

# Taking Privacy to a New Level: Texas Lowers Reporting Threshold for Security Breaches By Sean Price Texas Medicine January 2020

---

 [texmed.org/TexasMedicineDetail.aspx](https://texmed.org/TexasMedicineDetail.aspx)

Computer security breaches throw a wrench into the workings of medical practices and hospitals. Joseph Schneider, MD, a Dallas pediatrician and chair of the Texas Medical Association's Committee on Health Information Technology, saw that first-hand a few years ago.

"One of my employees had a hospital-owned computer with 800 names from a previous practice where [that employee] worked," Dr. Schneider said. "The computer got stolen, and it wasn't encrypted."

The employee and hospital staff spent hundreds of hours investigating how many patients were involved in the breach to determine whether they had to report it immediately to the U.S. Department of Health and Human Services Office for Civil Rights. Breaches involving 500 or more individuals must be reported within 60 days ([tma.tips/BreachNotices](https://tma.tips/BreachNotices)).

"The IT security folks had to figure out from backups whose information was in those files and how many there were," Dr. Schneider said. "It was a huge undertaking – far, far, far more expensive than encrypting and securing the computer."

The federal requirements have not changed, but starting Jan. 1, breach notification requirements will become even more stringent for Texas physicians or medical entities. The Texas Legislature dropped the threshold for breach reporting from 500 patients to 250. House Bill 4390 also requires medical entities to report breaches to the Texas attorney general's office within 60 days of the breach.

"That's a new development," says Troy Alexander, TMA associate director of advocacy. Not only is the threshold lower, "it's new reporting because it's not just [reporting] to the federal office about the breach. Reports on breaches also go to the [state] attorney general now."

It's too early to say how the new state threshold will affect Texas practices and hospitals, Dr. Schneider says. The change will probably cause a small uptick in the number of breaches reported overall.

"In this day and age, with electronic records, when there's a breach, it's generally a big breach," he said. "But I suspect that there are some breaches in that 250-to-500 range that will be triggered."

HB 4390 also established the Texas Privacy Protection Advisory Council to study and evaluate state, national, and international data privacy laws and then recommend to state officials specific changes by Sept. 1. The 15-member council, to which Dr. Schneider was appointed in November 2019, must include a representative from the medical profession.

Lawmakers created the council to keep Texas up-to-date on legal developments in personal privacy, Dr. Schneider says.

“It’s important to have an advisory group that is able to harmonize [privacy laws] so that we’re not making things so complex that it’s impossible to accomplish it. ... Whatever comes out of this [should be] as protective of privacy as it needs to be, but also as supportive of practice efficiency and effectiveness as it can be,” he said.

Data breaches have risen sharply over the past few years as more physicians use electronic medical records, according to the *HIPAA Journal*. In August 2019, health care data breaches of 500 or more records continued to be reported at a rate of more than 1.5 per day, or about 49 per month total, which was around twice the monthly average in 2018, the journal said. By September, the number of breaches had declined to 36 for the month, but the number of records compromised had actually risen 168%.

TMA has strong policy in support of protecting patient information ([www.texmed.org/TMAMedicalPrivacy](http://www.texmed.org/TMAMedicalPrivacy)).

Some physicians view all the work they do on privacy protection as a distraction from practicing medicine, Dr. Schneider says. But it’s essential, given the universal presence of computers, smart phones, and other devices that can be hacked.

“Having your identity stolen is a horrible experience, and as physicians we should be supportive of these efforts” by state lawmakers to improve privacy, he said. “In our practices we should be reinforcing with patients that their health information should be protected as they get access to more of it.”

Tex Med. 2020;116(1):28-29  
January 2020 *Texas Medicine* Contents  
*Texas Medicine* [Main Page](#)

## Resources: Computer Security

### TMA HIPAA Resource Center:

[www.texmed.org/hipaa](http://www.texmed.org/hipaa)

### HIPAA Gap Analysis and Training from TMA Practice Consulting:

[www.texmed.org/HIPAAConsulting](http://www.texmed.org/HIPAAConsulting)

### The Office of the National Coordinator free Security Risk Assessment Tool:

[tma.tips/SecurityAssessmentTool](http://tma.tips/SecurityAssessmentTool)

### Free CME for TMA members:

### HIPAA Security: Compliance and Case Studies

[tma.tips/HIPAASecurity](http://tma.tips/HIPAASecurity)

## Last Updated On

---

January 02, 2020

## Related Content

---

HIPAA

## Sean Price

---

## Reporter

---

(512) 370-1392

[sean.price\[at\]texmed\[dot\]org](mailto:sean.price[at]texmed[dot]org)

Sean Price is a reporter for *Texas Medicine* and *Texas Medicine Today*. He grew up in Fort Worth and graduated from the University of Texas at Austin. He's worked as an award-winning writer and editor for a variety of national magazine, book, and website publishers in New York and Washington. He's also helped produce Texas-based marketing campaigns designed to promote public health. Sean lives in Austin and enjoys hiking, photography, and spending time with his wife and two sons.



More stories by Sean Price