 

Data Security Plan

|  |  |
| --- | --- |
| WF Summary Details | |
| Version Date: |  |
| Workflow Name: |  |
| Proposal Org / Dept. No. |  |
| Principal Investigator: |  |
| DSP Submitted by: |  |
| Protocol File Uploaded to Study Documents: |  |

## HIPAA Identifier Options

| Options | option selected | how stored |
| --- | --- | --- |
| **Note**: You will refer to this list throughout the document. | If the identifier is not listed, it is not applicable. | Options include:   * Collect source data collection (receive, collect, or record at UVA) * Store long term at UVA * Send or transmit outside of UVA * Not Applicable |
| 1. Name |  |  |
| 2a. Postal address includes street and/or PO Box, and town or city, state, and zip code |  |  |
| 2b. Postal address that includes only town or city, state, and/or zip code |  |  |
| 3. All date elements (except year) for dates related to an individual, e.g. service date |  |  |
| 4. Telephone numbers |  |  |
| 5. Fax numbers |  |  |
| 6. Electronic mail addresses |  |  |
| 7. Social Security number |  |  |
| 8. Medical Record number |  |  |
| 9. Health plan beneficiary numbers |  |  |
| 10. Account numbers |  |  |
| 11. Certificate/license numbers |  |  |
| 12. Vehicle identifiers and serial numbers, including license plate numbers |  |  |
| 13. Device identifiers and serial numbers |  |  |
| 14. Web Universal Resource Locators (URLs) |  |  |
| 15. Internet Protocol (IP) address numbers |  |  |
| 16. Biometric identifiers, including finger and voice prints |  |  |
| 17. Full face photographic images and any comparable images |  |  |
| 18. Other unique number, characteristic, code related to an individual, e.g. initials |  |  |

## COLLECTION & STORAGE OF HUMAN SUBJECT RESEARCH DATA

### A) Paper Documents 3

| options | selected |
| --- | --- |
| Storage location |  |
| Other: (Please describe) |  |

**\*Appropriate UVA locations include one or more of the following:**

* Kept in a locked office in a building with 24-hour swipe locks when unattended
* Kept in a locked file cabinet in a locked room when unattended
* Kept in an office where study are personnel present in room at all times located in a building with 24-hour swipe locks or a room with a lock when unattended
* Behind two locked doors when unattended

### B) Emailed to other UVA Personnel

| options | selected |
| --- | --- |
| Research data emailed to UVA personnel, but with no HIPAA identifiers except dates.  -or/and-  Email only to and from UVA personnel with \*HS in the Global Address List |  |
| Other Email Characteristics: (Please describe) |  |

### C) Electronic Medical Record (EPIC)

| options | selected |
| --- | --- |
| Data will be collected in EPIC as part of routine care or as part of medical center encounters during the research study. |  |

### D) UVA-approved eCRF or Clinical Trials Management system

| List | used / selected |
| --- | --- |
| hstsdatalab.hscs.virginia.edu |  |
| hstsdsmpogapp.hscs.virginia.edu |  |
| musicvpn01.med.virginia.edu |  |
| OnCore (oncore.med.virginia.edu) |  |
| Redcap-int.hscs.virginia.edu |  |
| https://reveal.studymanager.com/ |  |
|  |  |
| I acknowledge that ANY electronic use devices used to connect to any servers/websites checked above are supported by UVA Health IT |  |

### E) UVA Servers & Websites

| List | used / selected |
| --- | --- |
| domatlas.eservices.virginia.edu |  |
| dom-titan.eservices.virginia.edu |  |
| Elson1.studenthealth.virginia.edu |  |
| es3.eservices.virginia.edu |  |
| gcrcserver.itc.virginia.edu |  |
| [\\HSCS-ss7](../../../../../../../../..//HSCS-ss7) |  |
| [\\HSCS-ss8](../../../../../../../../..//HSCS-ss8) |  |
| [\\HSCS-ss9](../../../../../../../../..//HSCS-ss9) |  |
| [\\HSCS-ss10](../../../../../../../../..//HSCS-ss10) |  |
| [\\HSCS-ss11](../../../../../../../../..//HSCS-ss11) |  |
| [\\HSCS-ss12](../../../../../../../../..//HSCS-ss12) |  |
| [\\HSCS-ss13](../../../../../../../../..//HSCS-ss13) |  |
| \\hscs-share1\ |  |
| \\hscs-share2\ |  |
| \\hscs-share3\ |  |
| \\radshare\ |  |
| upgusers.hscs.virginia.edu |  |
| Ivy Secure Computing Platform/ Ivy Secure Cloud/Ivy Cloud |  |
| School of Nursing SECURE NET |  |
| UVA HIT DropBox/Sookasa |  |
| UVA Qualtrics HSD survey tool: https://virginiahsd.co1.qualtrics.com/ControlPanel/ |  |
|  |  |

