University of Pittsburgh
Department of Critical Care Medicine

CRISMA Center
Data Management Core
Standard Operating Procedures

UPMC Data Center
Information Security
| **Purpose** | This document describes the CRISMA Center’s policies for the storage, access, security and use of human subject data in University of Pittsburgh Medical Center (UPMC) computing environments. |
| **Scope** | This document applies to all personnel employed by or using any computer owned and operated by CRISMA; all computers owned or operated by CRISMA; and all human subject data managed by within the UPMC computing environment. |
| **Definitions** | **Protected Health Information (PHI).** Any information about health status, provision of health care or payment of health care that can be linked to a specific individual.  
**HIPAA Privacy Rule.** The portion of the Health Insurance Portability and Accountability Act of 1996 that governs use and disclosure of PHI. Under the privacy rule, PHI can be used for research purposes with either patient approval or waiver by an authorized regulatory agency.  
**Common Rule.** US Federal regulations for protection of human subjects in research, described by the Department of Health and Human Services in the Code of Federal Regulations Title 45 Part 46.  
**De-identified data.** Health data that does not contain unique identifiers as defined by HIPAA.  
**Limited data set.** A de-identified data set that contains either (a) geographic subdivisions not smaller than a town, city, state and ZIP code; (b) dates, or (c) ages over 89  
**Safe harbor data set.** A de-identified data set that does not contain any of the unique identifiers as defined by HIPAA.  
**Researcher.** As defined by the Common Rule, any individual conducting or assisting in the conduct of a systematic investigation designed to develop or contribute generalizable knowledge.  
**Data management team.** The CRISMA operations manager and data developers responsible for ensuring compliance with HIPAA, the Common Rule, and other regulatory requirements for use of human subject data. |
| **Responsibilities** | **Research team responsibilities**  
CRISMA researchers responsible for ensuring that the CRISMA research projects involving PHI are reviewed and approved by the University of Pittsburgh Institutional Review Board (IRB). CRISMA researchers are responsible for adhering to IRB-approved data storage and analysis policies at all times. |
Data management team responsibilities
The data management team is responsible for enforcing the procedures described in this document for the storage, access, security and use of data. The Data management team includes:

- Francis Pike PhD, Director of the Biostatistics and Data Management Core;
- Lisa Weissfeld, Biostatistician;
- Michael Willochell, Data Manager and Honest Broker;
- Their immediate designees.

Procedures

Data types
- Data stored by the CRISMA UPMC Data Management Core are restricted to health data from patients in UPMC facilities or clinical and other biomedical data generated as part of a CRISMA-affiliated research project.

Receipt of data
- Data stored by the CRISMA UPMC Data Management Core can be received either electronically from a UPMC health facility, electronically from an external source, electronically using a web-based data entry interface, or physically via electronic media.
- Data transmitted electronically are encrypted using a FIPS 140-2 compliant software package with passwords communicated separately via a secure, pre-approved source.
- Data transmitted via a web-based interface are limited to prospective clinical studies that necessitate an on-line case report form. In this case CRISMA uses a secure web-based interface with intranet and extranet sites located in secure UPMC facilities and administered by the UPMC EMG Web Services Team. The servers use 128 bit Secure Socket Layer (SSL) encryption in all communications with client browsers and applications.
- Data transmitted physically are manually loaded onto UPMC servers using a secure local interface.

Physical data security
- CRISMA and UPMC jointly maintain a high-security, synergized data management platform specifically designed for research projects using sensitive patient information.
- Data management servers reside in UPMC server facilities that are secure, guarded, and designed specifically to house sensitive, private and protected data for UPMC health facilities. The servers are redundantly powered and protected by advanced fire extinguishing capabilities.
- The servers are compliant with HIPAA security regulations.
- Server access is restricted to authorized UPMC personnel with appropriate photo identification and security clearance.
### Electronic data security

- UPMC servers use multiple firewalls and industry standard encryption technologies to ensure electronic security. Server access occurs via Secure Socket Layer (SSL) with 128-bit key encryption.
- Data are managed using Microsoft SQL Server Management Studio on Microsoft Windows Operating Systems. Software security measures include automated security patch download, CLR integration, API asymmetric key encryption and routine security audits using Microsoft Baseline Security Analyzer (MBSA).
- Access to the data is limited to the CRISMA Data Management Team. Permissions are managed by UPMC Information Technology administrators with the same rigor as access to UPMC clinical data. Access is dependent upon recognition of the user, authentication of the facility, and specific permissions granted by the IT administrators.
- Data management team members undergo annual data security training, including instruction on the UPMC polices for data storage, create of a strong password, and proper data management habits.
- Servers hosting CRISMA data under annual vigorous Application Vulnerability Assessment (AVA) testing that examines for exploits, hacks, security breaches and other vulnerabilities.

### Data usage

- Data are released to researchers only in the form of a limited or safe harbor data set after appropriate honest brokering, as described in the CRISMA Data Management Core Honest Broker Standard Operating Procedures.
- Data are released only after submission and approval of a data request form, submission of proof of IRB approval, and execution of a signed data use agreement which outlines the necessary measures for data security.
- Limited and safe harbor datasets must still be safeguarded on password-protected computers at all times in accordance with project-specific IRB guidelines.

### Approval

This CRISMA Standard Operating Procedure was approved by the CRISMA Executive Committee on 3.4.2013.