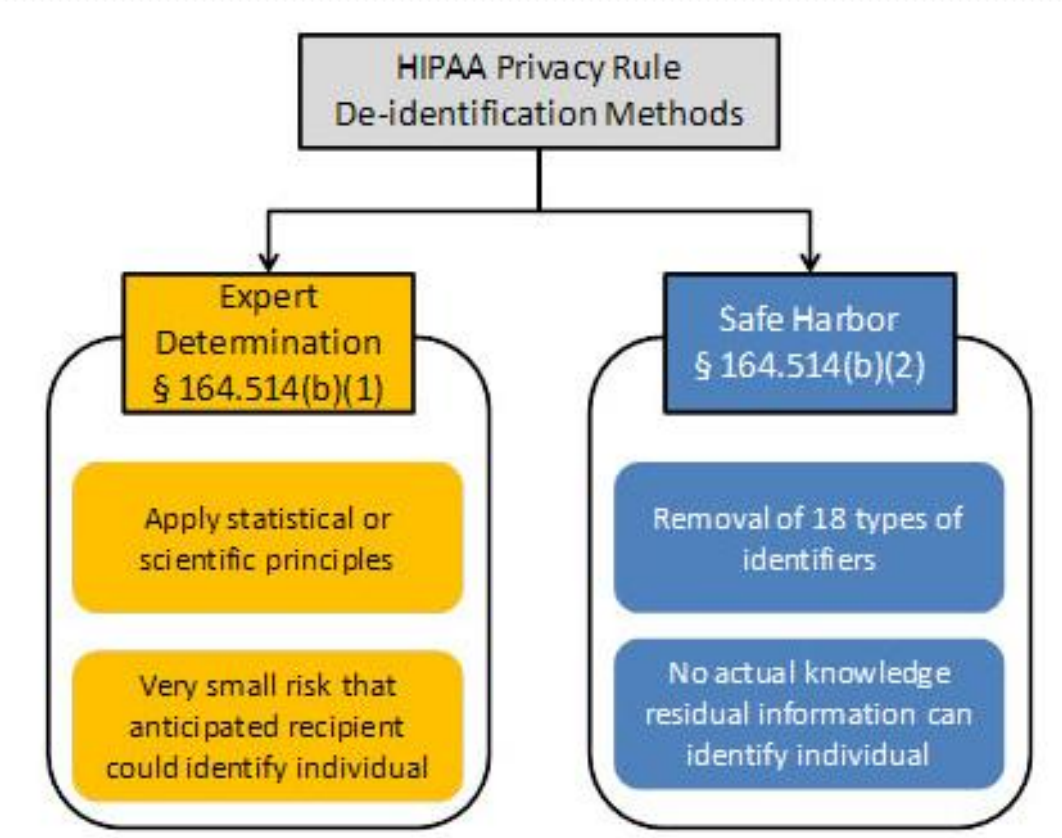
Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule

http://www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/De-identification/guidance.html#protected

De-Identification Methods



Expert Determination Method

Implementation specifications: requirements for de-identification of protected health information. A covered entity may determine that health information is not individually identifiable health information only if:

