



The Daily Dish

# HIPAA Just Wants to be Understood

CHRISTOPHER HOLT | AUGUST 18, 2021

One of the most frequently misunderstood areas of federal health law is the Health Insurance Portability and Accountability Act (HIPAA) and its related regulations and succeeding legislation. These misunderstandings have multiplied during the COVID-19 pandemic, as individuals, politicians, and businesses have misconstrued and misapplied HIPAA, often with little knowledge of the law's actual requirements.

Last month Dallas Cowboys quarterback Dak Prescott generated [headlines](#) when he implied that a reporter's question about his vaccination status was a HIPAA violation. More explicitly, Rep. Marjorie Taylor Greene [said](#) in response to a similar question, "You see, with HIPAA rights, we don't have to reveal our medical records, and that also includes our vaccine records." While neither Rep. Greene nor Mr. Prescott are under any obligation to answer reporters' questions about their health, such questions are not HIPAA violations. More pointedly, the Dallas Cowboys, Mr. Prescott's employer, would be within their legal rights to require that he provide proof of vaccination as a condition of his employment. This question of whether or not employers can require employees to disclose vaccination status has become so ubiquitous that the Department of Health and Human Services [addresses](#) it on its frequently asked questions page—spoiler alert, yes they can and no it isn't a HIPAA violation.

The reality, as Jake Griffin and I explain in our recent [Primer](#), is that HIPAA is far more limited in scope than generally understood, only applying to specified covered entities and business associates that work with protected health information (PHI). PHI is defined as "individually identifiable health information that includes demographic or health care information relating to the individual's past, present, or future physical and mental health." A business that does not handle PHI for its customers as a part of its function does not have to comply with HIPAA.

HIPAA was broader in scope than health privacy, but the primary aim of the privacy provisions was to revamp the way PHI was maintained by health care organizations and health care insurance companies, setting new standards to prevent health care fraud. Covered entities and business associates face significant penalties for mishandling PHI, up to \$1.5 million per year for each category of violation. But nothing in HIPAA prevents the corner store from requiring you to wear a mask, asking you to disclose what health condition precludes you from wearing a mask, or even requiring you to provide proof of vaccination.

Debates about masks, vaccines, employer mandates, employee rights and so on will continue for the foreseeable future; they aren't easy questions, and the legal framework isn't always clear. But please, please leave HIPAA out of it, HIPAA is tired of being misunderstood.