Request Name: _____

Project Title: _____

Primary Investigator: _____

Data Use Agreement
SEER Specialized Databases

Version	Implementation Date	Summary of Changes	Sections Updated	Changes Approved By
1.0	01/21/2026	Initial release	All	SRP leadership

This SEER Research Data Use Agreement (the "Agreement") outlines the terms for access to data in the National Institutes of Health (NIH) Surveillance, Epidemiology, and End Results (SEER) Specialized Databases (collectively, the "Databases"). The parties to this Agreement include the NIH, the "Data Access Requestor" indicated in the Data Access Request, and the Data Access Requestor's Institution as represented by the Institutional Signing Official (SO). The effective date of this Agreement is the date of Data Access Requestor's and Institutional Signing Official's signatures ("Effective Date").

PREAMBLE

1. The NIH has established NIH-designated cloud-based data repositories for securely storing and sharing data collected by the National Cancer Institute (NCI) SEER Program. The SEER Program developed the SEER Specialized Databases to support research and makes the Databases available through the SEER*Stat software or Virtual Cancer Data Access System (VCDAS). SEER Specialized Databases are controlled access data.

2. Data Access Requestor wishes to access the Databases for research. This Agreement governs Data Access Requestor's use and disclosure of data obtained from the Databases and data derived from that data (collectively referred to in this Agreement as "Data").

AGREEMENT AND TERMS OF USE

Restricted Use and Disclosure

The Data Access Requestor agrees to use the Data only for the purpose for which it was approved by the SEER Specialized Database Data Access Committee (DAC). If the Data Access Requestor wishes to investigate a different research question related to previously approved use of a SEER Specialized Database, a new data request must be submitted and approved by the SEER Specialized Database DAC.

Compliance

The Data Access Requestor agrees to use Data in full compliance with all applicable laws and NCI policies and guidance documents. To the extent NCI policies or guidance documents are inconsistent with the terms of this Agreement, the terms of this Agreement will supersede NCI policies or guidance.

No Data Linkage

The Data Access Requestor agrees **not** to link or attempt to link the Data with information in another database at the individual level, nor will they permit others to do so. This includes, but is not limited to, links or attempts to link two or more SEER Databases to which the Data Access Requestor has access.

Non-identification

Data Access Requestor agrees not to use controlled-access data sets obtained through the Data Access Request, either alone or in concert with any other information, to identify or contact individuals whose Data are contained in the Databases. These provisions do not apply to individual SEER registries which operate under state specific statues. All Data Access Requestor(s), conducting "human subjects research" within the scope of 45 CFR 46 must comply with the requirements contained therein. If the Data Access Requestor or any other person inadvertently discovers the identity of an individual whose Data is in the Databases, the Data Access Requestor will: (a) make no use of this knowledge, including informing others of the discovered identity, *aside from the* NCI Surveillance Research Program (SRP), (b) not contact any individual, and (b) notify all parties **UNDER SECTION Data Security and Unauthorized Data Release below.** The Data Access Requestor agrees not to generate information from Data that could allow the identities of individuals to be readily ascertained.

The Data Access Requestor will **not** attempt to identify or infer any geographic area if they are not specifically released in the SEER Specialized Database (e.g. identify state, registry, or county, etc. if they are not included in the specific SEER Specialized Database).

The Data Access Requestor will **not** attempt to identify or infer any data source or individual healthcare provider or healthcare facility (e.g. hospital, laboratory, oncology office, etc.).

Non-Transferability

The Institutional Requestor and Data Access Requestor agree to retain control of NIH controlled-access data accessed through the request and further agree not to distribute controlled-access data to any entity or individual not identified in the approved request. If the Data Access Requestor is provided access to controlled-access data for inter-institutional collaborative research described in the Research Use Statement of the Data Access Request, and all members of the collaboration are also Data Access Requestors through their home institution(s), data obtained through the Data Access Request may be securely transmitted within the collaborative group. Each Data Access Requestor and their Institutional Requestor will secure the data according to the NIH Security Best Practices for Users of Controlled-Access Data, the terms of this Agreement, and the Institutional Requestor's IT security requirements and policies.

The Institutional Requestor and Data Access Requestor acknowledge responsibility for ensuring the review and agreement to the terms within this Agreement that apply to them and the appropriate research use of controlled-access data obtained through the Data Access Request, subject to applicable laws and regulations. The Institutional Requestor and Data Access Requestor agree that controlled-access data obtained through the Data Access Request, in whole or in part, may not be sold to any individual at any point in time for any purpose.

