HealthInformation &theLaw
HealthInfoLaw.org
Myth Busters
January 2014

MYTH: A Data Use Agreement is always required for the use and disclosure of Protected Health Information.

FACT: Under HIPAA, a Data Use Agreement is only required when a covered entity releases a Limited Data Set to a non-covered entity for the purposes of research, public health or health care operations.

The HIPAA Privacy Rule establishes minimum federal requirements for the use and disclosure of protected health information (PHI) by covered entities. Generally, the rule is split between uses and disclosures of PHI by covered entities that require patient authorization and those that do not. Among the permitted uses of PHI without patient authorization are the very broad categories of research, public health activities, and health care operations. If two covered entities under HIPAA wish to use and disclose PHI for these reasons (in addition to other permitted uses), they may do so without obtaining patient authorization as long as all other requirements of the rule are met.

However, if a covered entity seeks to release PHI to a non-covered entity for research, public health activities or health care operations, then the covered entity may do so only in a "limited data set" and with an accompanying Data Use Agreement (DUA) executed between the covered entity and the recipient of the limited data set. Because the recipient is not a covered entity subject to HIPAA, the DUA is needed to protect an individual's privacy when the data are being used by the recipient.

A DUA is required to:

- identify who may use or receive the information;
- prohibit the recipient from using or further disclosing the information, except as permitted by the agreement or as permitted by law;
- establish the permitted uses and disclosures of the limited data set;
- require the recipient to use appropriate safeguards to prevent a use or disclosure that is not permitted by the agreement;
- require the recipient to ensure that any agents (including a subcontractor) to whom it provides the information will agree to the same restrictions as provided in the agreement; and
- require the recipient to report to the covered entity any unauthorized use or disclosure of which it becomes aware;
- prohibit the recipient from identifying the information or contacting the individuals.

The Privacy Rule also requires the covered entity that originally held the data to take any reasonable steps necessary to cure a breach of the DUA by the recipient of the data, or else discontinue all disclosures of PHI to the recipient and report the problem to the Department of Health and Human Services.

Note that fully de-identified data that does not constitute PHI may be used and released by the covered entity to whomever without patient authorization or a DUA.

For More Information:

- See our Fast Facts about Limited Data Sets.
- Learn about state and federal laws related to Privacy and Confidentiality.
- Read our overview of HIPAAand related resources.

Follow us on Twitter at @HealthInfoLaw