

Information & Technology Services

**Office of Information Security**

Data Security Plan (DSP)

Academy for Public Health Innovation

UNC Charlotte Representatives

Michael Moore, DSO

Michael Dulin, Academy Director

Third Party

Tresata (Cloud Based Service)

File Name

DRIVE-DSP.APHI.Dulin.pdf

|  |  |
| --- | --- |
| Date Created | Last Revisited |
| 7.13.2018 | X.XX.XX |

Table of Contents

[Data Security Plan](#1fob9te)

[1. General Information](#3znysh7)

[1.1 Identification](#2et92p0)

[1.2 Project Team: UNC Charlotte](#3dy6vkm)

[1.3 Project Team: Third Party](#1t3h5sf)

[1.4 IT Support Team](#2s8eyo1)

[1.5 Research Facility](#17dp8vu)

[1.6 Physical Location of Data](#3rdcrjn)

[2. Data Security Information](#lnxbz9)

[2.1 Data Description](#35nkun2)

[2.2 Data Transmission Security](#1ksv4uv)

[2.3 Data Location Security](#44sinio)

[2.4 Authorized Users](#2jxsxqh)

[3. Asset Security Information](#3j2qqm3)

[3.1 Asset: <Server | Workstation | Laptop>](#1y810tw)

[4. Security Training and Incident Reporting](#2xcytpi)

[5. Project termination](#1ci93xb)

[6. Certification](#qsh70q)

# Data Security Plan

*Please complete all the sections in this document with the up-to-date information. Insert N/A for sections that are not applicable.*

## 1. General Information

### 1.1 Identification

|  |  |
| --- | --- |
| Project Name: | Academy for Public Health Innovation- Community DRIVE |
| IRB Protocol #: | N/A - Multiple IRB Protocols will refer to this DSP |
| UNCC Project #: | N/A - Multiple Project #’s may refer to this DSP |
| NORM Proposal #: | N/A – Multiple NORM proposal #’s may refer to this DSP |
| Grant or Contract #: |  |
| Start Date: | X/XX/XX |
| Completion Date: | Continual – DSP will be reviewed annually  |
| Duration: | Continual |

### 1.2 Data Provider Contact Information

|  |  |
| --- | --- |
| Name/title | Community DRIVE Partner |
| Address |  |
| Phone: |  |
| Email: |  |
| URL: |  |

### 1.3 Project Team: APHI- Community DRIVE

|  |  |
| --- | --- |
| Principal Investigator: | Michael Dulin |
| College/Dept.:  | 249 Billingsly Road |
| Phone: | 704-641-2157 |
| Email: | Mike.dulin@mecklenburgcountync.gov |
| URL: | https://www.aphicommunitydrive.org |

|  |  |
| --- | --- |
| Research Team Member 1: | N/A |
| College/Dept.:  |  |
| Phone: |  |
| Email: |  |
| Additional Information: |  |

|  |  |
| --- | --- |
| Research Team Member 2: | N/A |
| College/Dept.:  |  |
| Phone: |  |
| Email: |  |
| Additional Information: |  |

### 1.4 Project Team: Third Party

|  |  |
| --- | --- |
| Organization 1: | Tresata |
| Primary Contact: | Michael Dulin |
| Office/Division/Dept.: | CMO |
| Additional Information: |  |
| Phone: | 704-641-2157 |
| Email: | mdulin3@uncc.edu |

|  |  |
| --- | --- |
| Organization 2: | AWS (Amazon Web Services) |
| Primary Contact: |  |
| Office/Division/Dept.:  |  |
| Additional Information: |  |
| Phone: |  |
| Email: |  |

### 1.5 IT Support Team

|  |  |
| --- | --- |
| Primary Technician: | Michael Moore |
| College/Dept.:  | College of Health and Human Services |
| Phone: | 704-687-7883 |
| Email: | Mmoor129@uncc.edu |
| Additional Information: |  |

|  |  |
| --- | --- |
| Secondary Technician: | Brittany Box |
| College/Dept.:  | Tresata |
| Phone: |  |
| Email: |  |
| Additional Information: |  |

