

That's a violation of HIPAA! But is it...

August 26, 2021

By Sarah M. Sawyer

It has certainly been an eventful summer from the reopening of businesses and office spaces, talk of a fall “comeback” with many employers hoping to return the majority of their workforce to working in person or operating in a hybrid model, and the elimination of mask mandates to the reinstatement of mask mandates, a delta surge, increased vaccine mandates, and approval of the Pfizer vaccine. As we have learned over the last 18 months, there is never a dull moment when it comes to the COVID-19 pandemic.

Over the last month, I have seen a sharp increase in companies mandating vaccination in the workplace and organizations requiring proof of immunization or a negative COVID-19 test to attend meetings or events. With these increases in mandatory policies, I have also been fielding many questions regarding HIPAA compliance. Namely, what do we need to do to comply with HIPAA when requesting and obtaining medical information, such as vaccination status?

Well, I am here to set the record straight-HIPAA probably doesn't apply to your business.

The Health Insurance Portability and Accountability Act of 1996, better known by its acronym, “HIPAA,” is a federal law that created national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. Since this law covers patients, it only applies to healthcare providers, health plans, healthcare clearinghouses (“Covered Entities”), and business associates acting on behalf of these Covered Entities. HIPAA does not cover businesses that are not in healthcare or acting on behalf of healthcare entities.

While HIPAA does not cover most businesses who call me with questions regarding HIPAA compliance, that does not mean they are not responsible for keeping medical information confidential and keeping it secure and out of the wrong hands. When it comes to protecting confidential medical information, other federal, state, and local laws likely apply. For example, when it comes to employees, under the Americans with Disabilities Act (ADA), employers are required to keep all employee medical information confidential and keep it in a confidential medical file separate from the employee's personnel file. There are also laws, such as the Family Education Rights and Privacy Act (FERPA), that protect the medical information of elementary, secondary, and post-secondary students.

While asking whether HIPAA applies is not technically relevant to most companies or organizations, the question has become a colloquial way of asking what they should do with confidential information to stay out of trouble, which is a thoughtful and necessary question. Ultimately, when obtaining or storing personal medical information of employees, clients, or event attendees, companies and organizations need to check federal, state, and local regulations to ensure compliance.