What is a Data Use Agreement?

A data use agreement (DUA) is an agreement required by the HIPAA Privacy Rule between a covered entity and a person or entity that receives a "limited data set" from the covered entity. The DUA must be specific and state that the recipient will use or disclose the information in the limited data set only for specific purposes limited to research, public health or health care operations.

Even though a limited data set excludes many direct identifiers of the individual (name, postal address information, telephone numbers, fax numbers, electronic mail addresses, social security numbers, medical record numbers, health plan beneficiary numbers, account numbers, certificate/license numbers, vehicle identifiers and serial numbers, device identifiers and serial numbers, web URLs, IP address numbers, biometric identifiers, and full face photographic images and any comparable images), it is still considered Protected Health Information (PHI). When such information is in the hands of non-covered entities, the Privacy Rule attempts to protect the privacy of individuals through the use of DUAs.

DUAs must adhere to the requirements set forth in the Privacy Rule. A DUA must:

- 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; and
- 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 (i.e., repair the damage caused by) a breach of the DUA by the recipient of the data. If the problem that caused the breach of the DUA cannot be resolved by the covered entity, then the covered entity must discontinue all disclosures of PHI to the recipient and report the problem to the Department of Health and Human Services.

For more information on state and federal laws related to Privacy and Confidentiality, click here. For more information about HIPAA, click here. *Follow us on Twitter at **@HealthInfoLaw***