SOP: Personally Identifiable Information (PII) Research Data Protections				
NUMBER	DATE	AUTHOR	APPROVED BY	PAGE
PRDP-002	10/25/2020	Mary M. A. Potter	Lisa M. Lee	1 of 8

1 PURPOSE

1.1 This standard operating procedure establishes the safeguards recommended for the collection, storage, disclosure, and disposition of personally identifiable information (PII). PII refers to any data or information about an individual that might reveal the identity or personal information or that could allow someone (whether part of the research project or an external person who gains access to the data) to directly identify a participant.

2 REVISIONS FROM PREVIOUS VERSION

2.1 None

3 POLICY

3.1 Virginia Tech researchers and study personnel are required to:

- 3.1.1 Protect research participants from harm that might result from unintended disclosure of or inappropriate use of confidential data.
- 3.1.2 Uphold the assurance of confidentiality given to the participants.
- 3.1.3 Adhere to the requirements specified in sponsorship or data use agreements.
- 3.1.4 Use optimal technology and storage and use methods to protect data securely without imposing unwarranted or excessive burdens on the research.
- 3.1.5 Disclose to research participants the protections afforded their data.

3.2 The type of PII collected, stored, or disclosed will determine the level of risk to participants and the safeguards required to mitigate that risk (please see **PRDP-001-SOP-Definitions** for specific examples of PII identifiers).

- 3.2.1 **Benign** information about individually identifiable persons
  - 3.2.1.1 Contains PII on human participants who have been given an assurance of confidentiality
  - 3.2.1.2 Accidental disclosure is unlikely to result in harm to participants
  - 3.2.1.3 The risks to the participant are be considered no greater than those associated with everyday life
- 3.2.2 **Moderately sensitive** information about individually identifiable persons
  - 3.2.2.1 Contains PII on human participants who have been given an assurance of confidentiality
  - 3.2.2.2 Could reasonably be expected to present a risk of civil liability, moderate psychological harm, financial harm, or material social harm to individuals or groups
  - 3.2.2.3 The risks to the research participant are considered greater than those associated with everyday life
- 3.2.3 **Very sensitive** information about individually identifiable persons
  - 3.2.3.1 Contains PII on human participants who have been given an assurance of confidentiality
  - 3.2.3.2 Could cause significant harm to an individual if exposed, including, but not limited to, serious risk of criminal liability, serious psychological harm or other significant injury, loss of insurability or employability, financial harm, or significant social harm to an individual or group
  - 3.2.3.3 The risks to the research participant are considered greater than those associated with everyday life
- 3.2.4 PII required for project management
  - 3.2.4.1 PII that is needed for project management but not needed for analysis must be separated from the data to be used for analysis at the earliest possible phase of the project by splitting the data into two files: one file containing the PII not needed for the analysis along with a unique ID that

is unrelated to personal characteristics, the other file containing the same unique ID and all of the data collected for the analysis. The common identifier in both data sets enables the researcher to re-link the PII and non-PII data at a future date, as the needs of the project require.

3.2.4.2 Removal of all PII (temporarily or permanently) significantly reduces the risk of harm to study participants but does not eliminate the potential for harm that might result from loss, theft, or unintended disclosure. Even when working with de-identified data, researchers should continue to use the minimum data protection standards outlined below.

4 RESPONSIBILITIES

4.1 All research staff (including student researchers) must ensure the security, confidentiality, and protection of research data.

4.2 The Principal Investigator of a research project (study, investigation) is the overall responsible party held accountable for the data security and protections of all research data.

5 PROCEDURE

5.1 Protections for **benign** information about individually identifiable persons include:

- 5.1.1 General guidelines
  - 5.1.1.1 Access
    - 5.1.1.1.1 Limit access to identifiable information to research personnel with a need to know.
  - 5.1.1.2 Printing
    - 5.1.1.2.1 Do not leave data or information unattended on copiers/printers.
    - 5.1.1.2.2 Send data or information to printers using stored/locked jobs where possible. Enter passcode at machine to print.
  - 5.1.1.3 Mailing paper-based information
    - 5.1.1.3.1 Put data or information in a closed envelope or box (if interoffice it must be placed in a sealed envelope inside the interoffice envelope).
    - 5.1.1.3.2 Send data or information via Interoffice or the US Postal Service.
  - 5.1.1.4 Storing electronic files on work or personal computer
    - 5.1.1.4.1 Computers must meet Virginia Tech security requirements for low risk data (See https://security.vt.edu/resources.html).
  - 5.1.1.5 Storing data/files on external portable storage media (USB, CD/DVD, back-up tape, etc.)
    - 5.1.1.5.1 Devices must be encrypted.
    - 5.1.1.5.2 Devices must be password protected.
  - 5.1.1.6 Sharing data/files with authorized individuals
    - 5.1.1.6.1 Share data or information with specific authorized individuals, not anonymous or guest links.
  - 5.1.1.7 Sending data/files to project staff or individuals under a data transfer arrangement
    - 5.1.1.7.1 Encrypt when transmitting data both internally and externally.
    - 5.1.1.7.2 Use a Virginia Tech supported secure file transfer methods (contact your departmental IT support for options within your area).
    - 5.1.1.7.3 On website forms, use HTTPS.