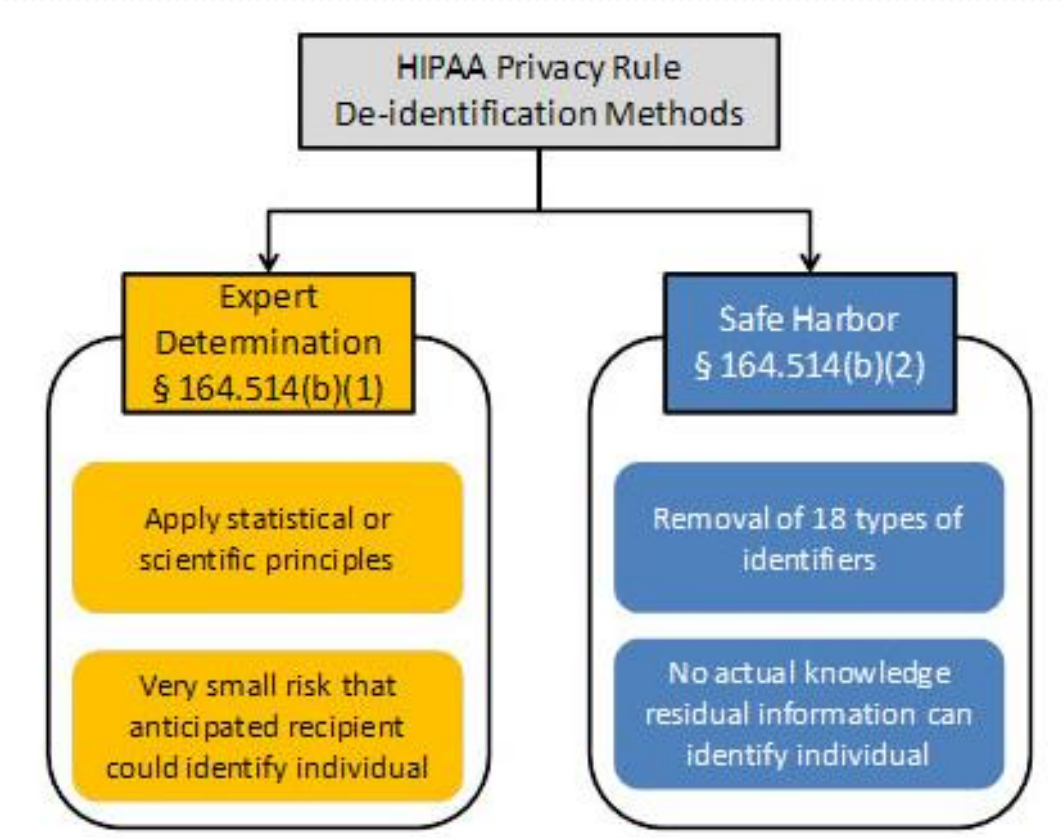
(1) A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable:
(i) Applying such principles and methods, determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify an individual who is a subject of the information; and
(ii) Documents the methods and results of the analysis that justify such determination;

Safe Harbor Method

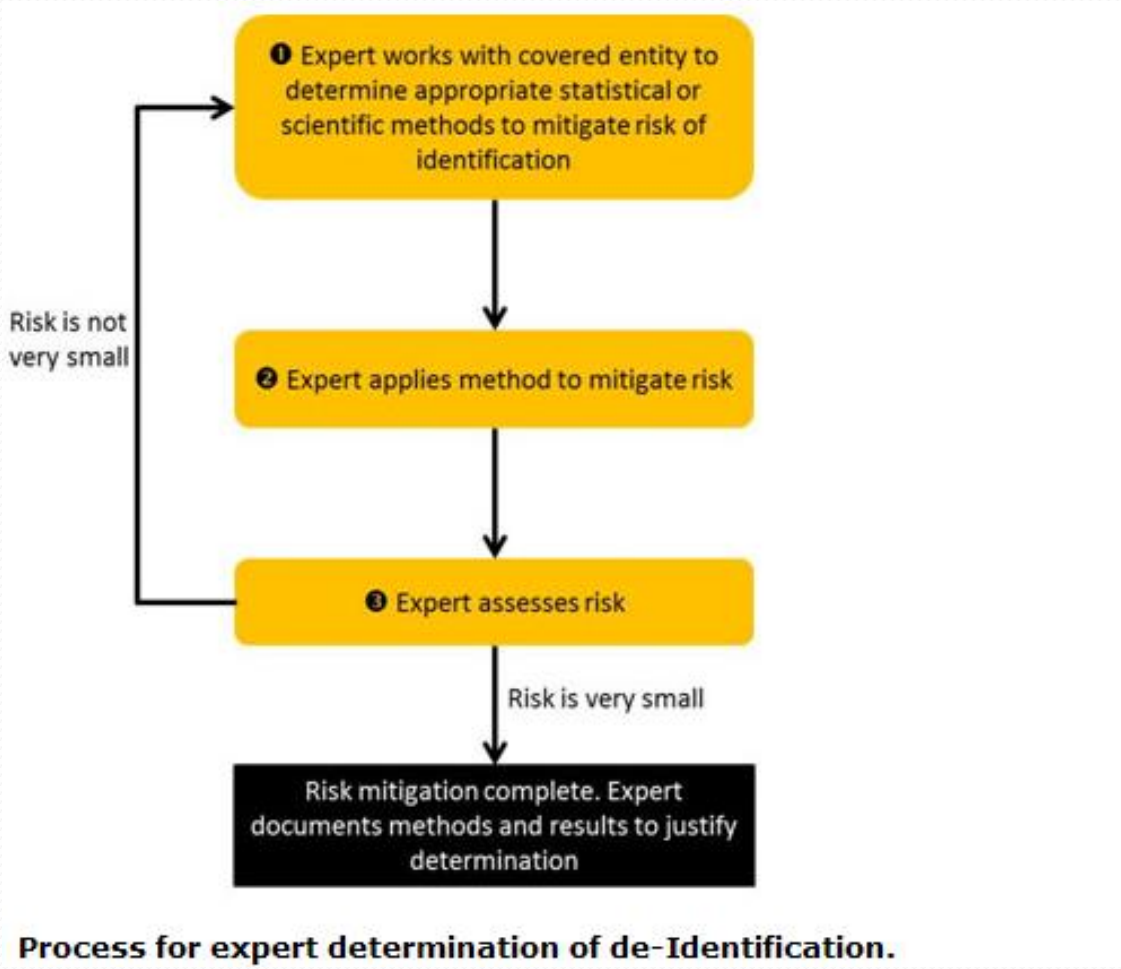
The following identifiers of the individual or of relatives, employers, or household members of the individual, are removed:

