

MYTH: There are no required disclosures under HIPAA

FACT: Covered entities are required to disclose protected health information to individuals and to HHS for compliance investigations.

The HIPAA Privacy Rule identifies a variety of purposes, such as treatment and public health, for which covered entities (such as health plans and most health care providers) and their business associates are permitted, but not required, to disclose or use an individual's protected health information (PHI). The Privacy Rule only specifies two situations in which a covered entity or business associate is required to disclose PHI. Covered entities are required to disclose an individual's PHI to that individual and to the Secretary of the US Department of Health and Human Services (HHS) for certain purposes.

Disclosures to the individual.

Access to PHI. Under the Privacy Rule, an individual has the right to request to inspect or obtain a copy of his or her own PHI maintained by a covered entity (CE). The CE must disclose the individual's PHI to him or her (or to a third party identified by the individual) upon request. A CE may deny access for very limited reasons, such as when the PHI requested is psychotherapy notes or when a provider determines that access is likely to endanger the individual's life. In most cases, a denial can be reviewed and the CE must comply with the determination of the reviewer. As is necessary, a business associate (BA) is required to disclose PHI to the individual, the individual's designee, or the CE to satisfy the CE's obligation to provide an electronic copy of the individual's PHI to the individual.

Accounting of disclosures. An individual may request and a CE is required to provide an accounting of the disclosures of the individual's PHI made by the CE in the previous six years. The CE is not required to include disclosures made for certain purposes, such as for treatment or health care operations.

Disclosures to the Secretary of HHS.

Investigations and compliance reviews. The Secretary of HHS is permitted to:

- Investigate any complaint filed by an individual alleging that a CE or BA is violating the HIPAA Rules; and

- Conduct a compliance review of a CE or BA to determine whether the CE or BA is complying with applicable provisions of the HIPAA Rules.

The Secretary will always conduct a compliance review and will always investigate complaints when a preliminary review of the facts indicates a possible violation by the CE or BA that is due to willful neglect.

Disclosures of PHI. When the Secretary conducts a compliance review or investigation for any reason, the CE or BA must give the Secretary access to any PHI relevant to the review or investigation.

Disclosures required by law. Laws other than HIPAA, including state laws, may require disclosures of PHI for certain purposes, such as to report child abuse. The Privacy Rule permits CEs to make disclosures required by other law that are for any of the following purposes and meet applicable requirements:

- Disclosures about victims of abuse, neglect, or domestic violence;
- Disclosures for judicial and administrative proceedings; and
- Disclosures for law enforcement purposes.

For More Information:

- [Learn](#) about state and federal privacy laws.
- [Read](#) an overview of HIPAA & related resources.

Follow us on Twitter at [@HealthInfoLaw](#)