5.1.1.8 Deleting electronic files
- 5.1.1.8.1 Use standard delete commands.
- 5.1.1.8.2 Empty trash bin after deleting.
- 5.1.1.8.3 Ensure that backup or archive files are deleted or have a scheduled recycle period.

5.1.2 Data collection
- 5.1.2.1 Data collection might be performed using internet, email, electronic data collection mechanisms, mobile or in-person survey tools. The tools should be Virginia Tech reviewed and approved survey tools, anonymous on-line tools, or project email.
- 5.1.2.2 Additional safeguards might be required by the IRB.

5.1.3 Data storage
- 5.1.3.1 **Benign** PII must be stored on any of the following devices that are, at a minimum, configured to require users to authenticate themselves using login ID and password and only allow access to authorized project team members and system administrators. These include:
  - 5.1.3.1.1 A server or workstation configured in a manner that is consistent with Virginia Tech security practices
  - 5.1.3.1.2 Institute/Department or centrally managed network file storage
  - 5.1.3.1.3 A secure cloud storage system vetted by Virginia Tech IT Security Office
  - 5.1.3.1.4 Removeable media (external drive, USB) managed using an audited, check-out/check-in system.
    - 5.1.3.1.4.1 When not in use, storage media must be kept in a locked drawer or cabinet in a secured space (e.g., a central storage area or an authorized project team member's office), with key access required for both the office and the storage location.
  - 5.1.3.1.5 Data collected or stored on paper forms that have PII (such as signed consent forms or questionnaires) must be stored in a locked file cabinet in a secure office space or building.

5.1.4 Approved devices
- 5.1.4.1 Virginia Tech devices that house the hard drive on which the data are stored
- 5.1.4.2 Devices physically connected to a Virginia Tech external hard drive or removable medium on which the data are stored
- 5.1.4.3 Devices authorized to access a Virginia Tech shared network drive on which the data are stored, or
- 5.1.4.4 Devices authorized to connect to a physically secured and firewall-protected server (e.g., terminal server, Linux server accessed via SSH) that has access to the data

5.1.5 Network access
- 5.1.5.1 The file storage system must be in a physically secured space that preferably requires the presentation of a valid, authorized key or keycard to enter that space.
- 5.1.5.2 The storage device must be protected through a network access control mechanism, such as a hardware or software-based firewall or router-based access control lists.

5.1.5.3 Only system administrators responsible for the maintenance and management of the network-based storage media may have direct physical access to the storage system's hardware.

5.1.5.4 Anyone attempting to access **benign** PII either directly from the file server or remotely via a network connected client device must provide an authorized Virginia Tech computer account (PID) and its associated password.

5.1.5.5 Network-based data may be accessed via wired or wireless network connections.

5.1.5.6 All passwords must be encrypted wherever they are stored and when they are transmitted over the network.

5.1.5.7 It is recommended that **benign** PII transmitted across the network be encrypted in transit.

5.1.5.8 All encryption protocols and key lengths used must be approved by the Virginia Tech IT Security Office.

5.1.5.9 The practices for managing **benign** PII should be reviewed by the researcher and understood by the research team at the start of the data set's lifecycle, annually during the lifecycle of the data set, and at the end of the data set's lifecycle.

5.2 Protections for **moderately sensitive** (moderate risk) information about individually identifiable persons include:

5.2.1 General guidelines

5.2.1.1 Access

5.2.1.1.1 Same as for benign

5.2.1.2 Printing

5.2.1.2.1 Same as for benign

5.2.1.3 Mailing paper-based information

5.2.1.3.1 Same as for benign

5.2.1.4 Storing electronic files on work computers

5.2.1.4.1 Computers must meet Virginia Tech security requirements for moderately sensitive data, including device password, anti-virus, current patches, encryption, and remote wiping (see https://security.vt.edu/resources.html).

