STRADLEY RONON

# Client Alert

A Publication of Stradley Ronon's
Cyber & Privacy and Health Care Practice Groups

WWW.STRADLEY.COM

FEBRUARY 13, 2019

Stradley Ronon Stevens & Young, LLP
2005 Market Street
Suite 2600
Philadelphia, PA 19103-7018
215.564.8000 Telephone
215.564.8120 Facsimile
www.stradley.com

With other offices in:
Washington, D.C.
New York
New Jersey
Illinois
Delaware



## Caution: Failure to Implement 'Voluntary' Health Care Cybersecurity Practices May Have Legal Ramifications

*by Kristin J. Jones and Samantha Kats*

Cyberattacks are becoming more prevalent and more sophisticated, and the health care industry, with its voluminous and valuable health records, continues to be a popular target. Given the increased frequency of cyberattacks, it is no surprise that health care cybersecurity remains a top priority of the U.S. Department of Health and Human Services (HHS). Cyberattacks not only disrupt an organization's business and cause reputational harm, but also put patients' identities at risk and can cost organizations millions of dollars. According to the Ponemon Institute's 2018 Cost of a Data Breach Report, the average health care data breach costs $408 per record, the highest of any industry for eight consecutive years.[1]

HHS recently released its four-volume guidance addressing cyberattacks, titled "Health Industry Cybersecurity Practices (HICP): Managing Threats and Protecting Patients," setting forth voluntary health care cybersecurity standards for all organizations in the health care sector.[2] Over 150 health care and cybersecurity leaders contributed to the HICP, which addresses cybersecurity needs based on the size of the organization and includes a variety of tips and useful resources. The HICP, among other things, summarizes the most common cybersecurity threats affecting health care and public health, identifies weaknesses that make organizations more vulnerable to cybersecurity threats, and shares best practices that organizations can implement to mitigate such threats, depending on an organization's size and complexity.

It is critical for organizations in the health care sector, regardless of size, structure and complexity, to review and strengthen their security systems, policies and procedures to more effectively block cyberattacks and protect their data. Although the guidance is "voluntary," ignoring the guidance could still have legal ramifications, especially for organizations in Pennsylvania.

### Although Voluntary, Could Redefine Standard of Care

In *Dittman v. UPMC* [3] (https://www.stradley.com/-/media/files/publications/2019/02/dittman-v-upmc.pdf?la=en&hash=25A4BA6527639C35B0A66AED8D531AF6), the Pennsylvania Supreme Court recognized – in the data breach context – a common law duty to safeguard against an unreasonable risk of harm in collecting and storing personal and financial information on an organization's computer systems. (See our prior coverage here https://www.stradley.com/insights/publications/2018/12/data-breach-response-december-6-2018). The court held, with respect to the "duty" element of a negligence claim, that the criminal acts of third parties do not relieve an organization from its duty to protect employees' personal and financial information from a data breach. The court further held that Pennsylvania's economic loss doctrine permits recovery on a negligence claim for "purely pecuniary damages" when there is a breach of a duty to safeguard sensitive personal

information on an internet-accessible computer system, as long as the breach of duty is independent of any contractual duties existing between the parties.

Although the HICP is voluntary, whether an organization followed its suggested practices may determine whether an organization acted reasonably to fulfill its duty to safeguard sensitive personal information on its systems. Organizations that fail to consider or implement suggested cybersecurity practices suitable for their organization will have a difficult time establishing that they met the standard of care and, depending on the extent of the breach, could result in a damages award in the millions, which could ultimately put the organization out of business.

The HHS Office for Civil Rights (OCR) will likely refer to the best practices and policies outlined in the HICP when auditing covered entities and their business associates. HIPAA's Security Rule requires covered entities and business associates to implement "reasonable and appropriate" safeguards to protect health information. The HICP provides new guidance about what may constitute reasonable and appropriate safeguards. Compliance officers, risk managers and privacy officers should use the HICP to evaluate whether their policies and procedures meet the standards for the security of protected health information. Organizations that rely on and take advantage of the resources and tips set forth in the guidance will be in a better position to prove their compliance with HIPAA during an audit.

## Takeaways

Organizations in the health care sector should take advantage of this guidance and view it as an opportunity to bolster their cybersecurity practices. This is an opportunity for organizations to revisit their policies and procedures, reinforce any weaknesses, and implement new processes or technologies that may be warranted. For the reasons discussed above as well as many others, it is crucial to engage a law firm like Stradley Ronon, whose attorneys are skilled at effectively and efficiently reviewing, advising on, drafting and implementing such policies and procedures and are experienced in avoiding and defending against related legal claims.

**Kristin J. Jones, CIPP/US** **Samantha Kats**

*For more information, contact Kristin J. Jones at 484.323.1355 or kjones@stradley.com or Samantha Kats at 484.323.1354 or skats@stradley.com.*

---

[1] Donovan, Fred, "Healthcare Data Breach Costs Remain Highest Among Industries." Health IT Security, available at https://healthitsecurity.com/news/healthcare-data-breach-costs-remain-highest-among-industries (last modified July 12, 2018).

[2] The guidance is available at https://www.phe.gov/Preparedness/planning/405d/Documents/HICP-Main-508.pdf.

[3] 196 A.3d 1036 (Pa. 2018).