SMITH ANDERSON
expectexcellence®

SMITH ANDERSON PARTNER DISCUSSES POSSIBLE HIPAA PENALTIES IN STORE FOR NATION'S NO. 1 CANCER CENTER WITH COMPLIANCE PUBLICATION

04.24.2019
COSMOS

In the *COSMOS* article, "**In Appeal, MD Anderson Says HIPAA Penalties Don't Apply Because It's a State Agency**," Smith Anderson partner **Joe Dickinson** comments on Texas-based MD Anderson Cancer Center's dispute over whether it should be required to pay civil monetary penalties (CMP) for violating HIPAA privacy or security regulations. According to *U.S. News & World* Report's "Best Hospitals" survey, MD Anderson has been ranked the number one hospital for cancer care in the nation in 2018-2019.

In MD Anderson's April 9 appeal of a $4.3 million penalty stemming from breaches caused by unencrypted thumb drives and a laptop, the cancer center stated that CMPs don't apply to "states and state agencies" such as itself because they were not included in the 1996 HIPAA statute. In fact, MD Anderson contends, the HHS Office for Civil Rights (OCR) overstepped its authority by adding them to the HIPAA regulations. It also added that the penalty, which was upheld in 2018 by an administrative law judge, exceeds statutory caps on HIPAA violations.

In the article, Joe emphasizes how this case illustrates how easily the need for encryption can fall through the cracks at large health systems. "They have so many assets – laptops, phones, thumb drives and pagers – that need to be encrypted that the human resources needed to make that happen can be prohibitive," he says. "They probably don't even have an accurate list of all devices with protected health information." Joe added that health systems make themselves more vulnerable by developing policies and procedures without ensuring they're implemented and followed.

Noting MD Anderson's appeal also contended that encryption is an "optional" standard, Joe says optional and addressable aren't the same thing and is sometimes lost on covered entities. "It's true that HIPAA doesn't require encryption – it's addressable," he says. However, Joe elaborates that covered entities have to assess whether addressable specifications in the security regulation are reasonable and appropriate, implement the specification, come up with a "reasonable and appropriate" alternate security measure, or do neither if they document why. "In theory you can do a thorough risk assessment and [determine] no alternative solution is reasonable and appropriate (as to encryption), even though today you probably can't because the cost of encryption has come down. It would be tough to meet that burden," Joe contends. He concludes that, in this case, that shouldn't apply to MD Anderson because allegedly it decided encryption was appropriate, adopted a policy and developed an encryption plan, but never carried it out.

Acknowledging that encrypting all mobile devices is "aspirational," especially when employees disregard their privacy and security training, Joe says, "The simple reality is, the volume of data and number of devices and end points we need to control makes it tough to do. It's a challenge for large health care organizations because

health care is the number-one target for cyber hacktivists and hackers."

Joe leads Smith Anderson's Data Use, Privacy and Security practice and has more than 25 years of business and legal experience. His practice often involves advising technology companies, for which he helps clients to identify their risks and to design, implement and manage data privacy and security programs for their business. Joe is also a seasoned speaker on data privacy and cybersecurity topics, and he has presented at some of the nation's most prestigious technology conferences.

*To read the full article, click **here**.*

PRACTICE AREAS

Data Privacy

Intellectual Property