

HHS Issues FAQs on HIPAA Privacy & COVID-19 or Flu Vaccine Status

November 1, 2021

Quick Facts

- In September, the Department of Health and Human Services (HHS) released a set of frequently asked questions (FAQs) addressing Health Insurance Portability and Accountability Act (HIPAA) privacy requirements and employee vaccines.
- The FAQs address to whom the privacy rule applies, what constitutes protected health information (PHI) and permitted uses and disclosures of PHI.
- The FAQs provide examples of situations where a request for an individual's vaccination status does not implicate the HIPAA Privacy Rule.
- The FAQs state that once a covered entity has information regarding an individual's vaccination status, that information is considered PHI and the covered entity may only use or disclose that information as permitted by the Privacy Rule or with written authorization from the individual.

HHS HIPAA Privacy Rule Guidance

On September 30, 2021, the HHS issued a set of frequently asked questions addressing common issues and misconceptions related to employee vaccines and the HIPAA privacy requirements (the Privacy Rule).

In a series of five questions and answers, the FAQs clarify:

- The entities to which the Privacy Rule applies (covered entities, and to some extent, business associates);
- The difference between information that is considered protected health information (PHI) and other types of information (e.g., employment information); and
- How covered entities are permitted to use and disclose PHI under the Privacy Rule.

The FAQs begin by emphasizing that the Privacy Rule regulates “covered entities,” which includes health plans (including employer-sponsored health plans), providers, healthcare clearinghouses, and to some extent, business associates. The Privacy Rule does not regulate employers, and it does not regulate individuals.

Second, the FAQs clarify that no entity (whether a covered entity or not) is prohibited from asking about another person's vaccination status; therefore, employers may request this information from employees, and providers or other covered entities may request this information from individuals. The Privacy Rule *does* become implicated once a covered entity (e.g., a provider or a health plan) knows a person's vaccination status. At this point, that information is considered PHI and the provider or health plan is bound by the Privacy Rule's requirements with respect to how it may use or disclose that information. (With limited exceptions, a covered entity may only use or disclose an individual's

PHI for purposes of treatment, payment, or healthcare operations unless it first obtains written authorization.)

Below are examples of situations the FAQs outline where a request for an individual's vaccine status does not implicate the Privacy Rule:

- An individual is asked by a school, employer, store, restaurant, entertainment venue, or another individual about their vaccination status;
- An individual asks another individual, their doctor, or a service provider whether they are vaccinated;
- An individual asks a company (e.g., a home health agency) whether its workforce members are vaccinated.

Note that in each of these examples, other federal or state laws may come into play. The point of the FAQs is that the Privacy Rule does not apply.

The FAQs also emphasize that because the Privacy Rule does not regulate individuals, an individual is never prohibited from disclosing to another person or entity information about the individual's vaccination status. In other words, nothing prevents an individual from voluntarily sharing whether they have been vaccinated.

Moreover, because the Privacy Rule does not regulate employers, it does not generally prevent employers from asking their workforce for information (or requiring the provision of information), including health information, that is needed as part of the terms of condition of employment. This includes:

- Requesting or requiring existing or prospective employees to provide documentation of their COVID-19 or flu vaccination status;
- Requesting or requiring existing or prospective employees to sign a HIPAA authorization form for a provider to disclose the individual's vaccination record to their employer;
- Requiring employees to wear a mask while in the employer's facility, on the employer's property, or in the normal course of performing their duties at another location; and/or
- Requiring employees to disclose whether they have received a COVID-19 vaccine in response to queries from current or prospective patients.

Again, note that in each of these examples, other federal or state laws may come into play with respect to what information an employer can request, how the employer must maintain it, and what the employer is able to do with that information. The point of the FAQs is that the HIPAA Privacy Rule does not apply.

Finally, the FAQs emphasize that once a covered entity (e.g., a provider or a health plan) has information regarding an individual's vaccination status, that information is considered PHI and the covered entity may only use or disclose that information as permitted by the Privacy Rule or pursuant to written authorization from the individual who is the subject of the PHI. Generally, the Privacy Rule permits covered entities to use and disclose PHI for purposes of treatment, payment and healthcare operations; for certain public policy-related purposes; and as required by law¹. Covered entities may

¹ The FAQs provide an example of a situation where a hospital may disclose vaccine information to employers, so long as certain conditions are met, in order for the employer to comply with requirements of the Occupational Safety and Health Administration (OSHA), the Mine Safety and Health Administration (MHSA), or state law to conduct an evaluation relating to medical surveillance of the workplace (e.g., surveillance of the spread of COVID-19 within the workforce) or to evaluate whether the individual has a work-related illness.

also disclose PHI to the individual who is the subject of the PHI. For employer-sponsored health plans, this means that PHI may generally only be used or disclosed for purposes of plan administration (e.g., claims payment or utilization/case management) unless a legal or public policy exception applies or unless the disclosure is being made to the individual who is the subject of the PHI. PHI may not be used for any employment-related purposes. Therefore, while an employer may gather vaccination information directly from employees for employment-related purposes (in which case the information is not PHI), an employer would **not** be permitted to gather information from its health plan records and then use this information (which is PHI) for non-health plan purposes, such as hiring or termination.

EPIC Employee Benefits Compliance Services

For further information on this or any other topics, please contact your EPIC benefits consulting team.

EPIC offers this material for general information only. EPIC does not intend this material to be, nor may any person receiving this information construe or rely on this material as, tax or legal advice. The matters addressed in this document and any related discussions or correspondence should be reviewed and discussed with legal counsel prior to acting or relying on these materials.