SPECIAL ADVERTISING FEATURE TO COLUMBUS BUSINESS FIRST

COLUMBUS BAR ASSOCIATION

Legal Connections

CBA www.cbalaw.org

LEGAL EXPERTISE FOR THE BUSINESS COMMUNITY

APRIL 2 , 2021

Our members can improve their online presence using the CBA's digital marketing studio. Visit cbalaw.org for details.

Jill Snitcher McQuain, Esq.
Executive Director
jill@cbalaw.org

INFORMATION BLOCKING IN 2021

Information blocking is a practice by a health care provider, a health information exchange or other designated actors that is likely to interfere with access, exchange or use of electronic health information, or EHI. The secretary of HHS has identified eight categories of "reasonable and necessary activities" that do not constitute information blocking, though a practice that does not meet the conditions of an exception would not automatically constitute information blocking. Such practices would not have guaranteed protection from penalties or disincentives and would be evaluated on a case-by-case basis to determine whether information blocking has occurred.

JENNIFER NELSON CARNEY, ESQ., ,
Bricker & Eckler

The applicability date for the information blocking regulations in the ONC Cures Act Final Rule was set as Nov. 2, 2020, but was subsequently adjusted in the ONC Interim Final Rule to April 5 in recognition of the significant demands that COVID-19 has placed on health care providers. With the pandemic unabated, the American Hospital Association recently urged the Department of Health and Human Services' Office of the National Coordinator for Health Information Technology to further extend the applicability date to Jan. 1, 2022, or six months after the end of the Public Health Emergency, whichever is later.

Given the extensive nature of the regulations, compliance with the information blocking requirements necessitates that many health care providers make significant administrative and technological overhauls, including conducting a thorough analysis of their internal processes and procedures to determine what operational changes need to be made. Adding to providers' burden is a lack of clarity on key elements of the regulations as well as confusion as to how the regulations intersect with the HIPAA Privacy Rule.

ONC has begun populating information blocking FAQs to assist health care providers in understanding the parameters of the regulations. In early January, ONC added several new FAQs, including clarification that the information blocking regulations do not require actors to proactively make EHI available to patients or others who have not requested the EHI. Instead, once a request to access, exchange or use EHI is made, providers must timely respond to the request. The ONC further stated that delays or other unnecessary impediments could implicate the information blocking provisions, which, in practice, could mean a patient would be able to access EHI, such as test results, in parallel to the availability of the test results to the ordering clinician. Such a practice is a departure from the normal sequence of events for many health care providers and is only one example of the significant changes providers must accommodate to comply with the regulations. ONC has indicated that it will continue to add FAQs, which should help guide providers.

Though the penalties for health providers are unknown (referenced only as existing in "future rulemaking to establish appropriate disincentives"), providers should focus on implementation of the necessary changes to their operations. It remains to be seen whether the current April 2021 implementation date is maintained or deferred, but health care providers should not delay their efforts to work toward compliance with the regulations.

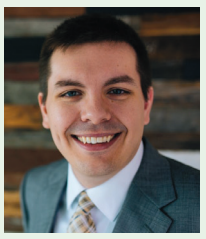
Read the article at www.bricker.com.

JOIN THE CBA FOR A SERIES ALL ABOUT CYBERSECURITY, COVERING CAUSES AND SOLUTIONS TO CYBERSECURITY CHALLENGES IN AN EVER-EVOLVING DIGITAL LANDSCAPE: CBALAW.ORG

IT'S NOT ME, IT'S YOU: THIRD-PARTY CYBERSECURITY VULNERABILITIES

You have hired the best IT team you can find. You invested in firewalls, anti-virus software, penetration testing and world-class intrusion detection systems. You train your staff monthly on security vulnerabilities, avoiding phishing scams and the importance of protecting their home office. Yet, with all these precautions and more, you overlooked one key gap: the vulnerability of third-party tools integrated into your systems and the systems of these third parties themselves.

As the recent Microsoft Exchange and SolarWinds data breach incidents have shown, one of the greatest threats to enterprise cybersecurity is coming from outside the house. Businesses often implicitly trust their third-party data processors and suppliers of software and hardware to be aware of and protect against security vulnerabilities.



JOSH STEVENS, ESQ.,
Mac Murray & Shuster LLP

For the most part, these processors and suppliers have every market incentive to protect data – a breach tied to their services can be ruinous. By the same token, a third-party vulnerability that exposes your company's data can harm consumers, reveal trade secrets, expose the business to regulatory penalties and lawsuits, and, importantly, tarnish the brand you have worked so hard to cultivate.

What can you do to help protect your business?

Do your homework
Before engaging any third-party data processor or integrating software or hardware from a third-party supplier, conduct due diligence on the security of the product and the policies and procedures the vendor has in place to protect its systems, identify and remediate security vulnerabilities, and respond to security breaches.

Seek experienced counsel in negotiating
Work with counsel to negotiate strong data security standards, data use limitations, security incident reporting, breach coordination, and indemnification and defense provisions into your contract.

Incorporate into your own processes
Update internal risk assessments and security strategies to account for the third party's contributions and monitor continuously.

No business can ever eliminate all security vulnerabilities, but by taking these important steps your business will be well positioned to reduce the risk of using third-party processors and suppliers.