COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 18, Number 8. August 31, 2018 Breach or No Breach, Sensitive Data Demand Special Attention, Safeguards

By HCCA Staff

The exposure of a database of thousands of Tennessee residents with HIV/AIDS on a server accessible to nearly 500 health department employees may not be a reportable breach, either under federal or state law, attorneys say. But the circumstances still offer lessons for how covered entities (CEs) beyond public health agencies should handle similarly sensitive data.

According to an investigation by *The Tennessean,* the Nashville Metro Public Health Department HIV/AIDS database—which contained names, addresses, Social Security numbers and health information such as lab results—resided for nine months unencrypted on a server accessible to the entire agency.

An employee moved the database to the server so that a researcher could access it, according to *The Tennessean*, but the researcher never accessed or utilized the data. Metro Health officials said in statements to *The Tennessean* that they don't believe the database was accessed improperly while it was on the unsecured server. However, there's no way to know for certain, because the server did not have features that would have monitored access or logged attempts to copy the data. Metro Health officials did not respond to phone messages from *RPP*.

David Holtzman, vice president, compliance strategies for CynergisTek Inc., says he's been unable to find a requirement to report this occurence as a breach in either federal or state regulation. "This incident points to the true vacuum that we have in federal and state requirements regarding notification to individuals when there has been a compromise of data that contains their sensitive health information when it's held by a business or a government agency," he says.

"The [Nashville Metro Public Health Department] has provided a limited amount of information about this incident, and in light of the information that has been made publicly available, it would be difficult to make definitive conclusions on what, if any, federal or state law would require notification," adds Holtzman. "However, there are no federal or state requirements that appear to compel notification in this instance."

No Monitoring, No Breach?

The Tennessean reported that the server where the data was stored did not have monitoring or access logging capability enabled. Metro Public Health said in statements to *The Tennessean* that it didn't consider this a HIPAA breach because it didn't appear that the database had been accessed, despite the fact that it had been left open to all 500 agency employees.

Holtzman says that "according to the reporting by *The Tennessean*, the Metro Public Health had policies and procedures which should have prohibited this. However, they had no safeguards in place that prevented or detected the impermissible movement of the data to the unsecured shared drive."

Still, Holtzman says this situation may in fact not be a HIPAA breach. It also may not be a breach under state law, he says, noting, "The fact here is the failure of Metro Public Health to have monitoring in place means there is no proof that the data has been acquired by an unauthorized person. So their lack of having in place appropriate

minimum safeguards shields them from the requirements of the state law specially designed to protect this type of information."

"A review of Tennessee's breach notification law finds that notification is required" of a breach, Holtzman says, but "it defines a breach of a secure system as the 'unauthorized acquisition of unencrypted computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the information holder.'" Holtzman adds: "Tennessee's law goes on to require notification only when unencrypted information is or is reasonably believed to have been acquired by an unauthorized person."

Richelle Marting, an attorney with the Forbes Law Group in Overland Park, Kansas, agrees that this may not be a reportable breach.

"You always look at HIPAA's definition of a breach in these situations," says Marting. "First, HIPAA presumes that an unauthorized access is a breach unless you can confirm a low probability the privacy or security of information has been compromised. So a very important preliminary determination involves whether there has in fact been inappropriate access. Here, Metro Public Health is likely weighing the fact that they don't believe the database was accessed inappropriately as a key factor in their decision."

Another factor is considering who may have had access to the database. "It appears that if someone had accessed it without permission, that person would have been an employee of the [health] department. That's different than a situation when the database is inadvertently made available to the public, for example, because their staff have probably received privacy and security training on how to protect information they come across in their jobs," she says.

Marting adds, "You also weigh factors such as whether the information was actually viewed or accessed, as opposed to merely an opportunity to view or access the information, to whom the use or disclosure was made, the nature and extent of the information, and the extent to which the risk to the information has been mitigated. If, by looking at those factors, you can determine there is a low probability the privacy or security of information was compromised, it does not have to be treated as a reportable breach."