# Responsible Data Use Attestation

The Regents of the University of Michigan holds data use agreement which approves access to data sets that contain protected health information (PHI). These data permit the research staff to develop comprehensive analyses of utilization and costs by linking files across years and types of files and are vital to the research aims of the institute. Without them, the team would not be able to conduct its approved research project.

The use of these data sources, from the Centers for Medicare & Medicaid (CMS) and other government and private sources, under the stewardship of the Regents of the University of Michigan, **is a privilege, not a right.** With this privilege comes the responsibility to protect the privacy of individuals who are the subjects of the data, to not use or disclose the data other than as permitted by the DUAs, and to appropriately secure the data at all times.

Federal Information Security Management (FISMA) standards defines a comprehensive framework to protect government information requiring safeguards at a level and scope of security that is not less than the level and scope of security requirements established by the Office of Management and Budget (OMB) in OMB Circular No. A-130, Appendix III--Security of Federal Automated Information Systems (https://obamawhitehouse.archives.gov/omb/circulars_a130_a130appendix_iii) as well as Federal Information Processing Standard 200 entitled "Minimum Security Requirements for Federal Information and Information Systems" (http://csrc.nist.gov/publications/fips/fips200/FIPS-200-final-march.pdf); and, Special Publication 800-53 "Recommended Security Controls for Federal Information Systems" (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf).

Data Suppression means no disclosure of direct findings, listings, or information derived from the file(s), with or without direct identifiers, if such findings, listings, or information can, by themselves or in combination with other data, be used to deduce an individual's identity. Examples of such data elements include, but are not limited to geographic location, age if >89, sex, diagnosis and procedure, admission/ discharge date(s), or date of death. Also, any use of CMS data in the creation of any document (manuscript, table, chart, study, report, etc.) must adhere to CMS' current cell size suppression policy. **This policy stipulates that no cell (e.g. admittances, discharges, patients, services) of 10 or less may be displayed.** Also, no use of percentages or other mathematical formulas may be used if they result in the display of a cell size of 10 or less or could be used to deduce that 1 to 10 CMS beneficiaries are part of a cell that combines patients from multiple data sources. Minimum Necessary Standard limits how much protected health information may be used, disclosed, and requested for research or other health care operational functions. The use and disclosure of protected health is limited to only what is necessary to satisfy a particular purpose or carry out a specific function. Minimum necessary standard is a key Health Information Portability Accountability Act of 1996 (HIPAA) privacy rule protection.

With access to the approved Medicare data through the UM VPN, users agree to comply with Michigan Medicine Security Policies delineate the expectations regarding the handling and enforcement of Michigan Medicine PHI security. The Michigan Medicine compliance website (http://med.umich.edu/u/compliance/index.htm) provides extensive information on HIPAA rules and requirements, data confidentiality and data security. In addition, the Michigan Medicine Compliance Program provides updates and education on a variety of data security topics; for example, information on using passwords and securing computer, laptops and other external media at http://www.safecomputing.umich.edu.

Please review each of the points below and acknowledge that you understand and agree with the following:

- ☐ I agree that I will not copy any of the original data files which were given to me OR any derivations of these data files onto ANY laptop computer (either personal or university-owned).
- ☐ I agree that I will not copy any of the original data files which were given to me OR any derivations of these data files onto ANY external media at ANY time, including but not limited to USB drives, flash drives, external hard drives, or any cloud computing storage space such as Dropbox or Box.
- ☐ I agree that I will not attempt to identify or contact any individual represented in the data.
- ☐ I agree that I will use original and derived data files for this project only. Use of the data for any unrelated data questions or projects is not allowed.
- ☐ I agree that I will shred and/or put in secured (locked) recycle bins any printouts with patient-level or unsuppressed data.
- ☐ I agree that I will not email any unsuppressed charts, tables, graphs or other summary data.
- ☐ I agree that I will not provide copies of the original data or derivations of these data files for any individual who is not an authorized party of the research project.
- ☐ I agree that it is my responsibility to seek out help from the UM Data Custodian or Health System's Privacy Office if I' am unclear or unsure about my data privacy and security obligations.
- ☐ I agree that I will completely destroy all original data files AND all derivations of these data files, including but not limited to, data summaries such as charts, tables, and graphs containing unsuppressed data, at the end of my involvement with the research project.
- ☐ I will transfer all data sources referred to in the above to another authorized member of the research project prior to destroying the files if the research project is still ongoing after my involvement ends.

Project Title: _____

PI: _____

**By signing below, I agree that I have read this entire document in its entirety and that I will abide by its terms and conditions.**

**Name (Printed)** **Signature** **Date**