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:
   (1) The geographic unit formed by combining all ZIP codes with the same three initial digits contains more than 20,000 people; and
   (2) 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. Fax numbers
6. Email 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) addresses
16. Biometric identifiers, including finger and voice prints
17. Full-face photographs and any comparable images
18. Any other unique identifying number, characteristic, or code, except as permitted by paragraph (c) of this section [Paragraph (c) is presented below in the section "Re-identification"]; and

De-Identification Methods



Data Scrubber Certification



Process for expert determination of de-Identification.

✓ Must be generalizable to other Institutions!

Vanderbilt Validation Plan

After lengthy discussions with our IRB, legal counsel, privacy office, and national privacy experts, we determined that in order to contribute free text we must:

1. Modify the MPOG Data Use Agreement to make ensure we are fully compliant with legal requirements
2. Run our free text through a more robust, previously validated filter (MIST), and repeat our prior analysis to determine the amount of PHI that is slipping through
3. Fully document our de-identification process

Recommendations for MPOG Steering Committee

- Standardize the PHI filtering process at all participating institutions that are contributing free text
- Standardize the validation process for evaluating the local efficacy of the PHI filter at each institution
- When errors occur, create a detailed reporting process. This process should include complete documentation of errors and how they can be corrected in the future. This information will then be disseminated to each individual site so they can follow the corrective action plan
- Each site contributing free text should meet with their IRB, privacy office, and legal counsel to obtain approval for their individual processes

Proposed Change to Data Use Agreement

- Modify Participants Obligations:
  - require and establish clear procedures for reporting discovery or disclosure of PHI (timeframe, reporting structure, corrective action plan)
- Modify Michigan Obligations:
  - Provide to participants within 5 business days of discovery of a PHI breach:
    - the date of the breach & the date of the discovery of the breach;
    - a description of the types of unsecured PHI that were involved;
    - identification of each individual whose unsecured PHI has been, or is reasonably believed to have been, accessed, acquired, or disclosed; and
    - any other details needed to complete an assessment of the risk of harm to the individual.
  - Participant will be responsible to provide notification to individuals whose unsecured PHI has been disclosed, as well as the Secretary and the media, as required by Sec. 13402 of the HITECH Act, 42 U.S.C.A. § 17932;
  - Michigan agrees to establish procedures to investigate the breach, mitigate losses, and protect against any future breaches, and to provide a description of these procedures and the specific findings of the investigation to Participant in the time and manner reasonably requested by Participant.

Process for Correcting Errors

- Identify Error
- Completely document error
  - Type of Error
  - Number of Records affected
  - Recommended corrective action, if known at site level
  - Report error to regulatory bodies if necessary
- Report the error to MPOG
- MPOG reviews & develops a resolution to the error
- MPOG provides sites with instructions on resolution
- Sites implement resolution