TCR requires additional data security measures to comply with the [Texas Cancer Incidence Reporting Act, Health and Safety Code, Chapter 82](https://www.dshs.texas.gov/tcr/lawrules.aspx). Steps must be taken to protect the confidentiality of the data during and after the study, including presentation of results. Presentation of results must comply with the [TCR Data Release Policy](https://www.dshs.texas.gov/tcr/data/policy.aspx).

Complete the Data Security and Confidentiality Agreement for each PI and/or any named collaborators with a copy of the data located at another institution.

**Institution Name:** Click or tap here to enter text.

**List location(s) where TCR data will be physically located at your institution** *(e.g., one or more non-portable and/or portable computers, a password-protected server accessed by how many computers, etc.).*

Click or tap here to enter text.

**List the individuals who will have access to the data at your institution.**

Click or tap here to enter text.

**Attach certification of human subjects training for each person listed above. Certification must be current; please check expiration date. *(List file names below.)***

Click or tap here to enter text.

**Initial each item listed below confirming plan to secure TCR data (and copies) physically, electronically, and administratively.**

|  |  |
| --- | --- |
| Initials | Access to data is limited to authorized personnel only. |
| Initials | Data is stored in locked cabinets or rooms. |
| Initials | Computers accessing data are password protected. |
| Initials | Computers are maintained with current operating system, applications, and security patches. |
| Initials | Antivirus application has current virus signatures running. |
| Initials | Computers accessing and/or storing TCR data are limited to work use only. |
| Initials | TCR data transported on a laptop or other portable electronic device will be encrypted, shipped via traceable courier, and never left unattended. |
| Initials | TCR data will never be transmitted via email or email attachment, including encrypted messages. |
| Initials | Upon study completion, all TCR data and copies will be securely shredded and completely wiped from all computers, servers, and electronic media. |
| Initials | After securely destroying all TCR data and copies, the PI will complete and submit to the TCR a [Certificate of Texas Cancer Registry Data Destruction](https://www.dshs.texas.gov/tcr/data/research/Certificate-of-TCR-Data-Destruction.docx). |

TCR Confidentiality Agreement

Cancer Epidemiology and Surveillance Branch

Texas Department of State Health Services

1. The data will be treated as strictly confidential.[[1]](#footnote-1)
2. The data will not be used for any purpose other than that specifically set forth in the approved IRB application.
3. The data will not be made available to any other individual, agency, institution, or firm and controls will be maintained to prevent unauthorized access.
4. No follow back of any type will be made to any individual, institution, or firm without prior Texas Department of State Health Services, Institutional Review Board approval.
5. All results of a study will be restricted to aggregate data and will not identify any individual, institution, or firm.
6. Confidential data will be destroyed or returned to the TCR after serving the purpose set forth above unless specific authority is granted for their retention.
7. The Texas Cancer Registry, Texas Department of State Health Services will be credited as the source of the data.
8. Copies of all abstracts and publications will be furnished to the Texas Cancer Registry within 60 days of presentation or publication.

By signature below of an administrative officer authorized to make such binding commitments, the sponsoring agency, institution, or firm assures compliance with the above conditions.

Insert image of signature or print, sign, and scan completed document.

Signature

Click to enter text.

Date

Click to enter text.

Print Name

Click to enter text.

Title

Click to enter text.

Address

Click to enter text.

Phone Number

1. Federal agencies which are subject to the Federal Freedom of Information Act and the Federal Privacy Act will not release confidential identifying data except as is required by those acts. [↑](#footnote-ref-1)