The Journal of the Michigan Dental Association

Volume 106 | Number 2 Article 4

2-1-2024

Dentistry and the Law: When Must a Data Breach be Reported?

Dan Schulte JD
Kerr Russell, dschulte@kerr-russell.com

When Must a Data Breach be Reported?

By Dan Schulte, JD
MDA Legal Counsel

Question: My practice billing person recently missed some time due to an illness. She was a few weeks behind in processing claims. She took home a thumb drive loaded with patient records so that she could work on getting caught up over a weekend without having to come into the office. The thumb drive disappeared. She claims she last saw it in a pile of papers at home on her dining room table where she was working and fears she accidentally threw it in the trash with the pile of papers by accident. Is this a HIPAA data breach? Do I need to report this to someone?

Answer: The HIPAA Breach Notification Rule, 45 CFR §§ 164.400-414, requires HIPAA-covered entities (including your dental practice) and their business associates to provide notification following a breach of unsecured protected health information. I will assume the thumb drive your biller took home contained protected health information. It is hard to imagine anyone would be able to process claims for payment without this type of information. I will further assume that the information was not encrypted, password protected, etc.

Since we are dealing with missing unsecured protected health information, a data breach requiring reporting is required unless you determine that there is a "low probability" that the missing protected health information has been compromised. When determining whether the probability is low you must make an assessment based on: (1) the nature and extent of the protected health information involved; (2) whether the protected health information was actually acquired or viewed by an unauthorized person(s) and what is known about that person(s); and (3) the extent to which the risk of disclosure of the protected health information can be or has been mitigated.

In your case, a judgment call must be made. There seems to be a low probability that the information on the missing thumb drive has been disclosed. This is because it went straight to your biller's home, it appears to have been misplaced there, and there is no indication that it is in the possession of an unauthorized person. You must document this risk assessment in writing.

If you are not comfortable concluding that there is a low probability of improper disclosure, you must determine which types of notification must be made. Individual notice and notice to the U.S. secretary of Health and Human Services is always required in such an instance.

Individual notice must be made to all patients whose protected health information was on the thumb drive. This notice must be in writing and be made by first-class mail without unreasonable delay and in no case later than 60 days following the discovery of a breach. This individual notice must include a description of how the breach occurred, the information involved, the steps affected individuals should take to protect themselves from potential harm, and what the covered entity is doing to investigate the breach, mitigate the harm, and prevent further breaches.

Notice to the secretary of Health and Human Services can be done electronically on the HHS website by filling out and electronically submitting a breach report form. You can find the form at hhs.gov/hipaa — search for "submitting notice of a breach to the secretary." If the breach affects 500 or more individuals, you must notify the secretary without unreasonable delay and in no case later than 60 days following the breach. If the breach affects fewer than 500 individuals, you may notify the secretary on an annual basis, no later than 60 days after the end of the calendar year in which the breaches are discovered.

If the breach affects more than 500 individuals, you must provide public notice using prominent media outlets in addition to the individual notice and notice to the secretary of Health and Human Services. ●

Editor's note: The MDA offers cyber liability and data breach insurance through specialty insurer Beazley. Visit mdaprograms.com and click on MDA Insurance Programs.