Investigator:	
Date	
Project title:	

SEER-MEDICARE DATA USE AGREEMENT (DUA)
PRINCIPAL INVESTIGATOR

Information pertaining to an individual's health status and medical treatment is sensitive. Therefore, specific laws, including the Privacy Act of 1974 and the Health Insurance Portability and Accountability Act of 1996, have been enacted to ensure the confidentiality of health information. In utilizing health data for research purposes, it is absolutely necessary to ensure, to the extent possible, that uses of such data will be limited to research. Uses for any other reason, particularly those resulting in personal disclosures, will be prosecuted to the full extent of the law. In addition, release of information about providers, i.e., the physicians and hospitals that provide care for cancer patients, may compromise the willingness of these providers to cooperate with the activities of the cancer registries. Therefore, considerations regarding the privacy of providers are also of great importance.

In order for the National Cancer Institute to provide the linked SEER-Surveillance, Epidemiology and End Results (SEER)-Medicare data to you, it is necessary that you agree to the following provisions:

1. You agree that the statements and methods made in your attached research proposal are complete and accurate.

2. You will not use the data for purposes other than described in your research proposal.

3. You will not permit others to use the data except for collaborators at your institution involved with the research as described in your proposal. Access to the SEER-Medicare data shall be limited to the minimum number of individuals necessary to achieve the purpose stated in your proposal. The specific location details of where the data will be stored must be provided in your proposal's data storage and management plan. If you plan to move the data to a new location at your institute you must contact NCI in writing prior to moving the data for instruction on how to handle the SEER-Medicare data.

4. You will establish and maintain the appropriate administrative, technical, and physical safeguards to protect the confidentiality of the data and to prevent unauthorized use or access to it, as described in your proposal. 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, which sets forth guidelines for security plans for automated information systems in Federal agencies.

5. You agree not to place the SEER-Medicare data on personal computers, portable devices and removable media without permission. Portable devices include any non-fixed equipment that contains an operating system which may be used to create, access or store SEER-Medicare data. This includes but is not limited to laptops, personal digital assistants (PDAs), and smart phones. Removable media include, but are not limited to CDs, DVDs, MP3 players, removable memory,

and USB drives (thumb drives). If approved, all data stored on any of these devices must be password protected AND encrypted. Approved encryption standards must be FIPS-140 compliant and include Advanced Encryption Algorithm (AES) that uses a 128, 192, or 256-bit key size. In the event that the data are lost or stolen, you agree to report the loss to the SEER-Medicare contact within 24-hours/first business day of discovering the loss. Cloud storage does not meet privacy rules and is not acceptable for storing SEER-Medicare data.

6. You may use an institutionally provided VPN to link to a time-sharing system for data access. In this case, the remote PC may support the VPN, but the SEER-Medicare data must remain on the institution's server. Additionally, access to the VPN shall be restricted to persons residing in the United States

7. You will store all media on which the SEER-Medicare data are delivered in a secure location, such as a locked file cabinet in a locked office, only accessible by you or appropriate designated staff.

8. You must maintain all datasets containing restricted variables physically separate from any other SEER-Medicare files. Separate access controls with strong user authentication (username/password, digital certifications, etc.) must be established to allow limited access to these files. You should be able to track all access to these files.

9. All SEER-Medicare data must reside at your institution under your purview. If you plan to leave this institution, you must contact NCI in writing prior to the transition for instructions on how to handle the SEER-Medicare data. You may not duplicate any SEER-Medicare files prior to the transition nor can you take SEER-Medicare data with you without written permission from NCI. All files under your purview must be destroyed prior to your departure or someone must agree to assume the responsibilities of the PI as described in this document.

10. You will not attempt to link nor permit others to link the SEER-Medicare data with individually identified records in another database without the written consent from the applicable SEER registries.

11. No one having access to the data will attempt to learn the identity of any persons with cancer in these data and/or their physicians or treating hospitals. If you discover or are able to deduce the identity of a specific patient or provider (individual or institution), you agree that you will not attempt to contact these individuals or institutions.