The Institutional Requestor must have policies and procedures to ensure that the Data Access Requestor completes the Project Close-out process (See Termination and Data Destruction Provision) before moving to a new institution. If a Data Access Requestor moves to a new institution without completing the Project Close-out

process, the Institutional Requestor must immediately notify the relevant NCI SEER Specialized Databases DAC at NCISEERSpecializedDatabasesDAC@nih.gov so that the project may be closed out and the data are destroyed according to NIH Security Best Practices for Users of Controlled-Access Data. A new Data Access Request, in which the new Institutional Requestor agrees to the Data Use Agreement, must be approved by the relevant NCI SEER Specialized Databases DAC(s) before controlled-access data may be re-accessed by the Data Access Requestor.

Data Security and Unauthorized Data Release

The Institutional Requestor and Data Access Requestor acknowledge NIH's expectation that they have reviewed and agree to manage the requested controlled-access data according to NIH's expectations set forth in the current NIH Security Best Practices for Users of Controlled-Access Data and the Institutional Requestor's IT security requirements and policies.

The Institutional Requestor or Data Access Requestor agree to notify the NIH Incident Response Team, NIH SEER Specialized DBs DAC at NCISEERSpecializedDatabasesDAC@nih.gov on the project request, and the NIH Data Management Incident (DMI) Notification inbox of any unauthorized data sharing, breaches of data security, identification of individuals in the Data or inadvertent data release that may compromise data confidentiality within 24 hours of when the incident is identified. For the NIH Incident Response Team, notifications can be made by phone (301) 496-HELP (4357); Toll Free Number: (866) 319-4357or TTY: (301) 496-8294 and can also be sent by email to NIHInfoSec@nih.gov or via the Report an Incident Link: https://irtportal.ocio.nih.gov/. For the NIH Data Management Incident (DMI) Notification inbox, email DMI_OER@mail.nih.gov.

As permitted by law, notifications should include any known information regarding the incident and a general description of the activities or process in place to define and remediate the situation fully. Within 3 business days of the notification, the Institutional Requestor and the Data Access Requestor agree to submit to the NIH SEER Specialized Databases DAC(s) and the NIH Data Management Incident Notification inbox a detailed written report including the date and nature of the event, actions taken or to be taken to remediate the issue(s), and plans or processes developed to prevent future incidents, including specific information on timelines anticipated for action. The Institutional Requestor and the Data Access Requestor agree to provide documentation verifying that the remediation plans have been implemented. Repeated violations or unresponsiveness to NIH requests may result in further compliance measures affecting the Institutional Requestor and/or the Data Access Requestor(s).

The NIH, or another entity designated by the NIH may, as permitted by law, also investigate any data security incident or policy violation. The Institutional Requestor and Data Access Requestor and their associates agree to support such investigations and provide information, within the limits of applicable local, state, Tribal, and federal laws and regulations. In addition, the Institutional Requestor and Data Access Requestor agree to work with the NIH to ensure that plans and procedures that are developed to address identified problems are mutually acceptable and consistent with applicable law.

Prohibited use of AI Tools and AI APIs

This Agreement explicitly prohibits any individual who has obtained Data from sharing raw data, specifically participant-specific data, with any other individual or entity that is not described in the data request, in any forum, in any medium. The use of AI tools, including generative and analytical models, pose a genuine risk of inadvertent data sharing due to the nature of how AI tools process, store, and regenerate information. AI tools, including but not limited to those with public-facing interfaces, including, but not limited to: proprietary Large Language Models (LLMs) such as OpenAI GPT Series, Google Gemini, Anthropic Claude or similar and open-source models such as Meta Llama, Mistral AI, DeepSeek, Qwen, and similar platforms, usually do not offer guarantees regarding the containment of data inputs. Any data input into a prompt or output generated from a prompt could result with proprietary data infringed, sent, saved, viewed, misinterpreted, or used in unforeseen public ways. As a result, the use of such AI tools which may release individual-level data to others, is in direct violation of this Agreement.

Approved Users of controlled-access data may develop or validate analytical and generative AI models using the controlled-access data so long as the use is described in an approved data request and performed on infrastructure compliant with NIH Best Practices for Users of Controlled Access Data. Use of public cloud AI services, browser-based AI assistants, or any tool that transmits data to an external provider is expressly forbidden. Approved Users must maintain records of all AI/ML tools and workflows used with controlled-access data, including software versions, usage logs, and locations of processing, and must provide such records to the NIH upon request. Approved Users may not share the model, including model parameters, except with collaborators who are also Approved Users and may not retain the AI model, including model parameters, upon closeout of the project. Approved Users may request to renew any expiring projects in order to continue using analytical and generative AI models. Approved Users may NOT use controlled-access data with any AI-powered product or service that transmits data outside of their secure computing environment, or that retains, reuses, or incorporates data for purposes other than the expressly permitted research activities approved in the Data Access Request. Therefore, controlled-access data may be analyzed using AI tools which provide guarantees that all data is safeguarded, contained, and will not be released to others. Prior to submission for publication or external presentation of any results derived from AI analyses involving controlled-access data, the outputs must be reviewed by a qualified human to ensure that no controlled-access data is disclosed, intentionally or unintentionally, in the publication or presentation.

