quickly to cyber threats.

While CISA was heavily supported by Congress and backed in both the private and public sectors, many commenters questioned whether CISA's privacy safeguards are enough and whether the liability protections are enough to reduce the fears of many different organizations that feel they will be sued based on the information they voluntarily divulge and share. Not surprisingly, CISA's ultimate value will depend heavily on whether organizations actually start sharing, receiving, and using other organizational

cybersecurity threat information.

CISA's value has been further challenged because of concerns regarding how the privacy rights of individuals may be affected when an organization voluntarily chooses to share information with the government. According to CISA, it requires participating organizations to first eliminate any information that is "not directly related" to a cybersecurity threat that the organization knows of at the time of sharing to be personal information that "identifies" a specific individual.

#### Cybersecurity best practices for the healthcare industry

The Cybersecurity Act of 2015 also directed the Department of Health and Human Services (HHS) to develop cybersecurity best practices for organizations in the healthcare industry. The relevant provision (Section 405 of Title IV) directs the HHS secretary to establish and regularly update a set of voluntary cybersecurity best practices standards. While these standards are to be consistent with the current HIPAA Security Rule, they may be more specific and potentially inconsistent with current industry practices.

CISA also directs the HHS secretary to create a new public-private task force to review the challenges to securing networked medical devices and other software or systems that connect to electronic health records. The task force is directed to report on ways healthcare stakeholders can improve their preparedness for, and response to, cybersecurity threats.

#### What's next?

While CISA has already passed, a lot of implementation steps have to be done over the next few months as follows:

- The Departments of Justice (DOJ) and Homeland Security (DHS) must issue privacy guidelines governing the federal government's receipt and handling of the cyber threat indicator information from the privacy sector organization. These privacy guidelines are to be released on February 16 in interim form, and in final form in June.
- The DOJ/DHS is to issue guidance to assist private entities in identifying types of cyber threat indicators that are unlikely to implicate privacy concerns when shared. These guidelines are also due February 16.
- The DOJ/DHS procedures on automated dissemination of cyber threat indicators among federal government agencies are due February 16 in interim form, and in final form in June.
- DHS is to establish a fully operational portal for the government to receive cyber security threat data from private entities. DHS is to certify to Congress by March 17 that this capability is operational.

#### Key takeaways for privacy professionals

One important takeaway from the enactment of CISA is that organizations engaging in cybersecurity threat information sharing have new guidance on how to consider and mitigate the privacy implications of such sharing, with more detailed information set to emerge in the coming months.

Organizations in the healthcare industry should pay close attention to the implementation of these CISA provisions. Although the standards are labeled voluntary, their publication may cause pressure to make them industry standards. In addition, both the cybersecurity best practices and task force report findings could be used against healthcare entities in administrative or judicial proceedings related to a cybersecurity incident.