Compliance Corner

HIPAA: Ignore at Your Peril

by Michelle DeBarge and Jody Erdfarb

In the ever-changing landscape of health-care laws and regulations, it has become increasingly difficult for dental providers to keep pace with requirements. Our new column, "Compliance Corner," offers AACA members an opportunity to ask our legal counsel questions and learn from the questions of others.

Michelle DeBarge and Jody Erdfarb are attorneys at Wiggin and Dana LLP, the AACA's regulatory and compliance counsel. Wiggin and Dana's health-care compliance team regularly counsels clients on compliance with HIPAA and other federal and state statutes and regulations, as well as contractual, corporate, and transactional matters. Wiggin and Dana LLP is currently offering AACA members a discounted rate for model HIPAA policies and individual counseling sessions. Please contact Jody Erdfarb at JErdfarb@wiggin.com for more information.

Dear Compliance Corner,

Does our midsize dental practice really have to take HIPAA seriously? Maybe I am worrying about this too much when we have other priorities to attend to. What is the likelihood that we would ever be audited or investigated for failing to implement HIPAA's requirements?

From
A HIPAA-chondriac

Dear HIPAA-chondriac,

Unfortunately, HIPAA enforcement has been on the rise and has recently become more aggressive than ever. If you had asked this question 10 years ago, I might have joked that your "HIPAA-chondriac" pen name was justified because there was little to no enforcement activity.

However, all of that changed with the enactment of the Health Information Technology for Economic and Clinical Health (HITECH) Act in 2009, when the HIPAA enforcement authority of the federal and state government, and the fines for HIPAA violations, increased substantially.

Whereas enforcement used to be primarily complaint driven, the United States Department of Health and Human Services' Office for Civil Rights (OCR) now proactively investigates and audits compliance. While OCR traditionally resolved investigations by merely requiring corrective action, it now imposes significant monetary penalties. Even a technical HIPAA violation could result in millions of dollars in penalties, even if there was no bad intent and even if, exercising reasonable diligence, the entity could not have known about the violation.

2016 was a record-breaking year in federal HIPAA enforcement activity. OCR entered into 13 resolution agreements for HIPAA violations. In comparison, there were only 6 OCR enforcement actions in each of 2015 and 2014. Moreover, OCR collected about $23 million in fines in 2016; the previous annual record was $7.4 million in 2014. In 2016, OCR also imposed the largest penalty ever assessed for HIPAA noncompliance when Advocate Health Care System agreed to pay $5.5 million to settle the government's allegation that it violated HIPAA by failing to adequately safeguard patient information. Advocate had self-reported the theft of 5 laptop computers and a breach of its patients' information by the contractor that was providing Advocate with consulting and billing services.

There have already been 9 resolution agreements in 2017, including a settlement for $5.5 million with Florida's Memorial Healthcare System. It might still be too early to tell, but so far, those hoping that HIPAA enforcement would slow down significantly under the Trump administration have been sorely

"Those hoping that HIPAA enforcement would slow down significantly under the Trump administration have been sorely disappointed."

disappointed—the majority of the 2017 settlements were announced after the appointment of new OCR director Roger Severino in late March.

Size doesn't matter

In addition, when it comes to HIPAA enforcement, size does not matter. OCR has pursued small providers for HIPAA violations before and indicates that it will not hesitate to do so again. Prior OCR Director Leon Rodriguez explicitly stated that he intended to send "a strong message to the health care industry that, regardless of size, covered entities must take action and will be held accountable for safeguarding their patients' health information." While HIPAA's Security Rule allows entities of different sizes to tailor compliance based on their size, OCR will pursue violators of all sizes.

For example, in April of 2016, a midsize orthopedic clinic in North Carolina agreed to pay $750,000 to settle the government's allegation that it violated HIPAA by failing to execute a business associate agreement prior to turning over the x-rays and personal health information of patients to a vendor that was contracted to transfer the images to electronic media. Also for example, in February 2016, a physical therapy provider in California agreed to pay $25,000 to resolve the government's allegation that it violated HIPAA by posting patient testimonials, including full names and full-face photos, to its website without obtaining HIPAA-compliant authorizations.

Indeed, in 2016 OCR explicitly announced its initiative to "more widely" investigate breaches affecting fewer than 500 individuals. In an email message posted to the OCR Privacy list server, OCR explained that its regional offices at that time investigated all reported breaches involving the health information of 500 or more individuals, but only investigated reports of smaller breaches "as resources permit." OCR announced that it "has begun an initiative to more widely investigate the root causes of breaches affecting fewer than 500 individuals." Each regional office would retain discretion to prioritize which smaller breaches to investigate, but would increase efforts to obtain corrective action to address noncompliance. While there has not yet been an OCR HIPAA enforcement action involving a dental provider, there is no doubt that dental practices that have not implemented a robust HIPAA compliance program are putting themselves at grave risk.

A multi-pronged attack

Keep in mind that OCR is not the only sheriff in town. Each state attorney general has the authority to enforce HIPAA, and they have not been shy about doing so. Other federal agencies, such as the Federal Trade Commission (FTC), have also used their authority to investigate and impose penalties when there have been security breaches or other privacy violations.

Disgruntled employees are often the ones to file complaints with government agencies, instigating costly and aggravating investigations, but patients themselves have become more aware of their privacy rights and have been increasingly willing both to report suspected violations to the government and to file lawsuits directly as well, using alleged HIPAA violations as the basis for their state law claims.

If the answer to your question is not yet clear, let's be explicit: Yes, a midsize dental practice really must take HIPAA compliance seriously. While the HIPAA regulations may seem overwhelming, compliance is achievable, and a little effort goes a long way. Conducting a risk analysis, establishing HIPAA policies, training staff, and reviewing contractor relationships are simple steps that providers can take. Every practice prioritizes where to expend limited resources, but if you have relegated HIPAA to the bottom of your list, it may be time to reprioritize. ■

"Disgruntled employees are often the ones to file complaints with government agencies, instigating costly and aggravating investigations."