Terms of Access Violations

The Institutional Requestor and Data Access Requestor acknowledge that the NIH may terminate the Data Access Request, including this Agreement, and immediately revoke or suspend the Institution's or the Data Access Requestor's access to all controlled-access datasets at any time if the Institutional Requestor and/or Data Access Requestor is found to be no longer in compliance with the terms described in this Agreement, or the policies, principles, and procedures of the NIH. The NIH may apply for injunctive or other equitable relief before courts of competent jurisdiction as remedy for breach of the Agreement, in addition to all other remedies available at law or in equity.

The Institutional Requestor or Data Access Requestor(s) agree to notify the SEER SD DAC at NCISEERSpecializedDatabasesDAC@nih.gov indicated in this Agreement, and the NIH Data Management Incident Notification inbox of any terms of access violations, hereinafter referred to as data management

incidents (DMIs), within 24 hours of when the incident is identified. For the NIH Data Management Incident Notification inbox, notifications can be sent to DMI_OER@mail.nih.gov. As permitted by law, notifications should include any known information regarding the incident and a general description of the activities or process in place to define and remediate the situation fully.

Within 3 business days of the notification(s), the Institutional Requestor and the Data Access Requestor agree to submit to the SEER Specialized Database DAC(s) indicated on the project request and the NIH Data Management Incident Notification inbox a detailed written report including the date and nature of the event, actions taken or to be taken to remediate the issue(s), and plans or processes developed to prevent future incidents, including specific information on timelines anticipated for action. The Institutional Requestor and the Data Access Requestor agree to provide documentation verifying that the remediation plans have been implemented. Repeated violations or unresponsiveness to NIH requests may result in further compliance measures affecting the Institutional Requestor and/or the Data Access Requestor.

As outlined in Term "Data Security and Unauthorized Data Release", all notifications of unauthorized data sharing, breaches of data security, or inadvertent data releases should also be sent to the NIH Incident Response Team. For the NIH Incident Response Team, notifications can be made by phone (301) 496-HELP (4357); Toll Free Number: (866) 319-4357or TTY: (301) 496-8294 and can also be sent by email to NIHInfoSec@nih.gov or via the Report an Incident Link: https://irtportal.ocio.nih.gov/.

The NIH, or another entity designated by the NIH, may, as permitted by law, also investigate any DMI. The Institutional Requestor and the Data Access Requestor and their associates agree to support such investigations and provide information, within the limits of applicable local, state, Tribal, and federal laws and regulations. In addition, Institutional Requestor and Data Access Requestor agree to work with NIH to assure that plans and procedures that are developed to address identified problems are mutually acceptable and consistent with applicable law.

Termination and Data Destruction

Upon Project Close-out, the Institutional Requestor and Data Access Requestor agree to destroy all copies and versions of the dataset(s) retrieved from NIH controlled-access data repositories

regardless of the storage medium or format in accord with the NIH Security Best Practices for Users of Controlled-Access Data. However, the Data Access Requestor may retain these data as necessary to comply with law, regulation, and government policy. A Data Access Requestor who retains data for any of these purposes, and their Institutional Requestor, continue to be a steward of the data and is responsible for the management of the retained data in accordance with the NIH Security Best Practices for Users of Controlled-Access Data, and any institutional policies.

After termination of the approved research project, the data may not be used to answer any additional research questions, even if they are within the scope of the approved Data Access Request, unless the Data Access Requestor submits a new Data Access Request and is approved by the NIH to conduct the additional research. If a Data Access Requestor retains data for any of these purposes, the Institutional Requestor and the Data Access Requestor are bound by the terms for Non-Identification,, Non-transferability, Data Security and Unauthorized Data Release, Terms of Access Violations, and Termination and Data Destruction until the data is destroyed.

Non-Endorsement, Indemnification

The Institutional Requestor and the Data Access Requestor acknowledge that although all reasonable efforts have been taken to ensure the accuracy and reliability of controlled-access data accessed through the request, the NIH and SEER registries do not and cannot warrant the results that may be obtained by using any data included therein. NIH and all contributors to these datasets disclaim all warranties as to performance or fitness of the data for any particular purpose.

No indemnification for any loss, claim, damage, or liability is intended or provided by any party under this agreement. Each party shall be liable for any loss, claim, damage, or liability that said party incurs because of its activities under this agreement, except that the NIH, as an agency of the United States, may be liable only to the extent provided under the Federal Tort Claims Act, 28 USC 2671 et seq.

