Health Insurance Portability and Accountability Act (HIPAA) of 1996
Stipulations Around De-Identification and Re-Identification

What is "De-Identification"?

Under HIPAA, the Privacy Rule protects all "individually identifiable health information" held or transmitted by a Covered Entity or its Business Associate, in any form or media, whether electronic, paper, or oral. The Privacy Rule calls this information "Protected Health Information" (PHI). By definition, "individually identifiable health information" is information, including demographic data that relates to:

- 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
- information that identifies the individual or for which there is a reasonable basis to believe it can be used to identify the individual

When health information does not identify an individual, and there is no reasonable basis to believe that it can be used to identify an individual, it is said to be "de-identified" and is not protected by the Privacy Rule. The standard for de-identification of individually identifiable health information is specified in 45 C.F.R., Section 164.514(a) of the HIPAA Privacy Rule. Section 164.514(b) of the Privacy Rule contains the implementation specifications that a Covered Entity or affiliated Business Associate must follow to meet the de-identification standard. In accordance with the Privacy Rule mandates, NVRF has utilized "Expert Determination" (a third party) to designate **INSTOR** data as de-identified.

Advantages of De-Identification

Enhanced security

Utilizing "de-identified" data not only protects all information all along the chain of transmission and storage, but also protects the information even in the case of malicious retrieval of data by means of hacking, legal subpoena, a computer virus attack, or misuse. Any information thus obtained would be useless as far as compromise of personal health information (and thus HIPAA rules) are concerned.

Research

De-identification of data readily allows research both locally by the participating site as well as in aggregate form by researchers in the stroke community (including those that might be at the participant site) that desire to publish process or outcomes data relating to aggregate data for the betterment of the common good and the advancement of science. All researchers are using data that is not personally identifiable.

What is "Re-Identification"?

The HIPAA Privacy Rule goes on to provide direction with respect to "re-identification" by the covered entity in §164.514(c). It is important to recognize that while the re-identification provision does not permit assignment of a code or other means of record identification that is derived from identifying individual information, a Covered Entity may disclose such derived information if an expert determines that the data meets the de-identification requirements at §164.514(b)(1). This is particularly the case if the resulting information cannot be translated to identify the individual.

The Privacy Rule no longer covers "de-identified health information" created following these methods because it does not fall within the definition of PHI (unless the information can be re-identified). This guidance provides clarification about the methodologies that can be applied to render PHI de-identified in compliance with the de-identification standard.