5.2.1.5 Storing files on external portable storage media (USB, CD/DVD, back-up tape, etc.)

5.2.1.5.1 Same as for benign

5.2.1.6 Sharing files with authorized individuals

5.2.1.6.1 Use approved collaboration tools.

5.2.1.6.2 Share with specific individuals, not anonymous or guest links.

5.2.1.7 Sending data/files to authorized individuals

5.2.1.7.1 Same as for benign

5.2.1.8 Deleting electronic files

Same as for benign

5.2.2 Data collection

5.2.2.1 Data collection must be performed using Virginia Tech reviewed and approved survey tools (e.g. Qualtrics, Red Cap, other).

5.2.2.2 Additional safeguards required by the IRB must be adopted.

5.2.3 Data storage

5.2.3.1 **Moderately sensitive** PII must be stored on any of the following devices that are, at a minimum, configured to require users to authenticate themselves using login ID and password and only allow access to authorized project team members and system administrators:

5.2.3.1.1 Same as for benign

5.2.4 Approved devices

5.2.4.1 Virginia Tech devices that house the hard drive on which the data are stored.

5.2.4.2 Virginia Tech devices physically connected to the external hard drive or removable medium on which the data are stored.

5.2.4.3 Virginia Tech devices authorized to access a shared network drive on which the data are stored.

5.2.4.4 Virginia Tech devices authorized to connect to a physically secured and firewall-protected server (e.g., terminal server, Linux server accessed via SSH) that has access to the data.

5.2.5 Network access

5.2.5.1 **Moderately sensitive** PII must not be copied to and/or stored on a personal workstation's hard drive.

5.2.5.2 The file storage system must be in a physically secured space that preferably requires the presentation of a valid, authorized key or keycard to enter that space.

5.2.5.3 The storage device must be protected through a network access control mechanism, such as a hardware or software-based firewall or router-based access control lists.

5.2.5.4 Only system administrators responsible for the maintenance and management of the network-based storage media may have direct physical access to the storage system's hardware.

5.2.5.5 Anyone attempting to access **moderately sensitive** PII either directly from the file server or remotely via a network connected client device must provide an authorized Virginia Tech computer account (PID) and its associated password.

5.2.5.6 When maintaining network-based storage systems containing **moderately sensitive** PII, system administrators are required to authenticate using an authentication mechanism approved by the Virginia Tech IT Security Office.

5.2.5.7 Network-based data may be accessed via wired or wireless network connections.

5.2.5.8 All passwords must be encrypted wherever they are stored and when they are transmitted over the network.

5.2.5.9 **Moderately sensitive** PII transmitted across the network must be encrypted in transit.

5.2.5.10 All encryption protocols and key lengths used must be approved by the Virginia Tech IT Security Office.

5.2.5.11 The practices for managing **moderately sensitive** PII should be reviewed by the researcher and the research team at the start of the data set's lifecycle, annually during the lifecycle of the data set, and at the end of the data set's lifecycle.

5.2.5.12 **Moderately sensitive** PII must not be accessed directly from a personal device through network file services, but through a server (e.g., terminal

server, Linux server accessed via SSH) approved by Virginia Tech IT Security Office that requires two-factor authentication.

5.2.5.13 Only project team members with need to know might be given access to materials related to **moderately sensitive** PII data (derivative results, output, etc.). These individuals should be identified on the IRB protocol associated with the proposed research.

5.2.5.14 For electronic data, access to the related data must be actively logged.

5.2.5.15 The practices for managing moderately sensitive PII should be reviewed by the researcher at the start of the data set's lifecycle, four times a year during the lifecycle of the data set, and at the end of the data set's lifecycle.

5.3 Protections for **very sensitive** information about individually identifiable persons include:

5.3.1 General guidelines

5.3.1.1 Access

5.3.1.1.1 Same as for benign

5.3.1.2 Printing

5.3.1.2.1 Same as for benign

5.3.1.3 Mailing paper-based information

5.3.1.3.1 Same as for benign

5.3.1.4 Storing electronic files on work computers

5.3.1.4.1 Computer must meet Virginia Tech security requirements for high risk data, including device password, anti-virus, current patches, encryption, and remote wiping (See https://security.vt.edu/resources.html).