12. No findings or information derived from the SEER-Medicare data may be released if such findings contain any combination of data elements that might allow the deduction of a patient's or providers' (individual or institution) identity. Numbers less than 11 (eleven) must be suppressed. Also, no use of percentages or other mathematical formulas may be used if they allow the derivation of patient, facility, or provider counts less than 11. Mapping of data related to reflect incidence, treatment, or survival at the registry-specific level or at other small areas is not permitted without prior approval from NCI and the involved registries. Although it is permissible to report registry names with registry-specific cancer rates (e.g., incidence, complications, mortality), registry names must be anonymized when reporting the quality or completeness of registry-specific data (e.g., case or treatment ascertainment). You agree that NCI shall be the sole judge as to whether the anonymization sufficiently precludes one from identifying or deducing the identity of a specific patient, provider (individual or institution) or registry with a reasonable degree of certainty.

13. You agree to provide a copy of all manuscripts to NCI for review and comment prior to publication submission. You further agree not to submit such findings to any third party prior to completion of NCI review. NCI agrees to complete the manuscript review process within 4 weeks of receiving any manuscript. NCI's review of the manuscript is for the sole purpose of assuring that data confidentiality is maintained (e.g., individual patients and/or providers cannot be identified) and that the focus of the manuscript was outlined in the approved SEER-Medicare proposal. Revisions will be necessary, if NCI determines that the format in which data are presented may result in identification of individual patients and/or providers or if the scope of the manuscript is not consistent with the approved proposal.

14. If requesting Oncotype Dx data, you agree to allow NCI to share your application for SEER-Medicare data and any manuscripts or reports that result from the analyses of such data with Exact Sciences (formerly Genomic Health), the company that developed the Oncotype Dx Assay. These documents will be shared with GHI for informational purposes only; all approval processes will be handled by NCI

15. You agree that in the event NCI determines or has a reasonable belief that you have violated any terms of this agreement, NCI may request that you destroy the data and all derivative files and send a certificate/ notification of destruction to NCI. You understand that as a result of NCI's determination or reasonable belief that a violation of this agreement has taken place, NCI may refuse to release further SEER-Medicare data to you for a period of time to be determined by NCI.

16. All files received may be retained for a maximum of five years. At the completion of the project or five years from receipt all files including all back-up files and original media must be destroyed and notification of destruction must be sent to NCI. Investigators who need to retain files beyond that period must contact NCI.

Please indicate the SEER-Medicare files you will use:

☐	Cancer File	Years	
☐	5% Cancer File	Years	
☐	Master Beneficiary Summary File (MBSF) Base A/B/C/D	Years	1999-2019
☐	Chronic Conditions Flags	Years	
☐	Other Chronic or Potentially Disabling Conditions	Years	
☐	Plan Characteristics File	Years	
☐	MedPAR	Years	
☐	Carrier Claims (NCH)	Years	
☐	Outpatient	Years	
☐	Home Health Agency (HHA)	Years	
☐	Hospice	Years	
☐	Durable medical equipment (DME)	Years	
☐	Part D Event (PDE) - with Drug Characteristics File appended	Years	
☐	Formulary File	Years	
☐	Prescriber Characteristics and Bridge File	Years	
☐	Pharmacy Characteristics and Bridge File	Years	
☐	Part D Medication Therapy Management File	Years	
☐	Minimum Data Set (MDS)	Years	
☐	Outcome and Assessment Information Set (OASIS)	Years	
☐	MD-PPAS (Medicare Data on Provider Practice and Specialty)	Years	
☐	Hospital Characteristics File	Years	
☒	Geographic – zip code/census tract files (automatically provided)	Years	1999-2019

These files will include:

☐ Cancer cases ☐ Non-cancer cases

Signature of Principal Investigator (In the case of students and fellows, the department chair or advisor from the student's academic institution must sign the data request)

Your signature indicates that you agree to comply with the above stated provisions. Deliberately making a false statement regarding any matter within the jurisdiction of any department or agency of the Federal Government violates 18 USC 1001 and is punishable by a fine up to $10,000 or up to five years in prison.

Name – (printed or typed)
Institution/Organization
Street Address
City/State/ZIP code
Phone number – including Area Code
Email address
Signature
Date