### F) Web-based or Cloud Format (not listed above)

| List | used / selected |
| --- | --- |
| Data will be collected and/or stored in UVABox or UVA-Collab |  |

|  |  |
| --- | --- |
| Check the HIPAA Identifiers stored on UVA Box or Collab |  |
|  |  |
| If you are using other web-based or cloud servers please describe: |  |

## Individual Use Devices

**Current list of individual use device choices available for use:**

* No Individual Use Devices will be used
* Flash (thumb) drive
* External drive
* CD or DVD
* Desktop Computer
* Laptop
* Tablet
* Smart phone
* Camera
* Video recorder
* Audio recorder
* Biometric recording device
* Fitness Trackers
* Other

|  |  |
| --- | --- |
|  | |
|  | |
| FIELDS AVAILABLE | SELECTED |
| If you selected “Other” above, please identify the device type: |  |
| Please describe your process for collecting, storing and/or transmitting data on the Individual Use Devices you selected in earlier steps (phones, flash drives, CDs, etc.): |  |
| Check the HIPAA Identifiers stored with the data on this device (e.g. such as full-face picture or video): |  |
| Describe any backups made of the data stored on the device. Please include the location & method of data transfer: |  |
| How long will the data remain on the individual-use device before being transferred? |  |
| After the information is transferred elsewhere, will you securely delete all the data from this device? |  |
| Will anyone other than the study team or sponsor/CRO have access to data on this device? |  |
| If yes, describe |  |
| Other storage alternatives that were considered and the reasons they are unworkable |  |
| The justification for storage of these data on this individual use device is: |  |
|  | |

## Transmission & Storage of the Human Subject Research Data Outside of UVA

| Question | answer |
| --- | --- |
| Will data be transmitted to a sponsor or a colleague at another institution? |  |
| Data will be emailed to non-UVA personnel via HSC secure email |  |
| I acknowledge that ANY electronic individual use devices used to connect to any servers/websites listed below are supported by UVA Health System IT. (CRO) |  |
| Check the HIPAA Identifiers stored by the Sponsor or CRO |  |
| If sharing data with anyone outside of UVA, do you confirm that you will obtain a contract with them via the School of Medicine Grants and Contracts Office or the Office of Sponsored Programs (OSP)? |  |
| Data will be sent and stored in an encrypted fashion (e.g. will only be shared and via Secure FX, Secure FTP, HTTPS, PGP) and the server/drive is configured to store data regulated by HIPAA |  |
| Name (URL) of website (e.g. http://remote.sponsor.com/project name) |  |
| Paper documents will shipped using trackable method. |  |
| Data encrypted on an individual use device and shipped using trackable method. Password to the encrypted data transmitted separately. |  |
| Data faxed to a receiving machine in a restricted-access location. The intended recipient is clearly indicated, alerted to the pending transmission and available to pick up immediately. |  |

## DATA SENSITIVITY

When paired with health information, any of the below data elements are considered Highly Sensitive Data by UVA’s Data Protection policy (<https://uvapolicy.virginia.edu/policy/IRM-003>).  Please note that Social Security Numbers, Driver’s license numbers, passport numbers, financial account numbers, and credit card numbers are considered Highly Sensitive Data regardless of whether or not they are paired with health information.

1. Name
2. Postal address, other than town or city, state, and zip code (e.g. street name or GPS information.)
3. Telephone numbers
4. Fax numbers
5. Electronic mail addresses
6. Social Security Numbers
7. Medical Record Numbers
8. Health plan beneficiary numbers
9. Account numbers (e.g. bank numbers, credit card numbers, hospital bill account number)
10. Certificate/license numbers (e.g. passport number, driver’s license number, medical board license number)
11. Vehicle identifiers and serial numbers, including license plate numbers
12. Device identifiers and serial numbers
13. Web Universal Resource Locators (URLs)
14. Internet Protocol (IP) address numbers
15. Biometric identifiers, including finger and voice prints
16. Full face photographic images and any comparable images

## Data Security Study Team

| Notes |
| --- |
|  |