Shumaker

APRIL 29, 2026 | PUBLICATION

Client Alert: The Government May Actually Be Here to Help - Health Insurance Portability and Accountability Act of 1996 (HIPAA) Part V

INDUSTRY SECTOR

Health Care

SERVICE LINE

Health Law

RELATED PROFESSIONALS

Grant P. Dearborn
Katherine H. Crawford

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

The United States Department of Health and Human Services (HHS) provides a helpful set of questions and answers on its website regarding the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Professionals should note that this guidance is informal and may be updated or withdrawn and may differ from state laws. Below, we highlight the following three questions and answers from the HHS website.

Who must comply with HIPAA privacy standards?

As required by Congress in HIPAA, the HIPAA Privacy Rule covers:

- Health plans
- Health care clearinghouses
- Health care providers who conduct certain financial and administrative transactions electronically. These electronic transactions are those for which standards have been adopted by the Secretary under HIPAA, such as electronic billing and fund transfers.

These entities (collectively called "covered entities") are bound by the privacy standards even if they contract with others (called "business associates") to perform some of their essential functions. The law does not give HHS the authority to regulate other types of private businesses or public agencies through this regulation. For example, HHS does not have the authority to regulate employers, life insurance companies, or public agencies that deliver social security or welfare benefits.

Created 12.19.02

Content reviewed last August 21, 2024.

Generally, what does the HIPAA Privacy Rule require the average provider or health plan to do?

For the average health care provider or health plan, the HIPAA Privacy Rule requires activities such as:

- Notifying patients about their privacy rights and how their information can be used.
- Adopting and implementing privacy procedures for its practice, hospital, or plan.
- Training employees to understand the privacy procedures.
- Designating an individual to be responsible for overseeing the adoption of and adherence to privacy procedures.
- Securing patient records containing individually identifiable health information to ensure they are not readily available to those who do not need them.

Responsible health care providers and businesses already take many of the kinds of steps required by the Rule to protect patients' privacy. Covered entities of all types and sizes are required to comply with the HIPAA Privacy Rule. To ease the burden of complying with the requirements, the HIPAA Privacy Rule gives needed flexibility for providers and plans to create their own privacy procedures, tailored to fit their size and needs. The scalability of the Rule provides a more efficient and appropriate means of safeguarding protected health information than would any single standard. For example,

- The privacy official at a small physician practice may be the office manager, who will have other non-privacy related duties; the privacy official at a large health plan may be a full-time position and may have the regular support and advice of a privacy staff or board.
- The training requirement may be satisfied by a small physician practice providing each new member of the workforce with a copy of its privacy policies and documenting that new members have reviewed the policies, whereas a large health plan may provide training through live instruction, video presentations, or interactive software programs.
- The policies and procedures of small providers may be more limited under the Rule than those of a large hospital or health plan, based on the volume of health information maintained and the number of interactions with those within and outside of the health care system.

Created 12.19.02

Updated 11.9.06

Content reviewed last Feb 15, 2023.

Does the HIPAA Privacy Rule require covered entities to keep patients' medical records for any period of time?

No, the HIPAA Privacy Rule does not include medical record retention requirements. Rather, state laws generally govern how long medical records are to be retained. However, the HIPAA Privacy Rule does require that covered entities apply appropriate administrative, technical, and physical safeguards to protect the privacy of medical records and other protected health information (PHI) for whatever period such information is maintained by a covered entity, including through disposal. See 45 CFR 164.530(c).

Created 2.18.09

Content reviewed last July 26, 2013.

A covered entity is responsible for ensuring that its workforce (i.e., employees, volunteers, and others under the covered entity's direct control) complies with the HIPAA Privacy Rule. As set forth above, there is not a one-size-fits-all approach to this. How a covered entity oversees and trains its workforce is dependent upon the resources and size of the entity. A covered entity should adopt policies and procedures that will be effective for its own operations, not just to check off a box to comply with the HIPAA Privacy Rule. While the HIPAA Privacy Rule establishes a framework for covered entities, such as the requirements for safeguarding PHI through disposal, an entity has some discretion in how it will ensure compliance with the Rule.

As mentioned above, the HIPAA Privacy Rule does not dictate how long a covered entity must keep a patient's medical record. Unless state law provides for a longer retention period, we recommend that covered entities retain patient medical records for at least 10 years.

For more information, please contact Grant Dearborn, Kate Crawford, or another member of Shumaker's Health Law Service Line.

Shumaker