What is "de-identified data" under the HIPAA Privacy Rule?

A covered entity may use and disclose Protected Health Information (PHI) only as described in the Privacy Rule. However, not all health information held by a covered entity is considered PHI. De-identified health information is not considered PHI and therefore not protected by the Privacy Rule. The process for the de-identification of information must adhere to specific standards under the Privacy Rule, but once de-identified, the information may be used and disclosed by a covered entity without restriction. There are two permitted methods for the de-identification of PHI: (1) the removal of 18 specific pieces of information from each record; or (2) a statistical verification of de-identification.

Under the first method, a covered entity can de-identify data by removing 18 items that could be used to identify the individual, those related to the individual, household members of the individual or the individual's employer. Additionally, the covered entity cannot have any actual knowledge that the information remaining could be used to identify the person who is the subject of the information. The 18 specific unique identifiers are*:*

- Names
- Geographic information smaller than a state, including address, city, county and zip code
- All elements of dates, except year, that directly relate to an individual
- Telephone numbers
- Fax numbers
- Email addresses
- Social security numbers
- Medical record numbers
- Health Plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers/serial numbers
- Device identifiers/serial numbers
- Web URLs
- IP address numbers
- Biometric identifiers
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code, unless otherwise permitted by the Privacy Rule for re-identification

A covered entity may assign a code or other means of record identification to allow de-identified information to be re-identified, but only if the code is known to the covered entity alone and the code is not related to or derived from the removed identifiers. Also, a covered entity may remove the identifiers itself or engage a business associate to do so.

Under the second method, instead of removing all 18 unique identifiers, covered entities may obtain a statistical verification of de-identification through certification by "a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable." The certification ensures there is a very small risk that the information could be used to identify the individual who is the subject of the information. The certification must document the results of the analysis that justify the de-identification determination as well as the methods used. The covered entity must keep the certification for at least six years from the date of its creation, or the date when it was last in effect, whichever is later.

For more information on state and federal laws related to privacy, see www.healthinfolaw.org/topics/63.
For more information about HIPAA, see www.healthinfolaw.org/federal-law/HIPAA.
Follow us on Twitter at **@HealthInfoLaw**