**NEW HAMPSHIRE EMERGENCY MEDICAL AND TRAUMA SERVICES**

**RECORDS DATA MANAGEMENT AND SECURITY PLAN**

Complete this form to provide details about your data management and security plan. The topics in this form address data security requirements defined under federal 45 CFR § 164.302-.316 “Security Standards for the Protection of Electronic Health Information”. Use as much space as is necessary in each area for comments or descriptions and attach any additional information required or which will support your application.

Once this form is completed and approved, it will be the official data management and security plan. Submit any changes to this plan to the Emergency Medical and Trauma Services Records Privacy Committee (ERPC) for prior review and approval before implementation.

|  |
| --- |
| **Project Title and Contact** |
| **Project Title:** | Click here to enter text. |
| **Principal Investigator:** | Click here to enter text. |
| **Application Date:** | Click here to enter a date. | **Internal Use Only:** | Click here to enter text. |
| **Section 1: Information System Description***Briefly* describe your information system structure and management to provide context for the rest of this documentInclude whether all or part of your system is managed by an institution or other organization, what resources are involved such as hardware or software, type of information/data stored in the system, if networked internally or externally and who the system supports and may access the system. |
| Click here to enter text. |
| **Section 2: Data Linkage and Collection Methods** |
| **Section 2.1: Data Linkage and Integration** * Enter comments and descriptions below
 |
| **Will data be linked or integrated with other data sources?** | [ ] Yes[ ] No |
| **Will linkage increase identifying data?** | [ ] Yes[ ]  No [ ]  Not Applicable |
| **Will data be transmitted over the internet or unsecure network?** | [ ] Yes[ ] No |
| Data Linkage Comments: Click here to enter text. |
| **Section 2.2: Data Collection Methods*** Describe how other data to be linked to EMTS data will be collected. Describe details in comments section below
 |
|[ ]  Not Applicable, Data will not be linked or integrated |
|[ ]  Paper and Pencil (e.g. written consent forms, electronic data printed out, paper source documents, etc.) |
|[ ]  Extraction from and linkage to other electronic Medical records systems |
|[ ]  Electronic data capture (e.g. Mobile Application, Smart Devices) |
|[ ]  External web-based surveys |
|[ ]  Other (Describe below) |
| Click here to enter text. |
| **Section 3: Administrative Safeguards** |
|  **Section 3.1 Assigned Security Responsibility*** Who is responsible for the Information System security?
 |
| [ ] The affiliated organization provides and manages the Information System (e.g. University or Hospital) and the institution IT department manages all administrative safeguards. * Describe setup or reference published sections in comments sections below
* Attach relevant organizational policies to application

[ ]  The research team or local organization IT section manages the Information System*.** Must complete all sections and attach associated policies
 |
| Click here to enter text. |
|  **Section 3.2 Security Management Process** |
|  **Section 3.2.1 Risk Analysis and Management** |
| Date of last HIPAA Security Risk Assessment: | Click or tap to enter a date. |
| Risk Management measures were implemented to reduce risks and vulnerabilities identified | Choose an item. |
| Risk Management Comments**:** Click here to enter text. |
|  **Section 3.2.2 Workforce Security Awareness, Training and Management**  |
|  *(Attach policies addressing the following topics or describe below)** Authorization and supervision of users accessing data including account and password management
* Protection from malicious software and intrusions
* Login monitoring and access
* Policies and user sanctions for failing to comply
* Cyber and data security awareness training requirements
* Training project team in all aspects of data security, privacy and protocols for the project
 |
| Click here to enter text. |
|  **Section 3.3 Data Access Agreements** |
|  [ ]  No individual or organization outside of the primary research team will have access to Data [ ]  Data will be accessed by contractors, consultants or one or more other organizations\*\*\*\*All Business Associate Agreements, contracts and/or Data Use Agreements *must be attached* to the application |
| Data Access Agreement Comments**:** Click here to enter text. |
| **Section 4: Physical Safeguards** |
| **4.1 Facility Access Controls*** Describe Access and security controls for physical locations where the data is stored and any devices such as work stations and mobile devices and any identifiable paper records or notes
 |
| Click here to enter text. |
| **4.2 Workstation Use and Security*** Describe how work stations are secured, who has access to the work stations and how that is managed and how login and use is logged for auditing
 |
| Click here to enter text. |
| **4.3 Device and Media Controls*** Describe what type of mobile media devices will be used, the reasons for use or the devices
* Who will have access to the devices
* Accountability process/policies for the devices
* How the devices will be encrypted
* The disposal and/or re-use process for the devices to ensure all data has been removed
 |
| Click here to enter text. |
| **Section 5: Technical Safeguards** |
|  **Section 5.1: Access Control*** Explain how your information system manages access control by addressing:
* Managing and issuing unique user ID
* Automatic Logoff
* Emergency access if system or devices are locked or primary user can’t access device to remove or destroy data
 |
| Click here to enter text. |
|  **Section 5.2: Connection and Transmission Integrity and Security*** Explain how your information system will maintain data integrity and security with any linkage between systems, if the system allows outside access, or data is transmitted between systems.
 |
| Click here to enter text. |
|  **Section 5.3: Data Encryption*** Explain how data will be encrypted on devices where the data is stored to prevent unauthorized users access to the data
 |
| Click here to enter text. |
| **Section 6: Data Destruction*** Describe the process for data destruction from all devices, servers, drives, paper files etc. after the project is complete.
 |
| Click here to enter text. |
| **Section 7: Attachments*** The following attachments should be included with this application
 |
|[ ]  Organizational policies, procedures or guidelines governing data administrative, physical or technical safeguards |
|[ ]  Minimum overview of training provided to all that may have access to EMTS data |
|[ ]  Copies of all Business Associate Agreements, Contracts with consultants or other organizations and/or Data Use Agreements with any entity associated with this project |
| **Section 8: Comments*** Enter any comments below that have not already been addressed and which you feel may help the ERPC to approve your application
 |
| Click here to enter text. |
| **Section 9: Signature** |
| **I have reviewed this Records Data Management and Security Plan. All statements made in this plan are true, complete, and correct to the best of my knowledge. I acknowledge that I will submit any changes to this plan to the ERPC for prior review and approval before implementation.** |
| Name of Person Submitting Plan: | Click here to enter text. |
| Title or Role in Project: | Click here to enter text. |
| Organization: | Click here to enter text. |
| Signature Date: | Click or tap to enter a date. |
| Signature: |  |
|  |  |  |