WILMERHALE

A public service announcement about the HIPAA Privacy Rule

June 18, 2021

HIPAA and COVID-19 have been in the news together a lot lately. Most of what you see is wrong. Here's a refresher — for yourself, and your strange friend who read something on the internet and is now a HIPAA expert or, all too frequently, a "HIPPA" expert.

First, HIPAA is not an overall health information privacy rule. The name of the statute may give some clues — the Health Insurance Portability and Accountability Act. The single "P" in the name is for portability, not privacy. Neither privacy nor security is in the name. The HIPAA Privacy Rule — drafted by the U.S. Department of Health and Human Services after the statute was passed — applies ONLY to specific "covered entities," meaning certain health care providers: doctors, pharmacies and hospitals, health plans (health insurers and government health programs) and health care clearinghouses. This limitation means there is a lot of health-related information not subject to HIPAA because there is no relevant "covered entity" involved.

Second, HIPAA never applies if a company — a store, an airplane, a concert venue, an amusement park, a sporting venue, etc., — asks you about your health status. There may be other relevant laws, but HIPAA essentially never applies here. HIPAA simply does not prevent these companies from asking about your COVID-19 status or your vaccination status.

Third, HIPAA does not apply if your employer asks you about your vaccination status. Employers who provide health insurance benefits to their employees may have some obligations in connection with HIPAA. However, these obligations apply only where health information is obtained by the employer through the health insurance program. So, if a company went to their health insurer and said, "which of our employees submitted claims related to COVID-19 treatment?" HIPAA would apply. Hint: Virtually no employer ever does this. If they asked the health insurer "who among our staff has been vaccinated," not only would they never do that, but the resulting information — if the health insurer would provide it — would be useless. How many of you submitted health insurance claims for your vaccination? Crickets. No one did.

Fourth, HIPAA still provides important privacy protections. You should understand both where HIPAA applies and where it does not. When you go to the doctor — at least most doctors, but that's another story — or have surgery at a hospital or obtain health insurance, HIPAA protects your personal data. It protects that data when the hospital or health insurer has it, when they exchange that information for appropriate purposes with other health care entities, and when they share that information with a vendor who provides services to the hospital or health insurer. If your employer calls up your doctor and asks, "Did my employee test positive for COVID?" the doctor is not allowed by the HIPAA Privacy Rule to respond.

Fifth, yes, HIPAA applies even if that vendor to the hospital is a technology company providing analytics services (they are called "business associates" and have both contractual obligations to their health care customer and legal obligations under the HIPAA rules). But, if that technology company also hosts social media data, or collects search terms, or allows you to post your own hot takes on HIPAA, that part isn't "on behalf of" a hospital or a health insurer and isn't subject to the HIPAA rules. That means when you post about your recent operation or your vaccination status on social media, that information – even if it is totally about your health — isn't subject to HIPAA.

HIPAA isn't perfect. Privacy and security was an afterthought when the statute was passed, so it isn't a well-thought-out set of overall health care privacy principles. No one would have started out with the idea of protecting the privacy of your health care information and ended up with HIPAA. Also, our society has evolved in many ways since the HIPAA law was passed in 1996, through technology and health care developments and in various other ways. But the Privacy Rule, in my humble opinion, after working with it daily for more than 20 years, does a very good job of protecting your privacy where it applies. It also permits the health care system overall to work relatively well by being both efficient and effective. But it doesn't provide this privacy protection where it doesn't apply. There may be other laws (and there are many other laws) that will protect your health information in certain other settings, and there are a variety of other regulators (like the U.S. FTC and state attorneys general) who care about protecting the privacy of health care information in these other settings.

But it is important to understand the volume of health care information collected and analyzed and processed is growing every day, and much of this data is outside the scope of protection of the HIPAA rules. COVID-19 exacerbated this trend because so much of the impact of COVID-19 data has been with entities not regulated by HIPAA.

So next time you are tempted to post something on Twitter, or argue with a store clerk, or otherwise loudly proclaim that "HIPAA prohibits this," think again. It might – but probably doesn't.

And whatever you do, please spell it right.

Contributors

Kirk J. Nahra

PARTNER

kirk.nahra@wilmerhale.com

+ 1 202 663 6128