### 1.6 Research Facility

|  |  |
| --- | --- |
| Physical Address: | CHHS 335E, 9201 University Boulevard  |
| Description: |  |
| Physical Address 2: |  |
| Description: |  |

### 1.6 Physical Location of Data

|  |  |
| --- | --- |
| Physical Address: | N/A – Data will be stored with a HIPAA compliant cloud service provider |
| Description: |  |
| Physical Address 2: |  |
| Description: |  |

## 2. Data Security Information

|  |
| --- |
| 2.1 Data DescriptionDescribe the data used in this research indicating whether the data contains:* **personally identifiable information** (PII) such as names, addresses, social security numbers (SSI), driver’s license, date of birth... etc or
* **student information** such as grades, assignments, courses or
* **protected health information** (PHI) such as health status, provision of health care, or payment for health care.

If the data has been de-identified, describe what fields have been removed and how the identifying information has been separated and coded. |
| Data will include (i) PII that will be used to link records and would include name, sex, birthdate, and address; (ii) PHI including: disease/condition, medications, tests results, and biometric measures; (iii) other sensitive information describing social determinants at the census tract level. |
|  2.2 Data Transmission SecurityDescribe how data was received and what security measures are used to protect access to data as it was transferred to computers where it would be analyzed. |
| Representatives at Mecklenburg County Public Health Department will be provided user-specific credentials to log into a secure HIPAA compliant network storage provider where data can be directly uploaded. Researchers within the academy will be provided their own credentials to reach and manipulate the data within the protected network storage space. The provider will be required to maintain a secure FTP server as well as secure Application server appropriately provisioned for the APHI project.

|  |
| --- |
| ***Recommendations****Possible modes of transmission** *Sent to researcher on an encrypted CD/DVD/external drive*
* *Downloaded by researcher from sponsor’s server via a secure transfer protocol (SFTP, SSL)*
* *Uploaded by sponsor to UNC Charlotte server via a secure transfer protocol (SFTP, SSL)*
* *Copied from workstation to UNC Charlotte server or cloud storage service or vice versa*

*For some identifiable data stored on UNC Charlotte servers or using a cloud storage service:**All data will be viewed and modified within encrypted files/folders on <UNC Charlotte or cloud vendor> servers. Certificates and private keys will be exported to removable media.* *For some de-identified data stored on UNC Charlotte servers:**All data will be viewed and modified on the server over a network connection using campus user account and strong passwords that change every 90 days. The data will not be downloaded to any local workstations. Only the Principal Investigator (PI) and Research Team members will be accessing the data. All the data is protected via an ACL permissions list. Only the researcher(s) and IT server administrators have access to the data. All data on the file server is backed up daily to an offsite facility over a network connection.* |

 |
| 2.3 Data Location SecurityDescribe the location(s) where the data is stored and analyzed and what security measures are used to ensure the data is protected from being accessed by unauthorized users. |
| All sensitive data associated with the APHI academy will be stored with a HIPAA certified network storage solution. As part of the contractual agreement with the network storage provider, the data will be encrypted at rest on the server environment and securely backed up as part of standard disaster recovery operating procedure. The server environment will be protected at all times by industry standard network firewall. All sensitive data processing will occur on the secure online environment. Data sets that are prepared for download for additional processing will be de-identified removing or recoding any and all of the eighteen categories of identifiable fields using methods specified in the Privacy Rules listed by the US Department of Health and Human Services. <http://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html>

|  |
| --- |
| ***Recommendations****For identifiable data:**All copies of data, both paper and electronic, will be stored in a locked cabinet CHHS 335. Only the APHI director and assigned APHI staff will have the keys to the cabinet. Only the APHI Director and UNC Charlotte Police & Public Safety office will have a key to CHHS 335. The decryption key will be stored on separate removable media which will be managed by the IT support team and stored in a locked office.**For de-identified data:**All copies of data, both paper and electronic, will be stored in a locked cabinet in CHHS 335. Only the APHI and assigned APHI staff will have the keys to the cabinet. Only the APHI director, the APHI staff and UNC Charlotte Police & Public Safety office have access to this office. The decryption key will be stored on separate removable media which will be managed by the Primary Technician and stored in a locked office.* |

 |
| 2.4 Authorized UsersSpecify who is authorized to access and analyze this data. |
| Michael Dulin, UNC Charlotte, College of Health and Human ServicesMichael Moore, UNC Charlotte, College of Health and Human ServicesAdditional access will be granted to future members of the APHI team after they receive training (including HIPAA compliance) and are reviewed as per the APHI data access policy. These access additions will be documented via the DSP amendment process.