Public Posting of Approved Users' Research Use Statements

The Institutional Requestor and the Data Access Requestor agree that information about themselves and the approved research use may be posted publicly on the SEER Specialized Database website. The information may include the Data Access Requestor's name and Institutional Requestor, project name, and Research Use Statement. Citations of publications resulting from the use of controlled-access data obtained through the Data Access Request may also be posted on the SEER website. The Data Access Requestor agrees that the NIH may use information provided in the DAR and other application materials for purposes of enforcing this Agreement and administering the NCI SEER Program.

Software

For all software provided to Data Access Requestor by the NCI Surveillance Research Program ("NCI Software"), the Data Access Requestor will not copy, distribute, reverse engineer, sell, lease, or incorporate NCI Software into any other software system.

Publications

The Data Access Requestor will not present or publish Data or the results of research conducted with Data in which an individual can be identified. Data Access Requestor will not publish information on an individual, including information generated by the case listing session of SEER*Stat, even if such information cannot directly identify an individual. The Data Access Requestor will follow all NCI policies, including any policy on small cell sizes. Statistics about any geography (county, state, registry) or demographic information (age, sex, race/ethnicity) based on counts 1 to 4 must be suppressed in all publications. Upon NIH request, authorized users will send a copy of any manuscript or book chapter generated through analysis conducted with the Databases.

Required Acknowledgments

The Data Access Requestor agrees to acknowledge the Databases and specific version of the dataset(s) analyzed, in all oral and written presentations, disclosures, and publications resulting from any analyses of Data. The appropriate citation is associated with the data file used, which may be found in Suggested Citations on the SEER*Stat Help menu.

TERMS AND DEFINITIONS

Approved Users: An individual or individuals who are named in the Data Access Request and have been approved to access the Data, but whom are not Collaborators (e.g. they are lab technicians, trainees, doctoral candidates, and post-doctoral or graduate students).

Collaborator: An individual whose identity has been validated and who is a permanent employee of their institution at a level equivalent to, but not limited to, that of an academic professor (e.g., assistance, associate, or non-tenure or tenure-track professor) or senior researcher, who is not under the direct supervision of the Data Access Requestor, who assists with the research project involving controlled-access data. This cannot be a lab technician or trainee, e.g., post-docs or graduate students. Internal collaborators are employees of the Institutional Requestor and work at the same institution as the Data Access Requestor. External collaborators are not employees of the Institutional Requestor and do not work at the same location as the Data Access Requestor.

Data Access Request: A request submitted to a SEER Specialized Database DAC for a specific research use specifying the data to which access is sought, the planned research use, and the names of collaborators.

Data Access Requestor: The individual who prepares and submits requests, Project Renewals, and Project close-outs. A Data Access Requestor is a permanent employee of their institution at a level equivalent to, but not limited to, that of an academic professor (e.g., assistance, associate, or non-tenure or tenure-track professor) or senior researcher; has oversight responsibility for others named on the request who will be granted access to the data; and can be accountable for ensuring that all aspects of data usage align with the terms of the agreement. This cannot be a lab technician or trainee, e.g., post-docs or graduate students.

Data Use Agreement (DUA): Terms of access that include how the data accessed should be secured and used by the Data Access Requestor, those they directly supervise, and any collaborators. The Institutional Requestor, through the Institutional Signing Official (SO), and the Data Access Requestor, are each signatories to the agreement and agree to adhere to terms of access.

Institutional Requestor: The home institution or corporation of the Data Access Requestor.

Institutional Signing Official: The label, “Institutional Signing Official” refers to the individual that has institutional authority to legally bind the institution in administrative matters. The individual fulfilling this role may have any number of titles in the institution but is typically located in its Office of Sponsored Research or equivalent

SEER Specialized Database Data Access Committee (DAC): SEER Specialized Database Data Access Committees (DACs) review and approve, or disapprove, requests from Data Access Requestors for proposed secondary research uses of controlled-access datasets.

Project Close-out: Termination of a research project that used controlled-access data from an NIH controlled-access data repository and confirmation of data destruction when the research is completed and/or discontinued.

Project Renewal: Renewal of a Data Access Requestor’s access to controlled-access datasets for a previously approved project with options to add or remove datasets, collaborators, or Key Personnel.

Progress Update: Information included with the Project Renewal or Project Close-out providing a summary of research progress and citing any presentations or publications with the approved controlled-access data.

Research Use Statement: A summary of research intent submitted by the Data Access Requestor that includes information about at least the following: research objectives, study design, and analysis plan.

SIGNATURE

Digitally certified institutional signatures are preferred.

By: _____

Name: _____

Title: _____

Organization: _____

Email: _____

Date: _____