SRTR | SCIENTIFIC REGISTRY OF
TRANSPLANT RECIPIENTS

Security Plan

for data use agreement

Project number (SRTR use only):
Date:

_____

Recipient name _____

1. On what type of computer system will the 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

2. Please list the full names and titles of all individuals who will be accessing this data.

<u>**Affirmative answers to all of the questions below will certify your compliance with the security agreement.**</u> **If you cannot check a box to confirm compliance, please contact the SRTR to discuss your situation.**

3. **Confidentiality agreements:**
    ☐ All users of the data will sign confidentiality agreements
    ☐ 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:**
    ☐ 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

6. **Virus protection software:**
    ☐ The computer system uses the following antivirus software (include version):
        _____

 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

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 (including original CDs) 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 when not in use and otherwise protected from loss or unauthorized release while in use, and will be shredded before disposal