5.3.1.5 Storing files on external portable storage media (USB, CD/DVD, back-up tape, etc.)

5.3.1.5.1 Same as for benign

5.3.1.6 Sharing data/files with authorized individuals

5.3.1.6.1 Use approved collaboration tools.

5.3.1.6.2 Share with specific individuals, not anonymous or guest links.

5.3.1.7 Sending data/files to authorized individuals

5.3.1.7.1 Same as for benign

5.3.1.8 Deleting electronic files

5.3.1.8.1 Same as for benign

5.3.2 Data collection

5.3.2.1 Data collection must be performed using Virginia Tech reviewed and approved survey tools (e.g. Qualtrics, Red Cap, other).

5.3.2.2 Additional safeguards may be imposed by the IRB.

5.3.2.3 **Very sensitive** PII must not be copied to and/or stored on a personal workstation's hard drive.

5.3.2.4 The storage device must be protected through a network access control mechanism, such as a hardware or software-based firewall or router-based access control lists.

5.3.2.5 Only system administrators responsible for the maintenance and management of the network-based storage media may have direct physical access to the storage system's hardware.

5.3.2.6 Anyone attempting to access **very sensitive** PII either directly from the file server or remotely via a network connected client device must

provide an authorized Virginia Tech computer account (PID) and its associated password.

5.3.2.7 When maintaining network-based storage systems containing **very sensitive** PII, system administrators are required to authenticate using multi-factor authentication.

5.3.2.8 Network-based data may be accessed via wired or wireless network connections.

5.3.2.9 All passwords must be encrypted wherever they are stored and when they are transmitted over the network.

5.3.2.10 **Very sensitive** PII transmitted across the network must be encrypted in transit.

5.3.2.11 All encryption protocols and key lengths used must be approved by the Virginia Tech IT Security Office.

5.3.2.12 The practices for managing **very sensitive** PII should be reviewed by the researcher at the start of the data set's lifecycle, annually during the lifecycle of the data set, and at the end of the data set's lifecycle.

5.3.2.13 **Very sensitive** PII access must be performed through a server (e.g., terminal server, Linux server accessed via SSH) approved by Virginia Tech IT Security Office that requires multi-factor authentication.

5.3.2.14 Only project team members might be given access to materials related to **very sensitive** PII data (derivative results, output, etc.). These individuals should be identified on the IRB protocol associated with the proposed research.

5.3.2.15 For electronic data, access to the related data must be actively logged and monitored.

5.3.2.16 The practices for managing moderately sensitive PII should be reviewed by the researcher at the start of the data set's lifecycle, four times a year during the lifecycle of the data set, and at the end of the data set's lifecycle.

5.3.2.17 **Very sensitive** PII access must be accessed through network file services, but through a server (e.g., terminal server, Linux server accessed via SSH) approved by Virginia Tech IT Security Office that requires two-factor authentication.

5.3.2.18 Access to the **very sensitive** data set must require a file encryption key to decrypt the data.

5.3.2.19 **Very sensitive** PII data must be stored in an encrypted manner using an encryption protocol and key length approved by the Virginia Tech IT Security Office.

5.3.2.20 **Very sensitive** PII data must not be copied to and/or stored on a workstation's hard drive.

5.3.2.21 The practices for managing very sensitive PII data should be reviewed by the researcher at the start of the data set's lifecycle, four times a year during the lifecycle of the data set, and at the end of the data set's lifecycle.

5.4 Data Protection Standards in Restricted Use Agreements

5.4.1 When a sponsor or data use agreement requires additional or project specific security measures the researcher should consult with the Privacy and Research Data Protection Program (prdp@vt.edu) for guidance on which standards are more secure with respect to the sensitivity levels of the data.

5.5 Data Disposition

5.5.1 Data should be archived to secure storage when not in active use using the mechanisms noted above, its location and data custodian documented.

5.5.2 A data disposition plan should be documented that includes how and when the 1) identifiers, and 2) the data themselves will be destroyed or permanently archived for future use.

5.5.3 Research data must be retained per federal requirements (6 years), or per NIH, NSF, FDA, or other Sponsor requirements.

5.5.4 Access to archived data is by the approved protocol, the designated data custodian, Scholarly Integrity and Research compliance (SIRC) staff, or administrators as needed.

5.5.5 Where possible, steps should be taken to allow open access to the data with application of appropriate deidentification procedures.

6 MATERIALS

6.1 PRDP-001 – SOP – Research Data Definitions

6.2 Virginia Tech IT Security Office Guidance on Protecting Sensitive Information

6.3 https://it.vt.edu/content/dam/it_vt_edu/policies/Minimum-Security-Standards.pdf

7 REFERENCES

None