

# Standard Operating Procedures

**Subject:** Web Security

**Date:** 15Jun2006

**Purpose:** The purpose of this Standard Operating Procedure (SOP) is to define standards for security and confidentiality of web-based systems. These standards augment rather than supplant applicable federal and state regulations.

**Scope:** This procedure applies to all web-based database projects developed or maintained in FPG Data Management and Analysis Center(DMAC). Separate procedures apply to FPG IT Services.

**Responsibility:** The project's Principal Investigator (PI) has responsibility to implement all applicable standards and regulations regarding the secure operation and confidentiality of any web-based system that DMAC develops.

## **Handling of Web-Based Confidential Information:**

- Identifying information
  - Identifying information can include names, addresses and phone numbers of subjects. Web-based applications—such as registries and participant lists—to store and/or display confidential or identifying information must adhere to appropriate Institutional Review Board standards. An explicit procedure for procuring written informed consent will usually be required.
  - Such databases must also be compliant with federal and state policies.
  - Data files containing research data—such as the results of standardized tests or completed survey instruments—must use arbitrary IDs instead of identifying information.
  
- Handling of Paper-Based Confidential Information: Hard copy (paper) records of identifying and confidential information creates a potential threat to client confidentiality.
  - All users of the data-base, including off-site users, should understand how to safeguard data files (on their local PC or storage media) and printed information from inadvertent disclosure.
  - Institutional Review Boards may require each user to undergo training and/or sign a written agreement expressly detailing user duties.
  
- Safeguarding against Intrusion: The following procedures should be employed as necessary to prevent unauthorized access into web-based applications:
  - Implement a Secure Socket Layer connection.
  - Verify the user's authorization on every page access.
  - Whenever possible, limit access to the application to certain IP addresses or sub-nets.