

HIPAA, COVID-19 Vaccination, and the Workplace¹

The US Department of Health and Human Services has issued the following guidance around the application of the Health Information Portability and Accountability Act (HIPAA) to COVID-19 vaccination information in the workplace. This guidance is provided as a resource to help answer the many questions that have been raised around this issue.

1. Does the HIPAA Privacy Rule prohibit businesses or individuals from asking whether their customers or clients have received a COVID-19 vaccine?

No. The Privacy Rule² does not prohibit **any person** (e.g., an individual or an entity such as a business), including HIPAA covered entities and business associates, from asking whether an individual has received a particular vaccine, including COVID-19 vaccines.

First, the Privacy Rule³ applies **only** to **covered entities**⁴ (health plans, health care clearinghouses, and health care providers that conduct standard electronic transactions) and, to some extent, their **business associates**.⁵

Second, the Privacy Rule **does not regulate** the ability of covered entities and business associates to request information from patients or visitors. Rather, the Privacy Rule regulates how and when covered entities and business associates are permitted to use⁶ and disclose⁷ **protected health information**⁸ (PHI) (e.g., PHI about whether an individual has received a COVID-19 vaccine) that covered entities and business associates create, receive, maintain, or transmit. Thus, the Privacy Rule **does not prohibit** a covered entity (e.g., a covered doctor, hospital, or health plan) or business associate from asking whether an individual (e.g., a patient or visitor) has received a particular vaccine, including COVID-19 vaccines, although it does regulate how and when a covered entity or its business associate may use or disclose information about an individual's vaccination status.

Additional examples. The Privacy Rule **does not apply** when an individual:

- Is asked about their vaccination status by a school,⁹ employer, store, restaurant, entertainment venue, or another individual.
- Asks another individual, their doctor, or a service provider whether they are vaccinated.
- Asks a company, such as a home health agency, whether its workforce members are vaccinated.

Other state or federal laws address whether individuals are required to disclose whether they have received a vaccine under certain circumstances.

2. Does the HIPAA Privacy Rule prevent customers or clients of a business from disclosing whether they have received a COVID-19 vaccine?

No. The Privacy Rule does not prevent any individual from disclosing whether that individual has been vaccinated against COVID-19 or any other disease. The Privacy Rule does not apply to individuals' disclosures about their own health information. It applies **only** to **covered entities**[10](#) and, to some extent their **business associates**.[11](#) Therefore, the Privacy Rule does not apply when an individual tells another person, such as a colleague or business owner, about their own vaccination status.

3. Does the HIPAA Privacy Rule prohibit an employer from requiring a workforce member to disclose whether they have received a COVID-19 vaccine to the employer, clients, or other parties?

No. The Privacy Rule does not apply to employment records, including employment records held by covered entities[12](#) or business associates[13](#) in their capacity as employers.[14](#) Generally, the Privacy Rule does not regulate what information can be requested from employees as part of the terms and conditions of employment that an employer may impose on its workforce.[15](#) However, other federal or state laws do address terms and conditions of employment.[16](#) For example, federal anti-discrimination laws do not prevent an employer from choosing to require that all employees physically entering the workplace be vaccinated against COVID-19 and provide documentation or other confirmation that they have met this requirement, subject to reasonable accommodation provisions and other equal employment opportunity considerations.[17](#) Documentation or other confirmation of vaccination, however, must be kept confidential and stored separately from the employee's personnel files under Title I of the Americans with Disabilities Act (ADA).[18](#)

4. Does the HIPAA Privacy Rule prohibit a covered entity or business associate from requiring its workforce members to disclose to their employers or other parties whether the workforce members have received a COVID-19 vaccine?

No. The Privacy Rule does not apply to employment records, including employment records held by covered entities[19](#) and business associates[20](#) acting in their capacity as employers.[21](#) Thus, the Privacy Rule generally **does not** regulate what information can be requested from employees as part of the terms and conditions of employment that a covered entity or business associate may impose on its workforce,[22](#) such as the ability of a covered entity or business associate[23](#) to require its workforce members to provide documentation of their vaccination against COVID-19 or to disclose whether they have been vaccinated to their employer, other workforce members, patients, or members of the public.

For example, the Privacy Rule **does not prohibit** a covered entity or business associate from requiring or requesting each workforce member to:

- Provide documentation of their COVID-19 or flu vaccination to their current or prospective employer.

