Cybersecurity Program Safe Harbor – A Physician's Perspective

By J. Ryan Williams, Esq., Brouse McDowell

There is no question that a data breach involving patient data will likely wreak havoc on a physician's practice. A physician will need to deal with the immediate concerns, such as trying to regain access to data after a ransomware attack, making sure hackers no longer have access to a network, or immediately notifying patients. A physician will also experience the anxiety of whether patients will leave the practice. And, finally, a physician will probably face government scrutiny and may even be the subject of patient lawsuits.

Everyone knows that the best approach to preventing a data breach is to proactively review data systems and implement reasonable safeguards designed to maintain the integrity and security of patient data. Unfortunately, despite a proactive approach, data breaches and other security incidents happen. A new law in Ohio seems to recognize the inevitability of dealing with a data breach and provides some peace of mind, albeit unknown at this point, that good faith attempts to try to avoid a data breach are not an exercise in futility.

This new Ohio law, which went into effect on Nov. 2, 2018, is known as The Cybersecurity Program Affirmative Defense. This law essentially creates a legal safe harbor against tort liability arising from a data breach. The legislative intent is clear—the law is simply an incentive to encourage voluntary action to achieve a higher level of cybersecurity. The law does not create new standards or impose any liability or obligation on organizations to implement or maintain a particular cybersecurity practice.

To qualify for this safe harbor, a physician must create, maintain and comply with a written cybersecurity program that satisfies two requirements. First, the written cybersecurity program must meet the law's design, scale and scope requirements. Second, the written cybersecurity program must conform to a recognized industry framework.

With respect to the design of the cybersecurity program, the law requires that the program must protect the security and confidentiality of the physician's electronic data, guard against anticipated threats or hazards to the security or integrity of the electronic data, and guard against unauthorized access to or acquisition of the electronic data. Under the law's scale and scope requirements, a cybersecurity program is appropriate if it is based on the size and complexity of the physician's practice, the nature and scope of the physician's activities, the sensitivity of the information to be protected, the cost and availability of tools to improve security and reduce risks, and the resources available to the physician in implementing the cybersecurity program.

In addition to the requirements of the law, the cybersecurity program must reasonably conform to an industry recognized framework. Not surprisingly, one such framework is the Security Rule under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). If a cybersecurity program reasonably conforms to the standards set forth in the HIPAA Security Rule, it will be deemed to have satisfied the law's industry recognized framework requirement.

On first impression, the law's safe harbor is definitely welcome, but its practical application is largely unknown. For physicians responding to a data breach, the potential liabilities that present themselves typically revolve around notifying patients (and providing patients with useful options to shield any negative outcomes from the breach; ie, credit monitoring, ID theft protection, etc.) and responding to government investigations. This is mainly because HIPAA does not include a private right of action (the law, like HIPAA, also does not create a private right of action). While Ohio law does recognize a private breach of privacy claim (which is a tort) in limited situations, breach of privacy claims are typically reserved to class action lawsuits involving hundreds if not thousands of affected patients. Not often are physicians subject to one-off patient lawsuits as the result of a data breach.

In addition, the safe harbor seems to have limited application, especially as the cybersecurity practices of physicians and other healthcare providers continue to evolve. The safe harbor applies when a data breach involves a person's personal or restricted electronic information. One component of the definition of "personal or restricted information" is encryption. If the information is encrypted, the safe harbor does not apply. This encryption component is consistent with HIPAA's breach notice rule, so it should not come as a surprise to physicians. However, encryption of data is becoming the standard and not the exception. Thus, the safe harbor would presumably never come into play for a physician who has taken the steps to properly encrypt patient data at all stages.

For physicians, the relationship between the law's design, scale and scope requirements, and the industry framework condition is important. On initial review, the design, scale and scope requirements of the law seem redundant. Under the HIPAA Security Rule, physicians are required to conduct security risk assessments in connection with implementing the Security Rule's technical, administrative and physical safeguards. The risk assessments required under the Security Rule include most of the components of the law's design, scale, and scope requirements. For example, a physician conducting a security risk assessment for purposes of the HIPAA Security Rule must take into account the physician's size and complexity, the nature and scope of the physician's activity and the resources available to the physician in implementing the safeguards of the HIPAA Security Rule. As such, a reasonably compliant HIPAA compliance plan that conforms to the HIPAA Security Rule, which requires an annual security risk assessment, should satisfy most, if not all, of the law's design, scale and scope requirements.

If nothing more, the law is likely to advance the intent of the Ohio General Assembly to incentivize and encourage physicians to remain diligent in their efforts to maintain a robust HIPAA compliance plan, including the implementation of safeguards under the HIPAA Security Rule designed to protect the security and integrity of electronic patient data. Nevertheless, it's too early to determine if the law will have any practical benefits to physicians. ■