## De-Identification Guidelines

Under HIPAA regulations, health information is not individually identifiable if it does not identify an individual and if the covered entity (i.e. provider) has no reasonable basis to believe it can be used to identify an individual. De-identified data is not subject to HIPAA regulations. Below outlines the Safe Harbor method, which is one of the two (2) methods to de-identify protected health information under the HIPAA Privacy Rule at 45 C.F.R. § 164.14(b)(2):

(i)     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:
     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 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; prescription numbers
9.   Health plan beneficiary numbers
10.  Account numbers (e.g. payment information)
11.  Certificate/license numbers
12.  VIN and serial numbers, including license plate numbers
13.  Device identifiers and serial numbers
14.  Web URLs
15.  Internet Protocol (IP) addresses
16.  Biometric identifiers, including finger and voice prints
17.  Full-face photographs and any comparable images (e.g. tattoo, birthmark)
18.  Any other unique identifying number, characteristic, or code, (e.g. current president of State University; pitcher of the baseball game last night, etc.) and

(ii)      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 who is a subject of the information.

**Derivatives of any of the listed identifiers cannot be disclosed.** For example, a data set that contained patient initials, or the last four digits of a Social Security number, would not meet the requirement of the Safe Harbor method for de-identification.

Review the Department of Health and Human Services Guidance for more details on proper de-Identification of protected health information to ensure the data you are submitting to this site meets the requirements under the Privacy Rule safe harbor method. *De-ID Guidance*

Section 164.514(a) of the HIPAA Privacy Rule provides the standard for de-identification of protected health information. 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.

**Exhibit A-3**

**<u>Text of De-Identification Pop-Up Reminder</u>**

This website is not intended to contain any HIPAA Protected Health Information ("PHI"), as that term is defined at 45 C.F.R. § 160.103. You agree that you will only post DE-IDENTIFIED data to this site as that term is defined at 45 C.F.R. §164.514(a)-(b). Please review your data to ensure proper de-identification prior to posting to this site. By accessing and posting your data to this website you agree to the foregoing. You also agree that any transmittal or posting of PHI shall occur at your or your company's own risk and that Cleveland Clinic shall not be liable as outlined in the Terms of Use.