Health Information Portability and Accountability Act (HIPPA)

What is a Covered Entity?

The Privacy Rule applies only to covered entities.

A Covered Entity is one of the following:

- **A Health Care Provider**
  - This includes providers such as:
    - Doctors
    - Clinics
    - Psychologists
    - Dentists
    - Chiropractors
    - Nursing Homes
    - Pharmacies
  - ...but only if they transmit any information in an electronic form in connection with a transaction for which HHS has adopted a standard.

- **A Health Plan**
  - This includes:
    - Health insurance companies
    - HMOs
    - Company health plans
    - Government programs that pay for health care, such as Medicare, Medicaid, and the military and veterans health care programs

- **A Health Care Clearinghouse**
  - This includes entities that process nonstandard health information they receive from another entity into a standard (i.e., standard electronic format or data content), or vice versa.

What is PHI?

Protected health information (PHI) is health information that is individually identifiable and created or held by a covered entity. Health information includes past, present, and future health information (mental and physical) about:

- Health history or condition of an individual
- Provision of care to an individual
- Payment for an individual’s care.

Health information is individually identifiable when it identifies an individual or there is a reasonable basis to believe the information can be used to identify an individual.

Limited-Data Sets

A limited data set is a special category of PHI that has all of the following identifiers removed:

1. Name
2. Postal address information other than town/city, state, and zip
3. Telephone number
4. Fax number
5. Email address
6. Social security number
7. Medical record number
8. Health plan number
9. Account numbers
10. Certificate or license numbers
11. Vehicle identification/serial numbers, including license plate numbers
12. Device identification/serial numbers
13. Universal resource locators (URLs)
14. Internet protocol (IP) addresses
15. Biometric identifiers, including finger and voice prints
16. Full face photographs and comparable images

Under the Privacy Rule, use or disclosure of limited data sets for research purposes requires a “Data Use Agreement.” **Data Use Agreement** – An agreement into which the covered entity enters with the intended recipient of a limited data set that establishes the ways in which the information in the limited data set may be used and how it will be protected.

**De-Identified Data**

De-identified data are not subject to the requirements of the Privacy Rule because they are not individually identifiable. There are two ways to de-identify data:

**Safe Harbor Method** – in which all of the following elements are removed from a data set:

1. Name
2. All geographic subdivisions smaller than a state (street address, city, county, precinct) Note: zip code or equivalents must be removed, but can retain first 3 digits of the geographic unit to which the zip code applies if the zip code area contains more than 20,000 people
3. For dates directly related to the individual, all elements of dates, except year (date of birth, admission date, discharge date, date of death)
4. All ages over 89 or dates indicating such an age
5. Telephone number
6. Fax number
7. Email address
8. Social security number
9. Medical record number
10. Health plan number
11. Account numbers
12. Certificate or license numbers
13. Vehicle identification/serial numbers, including license plate numbers
14. Device identification/serial numbers
15. Universal Resource Locators (URLs)
16. Internet protocol (IP) addresses
17. Biometric identifiers, including finger and voice prints
18. Full face photographs and comparable images
19. Any other unique identifying number, characteristic, or code.

Note: Item 19 is known as the “catch-all” provision and is intended to include items that are not otherwise specified but could make a data set identifiable.

**Statistical Method** – in which certification is provided by “a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable so that there is a ‘very small’ risk that the information could be used by the recipient to identify the individual who is the subject of the information, alone or in
combination with other reasonably available information.” For more information see NIH Guidance Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule.

**When Does the Privacy Rule Apply to Research?**

The HIPAA Privacy Rule affects research and researchers when either:

- Research creates or generates PHI, or
- Research requires access to and/or use of PHI.