- Sign a HIPAA authorization for a covered health care provider to disclose the workforce member's COVID-19 or varicella vaccination record to their employer.[24](#)
- 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.
- Disclose whether they have received a COVID-19 vaccine in response to queries from current or prospective patients.

Other federal or state laws address whether an employer may require a workforce member to obtain any vaccinations as a condition of employment and provide documentation or other confirmation of vaccination. These laws also address how employers must treat medical information that they obtain from employees. For example, documentation or other confirmation of vaccination must be kept confidential and stored separately from the employee's personnel files under Title I of the Americans with Disabilities Act (ADA).

5. Does the HIPAA Privacy Rule prohibit a doctor's office from disclosing an individual's protected health information (PHI), including whether they have received a COVID-19 vaccine, to the individual's employer or other parties?

Generally, yes. The Privacy Rule prohibits covered entities[25](#) and their business associates[26](#) from using or disclosing an individual's PHI[27](#) (e.g., information about whether the individual has received a vaccine, such as a COVID-19 vaccine; the individual's medical history or demographic information) except with the individual's authorization or as otherwise expressly permitted or required by the Privacy Rule.

Generally, where a covered entity or business associate is permitted to disclose PHI, it is limited to disclosing the PHI that is reasonably necessary to accomplish the stated purpose for the disclosure.[28](#)

For example, if consistent with other law and applicable ethical standards, under the Privacy Rule:

- A covered physician **is permitted** to disclose PHI relating to an individual's vaccination to the individual's health plan as necessary to obtain payment for the administration of a COVID-19 vaccine.[29](#)
- A covered pharmacy **is permitted** to disclose PHI relating to an individual's vaccination status (e.g., that an individual has received a COVID-19 vaccination, the date of vaccination, the vaccine manufacturer) to a public health authority, such as a state or local public health agency.[30](#) In such situations, the covered pharmacy may rely, if such reliance is reasonable under the circumstances, on a representation by the public health authority that the information requested constitutes the minimum necessary for the stated purpose(s) of the disclosure (e.g., to track and compare the effectiveness of different COVID-19 vaccines).[31](#)
- A health plan **is permitted** to disclose an individual's vaccination status where required to do so by law.[32](#)
- A covered nurse practitioner **is permitted** to provide PHI relating to an individual's COVID-19 vaccination status to the individual.[33](#)

- A covered clinician who is an investigator in a COVID-19 vaccine clinical trial **is permitted** to use or disclose PHI to the vaccine manufacturer and FDA about clinical trial participants for the purpose of activities related to the quality, safety, or effectiveness of the COVID-19 vaccine.³⁴ Such purposes include:
 - To collect or report adverse events, product defects or problems (including problems with the use or labeling of a product), or biological product deviations.
 - To track FDA-regulation products, including COVID-19 vaccines.
 - To enable product recalls, repairs, replacement, or lookback (including locating and notifying individuals who have received products that have been recalled, withdrawn, or are the subject of lookback).
 - To conduct post-marketing surveillance.
- A covered hospital **is permitted** to disclose PHI relating to an individual’s vaccination status to the individual’s employer so that the employer may 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,^{35,36} **and** all of the following conditions are met:
 - The covered hospital is providing the health care service to the individual at the request of the individual’s employer or as a member of the employer’s workforce.³⁷
 - The PHI that is disclosed consists of findings concerning work-related illness or workplace-related medical surveillance.
 - The employer needs the findings in order to comply with its obligations under the legal authorities of the Occupational Safety and Health Administration (OSHA), the Mine Safety and Health Administration (MSHA), or state laws having a similar purpose (*e.g.*, under OSHA’s recordkeeping requirements, worker side effects from vaccination constitute a “recordable illness,” and thus, employers are responsible for recording such side effects in certain circumstances³⁸).^{39,40}
 - The covered health care provider provides written notice to the individual that the PHI related to the medical surveillance of the workplace and work-related illnesses will be disclosed to the employer. (This can be accomplished by providing the individual with a copy of the notice at the time the health care is provided, or by posting the notice in a prominent place at the location where the health care is provided if the health care is being provided on the work site of the employer.)⁴¹

In other circumstances, the Privacy Rule generally requires a covered entity to obtain an individual’s written authorization before disclosing the individual’s PHI,⁴² such as disclosure of whether the individual has received a vaccine, to, for example:

- A sports arena or entertainment purveyor.
- A hotel, resort, or cruise ship.
- An airline or car rental agency.

NOTE: The Privacy Rule **does not** prohibit an individual from choosing to provide any of these individuals or entities with information regarding their vaccination status.