|  |
| --- |
| ***Recommendations****For project that includes additional researchers not listed in the DSP:**Only the APHI Director and assigned team members will make modifications to the data. The following individuals will also have access this data:** *All individuals who has signed a nondisclosure or confidentiality agreement*
* *ITS server administrators*
* *IT Support Team*
 |

 |

## 3. Asset Security Information

|  |
| --- |
| Give an overview of all the assets that will be used in this project. (following sections will contain detailed descriptions of assets) |
|  |

*Each asset should be described in detail below. Copy Section 3.1 for each additional type of uniquely configured asset.*

### 3.1 Asset: <Server | Workstation | Laptop>

|  |  |
| --- | --- |
| **Description:**-purpose of asset-installed software or services | **For workstations/laptops**All workstations used in this project will be clearly identified in the CHHS Equipment Master Database as maintained by the Data Security Officer for the College.Data analysis/visualization will be done with the following software:* SPSS
* SAS
* STATA
* SUDAAN
* QSR
* Atlas TI
* R
* Python
* Tableau
 |
| **Location:**-office or server room-name of user | CHHS 335E |
| **Operating System:** | Operating Systems for each asset are clearly identified in the CHHS Equipment Master Database as maintained by the Data Security Officer for the College. |
| **Authorized Users:**-type of user account-type of authentication-type of access | The following users accounts are authorized:Mdulin3Mmoor129

|  |
| --- |
| **Recommendations***For some identifiable or sensitive data:*Local user accounts will be created for each researcher. These user accounts will not have administrative access to the operating system. A local administrative level user will be added to the operating system that will be accessible to the IT Support Team identified above.*For most data:*The operating system will be bound to the UNC Charlotte AD domain with a specific policy that limits access to the user accounts of the PI and the Research and IT Support Teams. User accounts of PI and the research team will not have administrative access to the operating systemA local administrative level user will be added to the operating system that will be accessible to any University IT support person who is authorized to use the standard local administrator account that is added to all faculty and staff computers. |

 |
| **Security Controls:**-password complexity-access controls-network restrictions-firmware configuration-drive encryption-port control-screensaver settings-session lockouts-software whitelisting-communication tools | **Password Complexity**Password policy will conform to University Standard for Account Passwords, see: <http://itservices.uncc.edu/iso/standard-account-passwords>* Maximum Password Age = 90 days
* Minimum Password Length = 8 characters
* Maximum of 16 characters in length
* At least one uppercase letter (A-Z)
* At least one lowercase letter (a-z)
* At least one digit (0-9)
* At least one special character ! % \* + - / : \_
* Enforce password history to remember = 8 passwords

</recommended measures>**Access Controls**Network access will be enabled on machines utilized in this project as data will be stored in a secure network accessible storage space that is contractually certified as HIPAA compliant.Any academy members will be required to use Dual Authentication to access university systems including workstations.

|  |
| --- |
| **Recommendations***For some identifiable data:** All network access will be disabled
* Hard drive will be encrypted
* Firmware will be password protected to prevent starting up from another drive
* All ports that can be used to attach removable media will require that removable media to be encrypted
* Screensaver will be enabled after no more than 5 minutes
* When the screensaver has been activated, logon is required to access

*If project involves de-identification with a laptop:** The computer that will be used for this project will be secured to the desk in this office while it has data that has not yet been de-identified.

