Instructions for Completing the Limited Data Set Data Use Agreement (DUA) (CMS-R-0235L)

Contents

Section 8b.

The User may not disclose the limited data set file(s) specified in section 4 of this Agreement to a Secondary User until and unless the Secondary User enters into a DUA with CMS. CMS will only enter into a DUA with a Secondary User if the purpose for which the secondary use of the limited data set file(s) is consistent with the purpose specified in Section 3 of this Agreement.

Section 3.

The User represents that the limited data set files in section 4 above will be used solely for the following research purpose (provide a brief summary of the purpose below):
Using Machine Learning to Predict High Utilizers of Healthcare

Section 4.

The following CMS limited data set file(s) is/are covered under this Agreement.

File	Year(s)
Master Beneficiary Summary (Annual) File	2Q 2017 – 3Q 2018
Carrier Standard Analytic File	2Q 2017 – 3Q 2018
Home Health Standard Analytic File	2Q 2017 – 3Q 2018
Hospice Standard Analytic File	2Q 2017 – 3Q 2018
Inpatient Standard Analytic File	2Q 2017 – 3Q 2018
Outpatient Standard Analytic File	2Q 2017 – 3Q 2018
Skilled Nursing Facility Standard Analytic File	2Q 2017 – 3Q 2018

Section 9.

The User agrees to establish appropriate administrative, technical, and physical safeguards to protect the confidentiality of the limited data set file(s) and to prevent unauthorized use or access to it. The safeguards shall provide a level and scope of security that is not less than the level and scope of security established by the Office of Management and Budget (OMB) in OMB Circular No. A—130, Appendix III, Security of Federal Automated Information Systems http://www.whitehouse.gov/omb/circulars/a130/a130.html) [now: https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf], which sets forth guidelines for security plans for automated information systems in Federal agencies. The User acknowledges that the use of unsecured telecommunications, include the Internet, to transmit individually identifiable or deducible information derived from the limited data set file(s) must not be physically moved or electronically transmitted in any way from the site indicated in section 15 without prior written approval from CMS.

Attachment A.

Data Management Safeguards

Nascate adheres to NIST 800-53 for its IT Security posture. In addition, Nascate relies upon several policies, procedures, standards, and testing to secure its data. With the main focus on Nascate Privacy Manual and Nascate Technical Security Policy, Nascate has implemented technical, administrative, and physical controls for the safeguarding of data.

A sampling of these controls includes:

- Access Control
- Logging
- Monitoring
- Firewall
- Intrusion Detection and Prevention
- Antivirus
- Encryption
- Two-Factor Authentication
- System Hardening
- Risk Assessment
- Data Classification
- Awareness and Training
- Incident Response

Key Personnel

I, Kevin Buchan Jr. (user of the data), and Walt Mykins (custodian of the data) will be the only personnel who will have access to the data, except for temporary access granted to limited personnel deemed essential in the processing of the data.