For additional information on the Privacy Rule and its application, visit <https://www.hhs.gov/hipaa/for-individuals/index.html>.

Resources

The CDC issued “Updated Healthcare Infection Prevention and Control Recommendations in Response to COVID-19 Vaccination,” available at <https://www.cdc.gov/coronavirus/2019-ncov/hcp/infection-control-after-vaccination.html>.

OSHA, at the U.S. Department of Labor, published “Protecting Workers: Guidance on Mitigating and Preventing the Spread of COVID-19 in the Workplace”, available at <https://www.osha.gov/coronavirus/safework>. Additional guidance and resources on COVID-19 and the workplace, are available at <https://www.osha.gov/coronavirus>.

The U.S. Equal Employment Opportunity Commission issued guidance entitled, “What You Should Know About COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws,” available at <https://www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws>.

Footnotes

1. [\[1\]](#) The HHS Office for Civil Rights (OCR) is issuing these FAQs to address questions about when and how the HIPAA Rules apply to uses and disclosures of COVID-19 vaccination-related information. However, the information in the FAQs concerning the HIPAA Rules is applicable to all vaccinations, regardless of the disease or condition being addressed or whether the vaccine has been fully approved or authorized via an emergency use authorization (EUA).
2. [\[2\]](#) The “Privacy Rule” refers to the privacy regulations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA), 45 CFR part 160 and subparts A and E of part 164. OCR administers the HIPAA Privacy, Security, Breach Notification, and Enforcement Rules (collectively known as the HIPAA Rules), 45 CFR parts 160 and 164. This guidance focuses on the Privacy Rule, which regulates uses and disclosures of protected health information (PHI).
3. [\[3\]](#) The HIPAA Privacy, Security, and Breach Notification Rules, 45 CFR Parts 160 and 164.
4. [\[4\]](#) See 45 CFR 160.103 (definition of “Covered entity”). See also <https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html>.
5. [\[5\]](#) See 45 CFR 160.103 (definition of “Business associate”). See also Direct Liability of Business Associates Fact Sheet at <https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/business-associates/factsheet/index.html>. Examples of

business associates include health care claims processing services, medical transcriptionists, and accounting firms that have access to protected health information.

6. [☞](#) See 45 CFR 160.103 (definition of “Use”).

7. [☞](#) See 45 CFR 160.103 (definition of “Disclosure”).

8. [☞](#) See 45 CFR 160.103 (definition of “Protected health information”).

9. [☞](#) While the Privacy Rule does not regulate whether schools can ask individuals whether they have received a vaccine, the HIPAA Rules may regulate how the information is handled once it is in the possession of a school when that school is subject to the HIPAA Rules (*i.e.*, when the school is a covered entity) and the health information does not meet the definition of “education records” covered by the Family Educational Rights and Privacy Act (FERPA). See 45 CFR 160.103 excluding individually identifiable health information in education records covered under FERPA from the definition of “protected health information.” See also Joint Guidance on the Application of the *Family Educational Rights and Privacy Act (FERPA)* And the *Health Insurance Portability and Accountability Act of 1996 (HIPAA)* to Student Health Records, US Department of Health and Human Services and US Department of Education (December 2019), available at <https://www.hhs.gov/sites/default/files/2019-hipaa-ferpa-joint-guidance.pdf> - PDF, describing what types of institutions FERPA applies to and what information is included in “education records.”

10. [☞](#) See 45 CFR 160.103 (definition of “Covered entity”).

11. [☞](#) See 45 CFR 160.103 (definition of “Business associate”).

12. [☞](#) See 45 CFR 160.103 (definition of “Covered entity”).

13. [☞](#) See 45 CFR 160.103 (definition of “Business associate”).

14. [☞](#) See 45 CFR 160.103 (definition of “Protected health information”). HHS addressed questions regarding the application of the HIPAA Privacy Rule to employers in the preambles to the 2000 Privacy Rule and the 2002 Modifications to the HIPAA Privacy Rule. “With regard to employers, we do not have statutory authority to regulate them. Therefore, it is beyond the scope of this regulation to prohibit employers from requesting or obtaining protected health information.” 65 FR 82426, 82592 (December 28, 2000). “[T]he Department must remain within the boundaries set by the statute, which does not include employers per se as covered entities. Thus, we cannot regulate employers, even when it is a covered entity acting as an employer.” 67 FR 53182, 53192 (August 14, 2002).

