Health Insurance Portability and Accountability Act (HIPAA) Checklist

The Privacy Rule is a Federal regulation under HIPAA that protects the privacy of personal health information (PHI) that identifies individuals who are living or deceased. Researchers who access health information, epidemiological databases, disease registries, hospital discharge records, government compilations of vital and health statistics, tissue and data repositories, etc., to create individually identifiable health information in connection with an experimental intervention, must use this form to ensure that HIPAA requirements are met.

*Note: The full text of the Privacy Rule may be found at the web site of the Office for Civil Rights (OCR): http://www.hhs.gov/ocr/hipaa

To de-identify data and protect the identity of an individual or the individual’s relatives, employers, or household members, the following 18 elements or identifiers must be removed:

1. Names
2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP Code, and their equivalent geographical codes, except for the initial three digits of a 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. B) The initial three digits of a ZIP Code for all such geographic units containing 20,000 or fewer people are changed to 000.
3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; 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. Facsimile numbers
6. Electronic mail addresses
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web universal resource locators (URLs)
15. Internet protocol (IP) address numbers
16. Biometric identifiers, including fingerprints and voiceprints
17. Full-face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code, unless otherwise permitted by the Privacy Rule for re-identification
Authorization Agreement for Research Uses and Disclosures

Individuals may agree to disclose his/her PHI by signing an Authorization Agreement (AA). This agreement is in addition to the Informed Consent to participate in research and is specific only to the current research study and not for future research studies. The (AA) must be kept for six years from the date of creation or the date it was last in effect, whichever is later. The AA focuses on privacy risks and states how, why, and to whom the PHI will be used and/or disclosed for research. The AA can be combined with an informed consent document and must be written in plain language, containing the core elements and required statements listed below.

Authorization Core Elements:

- A description of the PHI to be used or disclosed, identifying the information in a specific and meaningful manner
- The names or other specific identification of the person or persons (or class of persons) authorized to make the requested use or disclosure.
- The names or other specific identification of the person or persons (or class of persons) to whom the covered entity may make the requested use or disclosure
- A description of each purpose of the requested use or disclosure
- Authorization expiration date or expiration event that relates to the individual or to the purpose of the use or disclosure (‘end of the research study” or “non” are permissible for research, including for the creation and maintenance of a research database or repository).
- Signature of the individual and date. If the individual’s legally authorized representative signs the AA, a description of the representative’s authority to act for the individual must also be provided.

Authorization Required Statements:

- A statement of the individual’s right to revoke his/her AA and how to do so, and if applicable, the exceptions to the right to revoke his/her AA or reference to the corresponding section of the covered entity’s notice of privacy practices.
- Whether treatment, payment, enrollment, or eligibility of benefits can be conditioned on Authorization, including research-related treatment and Consequences of refusing to sign the AA, if applicable.
- A statement of the potential risk that HI will be re-disclosed by the recipient. This may be a general statement that the Privacy Rule may no longer protect PHI disclosed to the recipient.