Virtual Pooled Registry Cancer Linkage System (VPR-CLS)

Checklist of Cancer Registry Security Protections

This form is to be completed by each participating registry and maintained on file within the VPR-CLS to document adequate security protections for study data that are downloaded and used for linkages.

Name of Registry: Click here to enter text.

1. On what type of computer system will the study data be stored and used? Please answer this for each computer on which the data will be stored or used. Check all that apply.

   ☐ Laptop with an encrypted hard drive

   ☐ Personal/home-user computer

   ☐ Institutional stationary computer not connected to network or internet

   ☐ Institutional stationary computer connected to network or internet

   ☐ Institutional network servers

2. Please list the **titles of all individuals** who will access study data files, including the registry VPR Liaison.

   Click here to enter text.

Affirmative answers to all of the questions below will certify your registry compliance with the necessary security protections. If you cannot check a box to confirm compliance, please contact Castine Clerkin at NAACCR, cclerkin@naaccr.org .

3. Confidentiality agreements:
   ☐ All users of the data sign confidentiality agreements as part of routine registry procedures
   ☐ All users of the data receive training on proper procedures for working with patient-level data

4. System Controls to limit access to the data:
   ☐ Network folder or data file permissions will be set to allow access by only authorized personnel

5. Computer system security plan:
   ☐ A security plan exists for this computer system providing for protection of patient-level data

☐ PII/PHI are encrypted both in transit and at rest

6. Virus protection software:

   ☐ The computer system uses the following antivirus software (include version):

   Click here to enter text.

   ☐ The virus definitions used by the software have been updated within the last 30 days and the software automatically checks for updates at least once a week

7. Firewall:
   ☐ The organization's network system is protected by a firewall
   ☐ The individual computer system has the operating system firewall or some other software firewall activated

8. Computer locking:
   ☐ The computer automatically locks, requiring a password to unlock, after no more than 20 minutes of inactivity
   ☐ Institution requires strong passwords (length and complexity), has rules for password expiration/renewal, and limits unsuccessful login attempts

9. Physical security:
   ☐ Physical access to the servers and/or computers is restricted to authorized personnel
   ☐ The computer is located in a room inaccessible to the general public (with at least one locked door) when not in use

10. Securing electronic copies:
    ☐ All electronic copies of the patient-level data files on removable media will be secured in a locked cabinet or room accessible only to authorized users when not in use

11. Securing paper copies:
    ☐ All paper materials containing patient-level data records will be secured in locked offices and/or locked filing cabinets when not in use and otherwise protected from loss or unauthorized release while in use, and will be shredded before disposal

Completed by (Name/Title): **Click here to enter text.**

Date Completed: **Click here to enter text.**