

Limited Data Set vs. De-identified Information

*Wendy Duncan
Privacy Officer for Research
February 2026*



Covered Entity

Definition 45 CFR [160.103](#)

Hybrid entity, meaning that the entity is a single legal entity that performs both covered and non-covered functions.

A Health Care Provider

- Doctor
- Clinic
- Pharmacy
- Psychologist, etc.

...but only if they transmit any health information in an electronic form in connection with a transaction for which HHS has adopted a standard.

A Health Plan

- 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.

HIPAA Overview



Protected Health Information (PHI)

The HIPAA Privacy Rule protects most “**individually identifiable health information**” held or transmitted by a covered entity or its business associate, in **any form** or medium, whether electronic, on paper, or oral.

- 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.
- Protected health information includes many common identifiers (e.g., name, address, birth date, Social Security Number) when they can be associated with the health information listed above.

HIPAA Overview



De-Identified Data - Can not include...

- Name
- Street address, city, county, precinct, [zip codes*](#) (“smaller than State”)
- Dates e.g. DOB, admission date, discharge date, date of death; and all **ages over 89** (single category of age 90 or older)
- Social Security number
- Telephone/fax numbers, E-mail addresses, URLs, (IP) address numbers
- Medical record numbers
- Health plan beneficiary numbers, Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- Biometric identifiers, including finger and voice prints
- Full-face photographic images and any comparable images
- Any other unique identifying numbers, characteristics or codes

USING or DISCLOSING PHI

*population of 20,000 or fewer persons



De-Identified Data

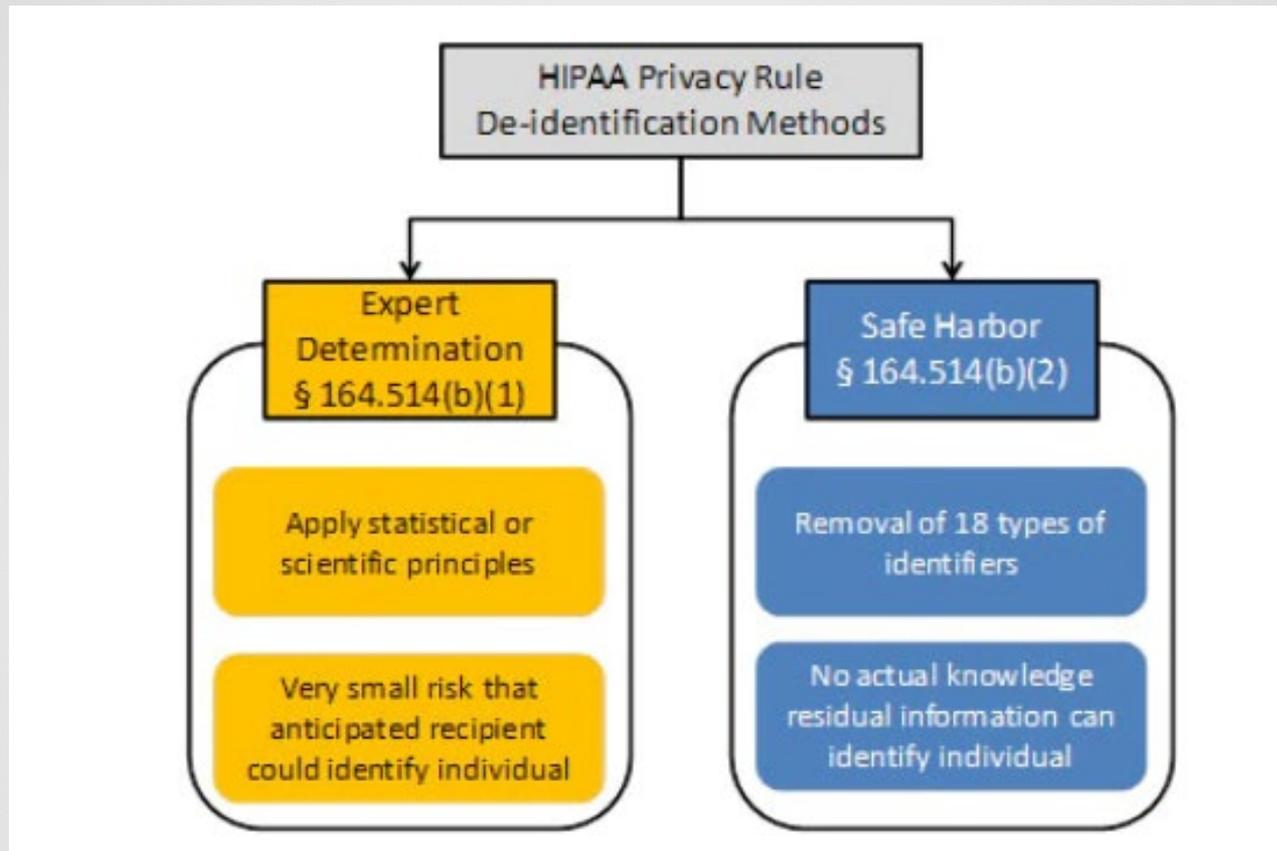
Section **164.514(a)** of the HIPAA Privacy Rule provides the standard for de-identification of protected health information. Under this standard, health information is not individually identifiable if it does not identify an individual and if the covered entity has **no reasonable basis** to believe it can be used to identify an individual.

Sections [164.514\(b\)](#) and (c) of the Privacy Rule contain the implementation specifications that a covered entity **must follow to meet the de-identification standard**. The Privacy Rule provides two methods by which health information can be designated as de-identified.

USING or DISCLOSING PHI



De-Identified Data



USING or DISCLOSING PHI



De-Identified Data

Sections 164.514(b)

“Expert Determination” method- A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable

“Safe Harbor” method- All 18 identifiers are removed and the covered entity does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual

Sections 164.514(c)

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

USING or DISCLOSING PHI



Limited Data Sets

- Can be used without the subject's authorization, but is still subject to HIPAA regulations
- Permitted HIPAA identifiers include zip code/city/state, dates (e.g., DOB, DOS, and unique codes)
 - This excludes MRN, Health Plan #, Name, Contact information
- Need HIPAA-compliant DUA in order to disclose
 - Limitations on the recipient(s) and data use
 - Terms they will follow to safeguard data
 - Duty to notify us of unauthorized disclosures
 - Assurance that they will not attempt to identify or contact individuals
 - Ensure agents/contractors agree to the same restrictions

USING or DISCLOSING PHI



Resources

- [HHS Guidance](#)
- URochester [HIPAA Policies](#)
 - OP-25 Research policies & Limited Data Sets
 - OP-30 De-Identification
- URochester [Research Forms & Guidance](#) [Soon to be updated]

RESOURCES



QUESTIONS?

Wendy_Duncan@URMC.Rochester.edu

Bookings Page: [CLICK HERE](#)

Or

PrivacyTeam-URMC@URMC.Rochester.edu