15. [☞](#) See 45 CFR 160.103 (definition of “Workforce”).

16. [☞](#) See EEOC, [What You Should Know about COVID-19 and the ADA, the Rehabilitation Act, and Other EEO Laws](#), § K (June 28, 2021), available at

<https://www.eeoc.gov/wysk/what-you-should-know-about-covid-19-and-ada-rehabilitation-act-and-other-eeo-laws>. See generally Shen, Wen W. (2019). “Legal Sidebar: An Overview of State and Federal Authority to Impose Vaccination Requirements” (CRS Report No. LSB10300), available at <https://crsreports.congress.gov/product/pdf/LSB/LSB10300>. See also information about state vaccination laws on the websites of the [Centers for Disease Control and Prevention](#) (CDC) and the [National Conference of State Legislators](#) (NCSL).

17. [☞](#) See EEOC, *What You Should Know*, at § K.
18. [☞](#) See *id.*, § K.4.
19. [☞](#) See 45 CFR 160.103 (definition of “Covered entity”).
20. [☞](#) See 45 CFR 160.103 (definition of “Business associate”).
21. [☞](#) See 45 CFR 160.103 (definition of “Protected health information”).
22. [☞](#) See 45 CFR 160.103 (definition of “Workforce”). For additional information, see FAQ 301, <https://www.hhs.gov/hipaa/for-professionals/faq/301/does-the-hipaa-public-health-provision-permit-health-care-providers-to-disclose-information-from-pre-employment-physicals/index.html>.
23. [☞](#) See 45 CFR 160.103 (definitions of “Business associate” and “Covered entity”). See also <https://www.hhs.gov/hipaa/for-professionals/covered-entities/index.html>.
24. [☞](#) See 45 CFR 164.508(b)(4)(iii).
25. [☞](#) See 45 CFR 160.103 (definition of “Covered entity”).
26. [☞](#) See 45 CFR 160.103 (definition of “Business associate”).
27. [☞](#) See 45 CFR 160.103 (definition of “Protected health information”).
28. [☞](#) See 45 CFR 164.514(d)(3).
29. [☞](#) See 45 CFR 164.506(c)(1).
30. [☞](#) See 45 CFR 164.512(b)(1)(i).
31. [☞](#) See 45 CFR 164.514(d)(3)(iii)(A).
32. [☞](#) See 45 CFR 164.512(a).

33. [↗](#) See 45 CFR 164.502(a)(1)(i) (permitting a covered entity to use or disclose an individual’s PHI to the individual). Note, when an individual, or their personal representative, requests access to the individual’s PHI, in addition to the disclosure being permissible, it is also required under an individual’s right of access. See 45 CFR 164.524 (providing individuals with the right of access to inspect and obtain a copy of PHI about the individual in a designated record set).
34. [↗](#) See 45 CFR 164.512(b)(1)(iii).
35. [↗](#) See 29 CFR 1904.5 (definition of “Work-related illness”). See also OSHA’s [website](#) for guidance on the application of OSHA requirements to COVID-19.
36. [↗](#) See 45 CFR 164.512(b)(1)(v). See also FAQ 301, <https://www.hhs.gov/hipaa/for-professionals/faq/301/does-the-hipaa-public-health-provision-permit-health-care-providers-to-disclose-information-from-pre-employment-physicals/index.html>.
37. [↗](#) See 45 CFR 164.512(b)(1)(v)(A).
38. [↗](#) See OSHA, Protecting Workers: Guidance on Mitigating and Preventing the Spread of COVID-19 in the Workplace, at § 9 (June 10, 2021), available at <https://www.osha.gov/coronavirus/safework> (describing recording and reporting requirements related to COVID-19 infections and deaths and the current exception to requirements to record worker side effects from COVID-19 vaccination through May 2022).
39. [↗](#) See 45 CFR 164.512(b)(1)(v)(C).
40. [↗](#) Covered entities must implement policies and procedures with respect to PHI that are designed to comply with the requirements of the Privacy Rule, which would include, if applicable to the covered entity, a policy and procedure to ensure that disclosures to an employer under 45 CFR 164.512(b)(1)(v) meet the conditions specified in that paragraph. See 45 CFR 164.530(i)(1).
41. [↗](#) See 45 CFR 164.512(b)(1)(v)(D).
42. [↗](#) Subject to the permissions for disclosures required by law and those necessary to lessen or prevent a serious and imminent threat. See 45 CFR 164.512(a) and 164.512(j).