HIPAA Compliance for the American Heart Association's Open Data Policy

Background

The American Heart Association's (the Association) Open Data policy requires that grant applicants include a data sharing plan as part of the application process for most programs. The data sharing plan must safeguard identifying information related to research subjects to comply with the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Privacy Rule. The HIPAA Privacy Rule establishes the conditions under which "protected health information" may be used or disclosed. Protected health information (PHI) is information, including demographic information, which relates to:

- the individual's past, present, or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual, and that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual.

PHI includes many common identifiers (e.g., name, address, birth date, Social Security Number) when they can be associated with the health information listed above. The relationship with health information is fundamental. Identifying information alone, such as personal names, residential addresses, or phone numbers, would not necessarily be designated as PHI. For instance, if such information was reported as part of a publicly accessible data source, such as a phone book or, publicly available through an internet search, then this information would not be PHI because it is not related to heath data. If such information was listed with health condition, health care provision or payment data, such as an indication that the individual was treated at a certain clinic, then this information would be PHI.

De-Identification and its Rationale: Maintaining Compliance

The United States Department of Health and Human Services has developed guidance for methods to achieve de-identification in compliance with the HIPAA Privacy Rule. These methods fall into two tracks, 1) a formal determination by a qualified expert; or 2) the removal of specified individual identifiers as well as absence of actual knowledge by the covered entity that the remaining information could be used alone or in combination with other information to identify the individual. It is the second of these paths (deemed the "Safe Harbor" method by HHS) that is most relevant to the Association's Open Data policy. The Safe Harbor method §164.514(b)(2) of de-identification requires the removal of 18 specific elements from the research data. Additionally, there is no "knowledge of residual information" that can identify the individual, making *re-identification* more difficult. The 18 identifiers to be removed from data:

1. Names

2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code, and their equivalent geocodes, except for the initial three digits of the ZIP code if, according to the current publicly available data from the Bureau of the Census:
(a) The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; and (b) The initial three digits of a ZIP code for all such geographic units containing 20,000 or fewer people is changed to 000

3. All elements of dates (except year) for dates that are directly related to an individual, including birth date, admission date, discharge date, death date, and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older

4. Telephone numbers

5. Vehicle identifiers and serial numbers, including license plate numbers

6. Fax numbers

7. Device identifiers and serial numbers

8. Email addresses

9. Web Universal Resource Locators (URLs)

10. Social security numbers

11. Internet Protocol (IP) addresses

12. Medical record numbers

13. Biometric identifiers, including finger and voice prints

14. Health plan beneficiary numbers

15. Full-face photographs and any comparable images

16. Account numbers

17. Any other unique identifying number, characteristic, or code, except as permitted by "Re-identification"*:

> **Re-identification.* A covered entity may assign a code or other means of record identification to allow information de-identified under this section to be re-identified by the covered entity, provided that:
> (a) *Derivation.* The code or other means of record identification is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and
> (b) *Security.* The covered entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

18. Certificate/license numbers

The researcher responsible for the data should also warrant that he/she does not have actual knowledge that the remaining information could be used alone or in combination with other information to identify an individual who is a subject of the information. The Department of Health and Human Services provides examples that delve into some of the intricacies associated with the Safe Harbor method.

Demonstrating Compliance
As required by the Association's Open Data policy, the grant application for most programs will include the applicant's proposed data sharing plan. Within this section, there is language that describes the applicant's plan for compliance with HIPAA regulations. In the event that HIPAA noncompliance is identified during compliance monitoring of the award, the awardee will be contacted, the dataset(s) in question must be taken down immediately, and the awardee will be referred to the Safe Harbor method details for correction and resharing of their data.

Updated: July 22, 2026