*For most identified data:** Hard drive will be encrypted
* Firmware will be password protected to prevent starting up from another drive
* All ports that can be used to attach removable media will require that removable media to be encrypted
* Screensaver will be enabled after no more than 5 minutes
* When the screensaver has been activated logon is required to access

*For servers:** access is managed through AD/PAM/SASL/LDAP/Kerberos authentication and access control lists
 |

 |
| **Backup:**-type of backup-type of drive-encryption-retention-physical storage | Sensitive Project Data Backup will not occur at the individual level and will instead be coordinated as part of the contractually obligated requirements of the data provider.

|  |
| --- |
| **Recommendations***Physical Drive:*Data will be backed up to a drive that is encrypted using Advanced Encryption Standard (AES) 128-bit*Backup Encryption Key:*The decryption key will be stored on separate removable media which will be managed by the IT support team and stored in a locked office in <office location>.*ITS Network File Storage:*Data stored on ITS network shares is backed up daily and these daily snapshots are retained for at least 30 days. All data (including snapshots) are replicated at a remote data center. Data backup is NOT encrypted. |

 |
| **Data Destruction Plan:**-file deletion-hard drive deletion-drive destruction-media destruction-encryption key removal | Upon completion of each academy project, data will be reviewed by the APHI Director for relevancy in existing and future projects. If data is deemed to be subject to termination, encrypted data folders will be deleted from the network storage. The Data Security Officer and the APHI Directory will meet annually to review all existing data sets on the secure network storage.

|  |
| --- |
| **Recommendations***For data stored on hard drives:**All hard drives that contain data will be securely wiped or degaussed after the project is over. All hardcopy data will remain secured in the locked cabinet until transferred to designated shred bins or manually shredded via cross-cut shredder.**For data stored on network drives with filesystem-level encryption:**All encrypted data folders and key file will be deleted from the network share. Removing the key file will revoke access to the <Network Folder> in each user’s folder, rendering it unusable. Any backups of the folders will remain on tape and be overwritten as part of the normal tape recycling procedure when a backup tape expires.**For data stored on network drives without encryption:**All data files will be deleted from the network share and all copies of the data retained in backed up daily snapshots will be deleted within 90 days.**For data stored using cloud-based services:**All encrypted data files and folders will be deleted from the cloud servers as well as all copies that may have been synchronized to various devices.**For data that will be archived indefinitely:**All data files will be archived in the following location:**Archived data will be reviewed yearly for relevance.* |

 |
| **Additional System Use:**Other usage including:-other research projects-non-research usage | N/A

|  |
| --- |
| **Recommendation**Usage is limited only to the APHI team. |

 |
| **Technical Contact(s):** | Michael Moore, mmoor129@uncc.edu |

## 4. Security Training and Incident Reporting (HIPAA Breach Notification Steps)\*

All researchers will complete security awareness training. All researchers will report any security incidents following the UNC Charlotte Guideline for Reporting Information Security Incidents (see: <http://itservices.uncc.edu/iso/guideline-reporting-information-security-incidents>)

## 5. Project termination

All data sets will be reviewed on an annual basis by the DSO and the APHI Director to determine relevancy to the project. Upon completion of any project, data will be reviewed by the APHI Director for relevancy in existing and future projects. If data is deemed to be subject to termination, encrypted data folders will be removed from the secure network storage. All other hard copy materials will be kept at the physical location for data collection until they are no longer needed for verification. Following this, all information will be destroyed. Any associated research compliance documentation will also be reviewed for renewal during this time.

If data is deemed relevant in future or proposed projects, this data security plan will be amended or a new plan created based on the information associated with the new project. Any new research would be subject to approval through appropriate university procedures.

## 6. Certification

I have reviewed the requirements of the data use agreement and the security procedures in this plan that describe the required protection procedures for securing, accessing and using the restricted-use data.

I have also reviewed the UNC Charlotte Standards and Guidelines (see: <http://itservices.uncc.edu/home/it-policies-standards/standards-and-guidelines>) and agree to maintain compliance.

I hereby certify that the computer system, physical location security procedures, and access procedures meet all of the data use agreement requirements and will be implemented for the duration of the project and License period.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

APHI Director Signature Date

<Name, Title, Contact Details>

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

College Data Security Officer Signature Date

<Name, Title, Contact Details>

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Chief Information Security Officer Signature *(optional)*  Date

<Name, Title, Contact Details>