HIPAA Identifiers & Data Protection Standards

Office of Research Integrity & Compliance | Version 2
Updated: June 21, 2017

This document provides researchers with a list of identifying information prevents an IRB protocol application from being reviewer as exempt. Standards for protecting identifiable data are also included. If further assistance or clarification is required, please contact the ORIC at 304-293-7073, or at IRB@mail.wvu.edu.

Identifiable Information

1. Names
2. All geographical subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, 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; 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 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. Phone numbers
5. Fax numbers
6. Electronic mail (e-mail) addresses
7. Social Security numbers
8. Medical Record numbers (MRN)
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate or 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
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images
18. Any other unique identifying number, characteristic, or code
    a. Note: This does not mean the unique code assigned by the investigator to code the data.

Standards to Protect Privacy and Re-identification

Prior to protocol submission to the IRB and once IRB approval is obtained, the PI must have a clear plan of how research records will be secured, because security is key to maintaining subject confidentiality. Documents to secure include subject/patient listing, consents, and data collection forms.

De-identification of data collection tools follows HIPAA principles. When coding is used as a form of de-identification, the master code listing (or subject listing) must be kept in a separate secure area away from the coded data collection tool (s) so de-identification is maintained. To maintain confidentiality, all team members must be knowledgeable on what a HIPAA identifier is and what to document on the data collection tool. No additional subject information can be used if it was not previously approved by the IRB.

Any code used to replace the identifiers in datasets cannot be derived from any information related to the individual and the master codes, nor can the method to derive the codes be disclosed. For example, a subject's initials cannot be used to code their data because the initials are derived from their name. Additionally, the researcher must not have actual knowledge that the research subject could be re-identified from the remaining identifiers in the PHI used in the research study. In other words, the information would still be considered identifiable is there was a way to identify the individual even though all of the 18 identifiers were removed.

If data are de-identified by a third party, the third party should fill out the De-Identification Certification Form. The form should be attached to the protocol submission. The WVU researcher could then file as an NHSR (Non-Human Subject Research) protocol submission.

Most data are maintained in a secure, password protected computer. A secure computer can hold PHI. Use of a flash drive as a means for data collection can also be used in two ways. First, the USB flash drive must be encrypted to prevent easy access to subject information. Second, only code numbers can be used on the flash drive, not any identifying information like names or the medical chart number. The IRB recommends that the use of USB and other mobile storage devices be discouraged. Any breach of confidentiality due to loss or theft must be reported to the IRB as an unanticipated problem involving risk to the subject or others (UPIRTSO). Any individuals who are no longer a member of the research teams must return subject data.

Guidance on Protocol Submissions

If data is recorded in such a manner that none of the 18 HIPAA identifiers are included, the study can be submitted as an exemption, category 4 with a HIPAA Waiver.

If the data is recorded with identifiers the study must be an expedited or full board review (depending on the level of risk). If the level of risk is expedited and HIPAA is recorded submit a HIPAA Waiver and a consent form waiver.

For any questions, please contact the Office of Research Integrity and Compliance at 304-293-7073 or by email at IRB@mail.wvu.edu.