**ADDENDUM I**

**OU Registry and Data Banking Addendum**

**SECTION I**

**DATE:**

**IRB:**

**TITLE OF PROTOCOL:**

**PRINCIPAL INVESTIGATOR:**

**SECTION II**

***INSTRUCTIONS:*** All OU approved research must comply with OU Information Security Policies and OU Security Procedures relating to the safeguarding of electronic Protected Health Information (ePHI) in accordance with HHS regulations at 45 CFR 164 (HIPAA) and FDA regulations at 21 CFR 11.

Submit this addendum with the IRB application for research involving registries and data banking. To determine if the research is approvable under the applicable regulations, the investigator must provide thorough and complete responses to the questions below.

**1. Who is the information custodian for this database/registry?**

*Note: The information custodian is responsible for the creation, maintenance and security of the database. This role may be assigned to the PI, coordinator, or the other administrative personnel involved in the conduct of the study.*

**2. Who is the system administrator for this database/registry?**

*Note: System administrators are the people responsible for configuring, administering and maintaining hardware and operating systems. In many cases, the system administrator function is performed by OU ITS*

**3. How will the research data be archived or destroyed when the data is no longer required?** *Note: Simply reformatting the hard drive will not meet the destruction criteria. With forensic tools, hard drive data can be retrieved after a reformatting of the drive. ITS can assist with proper disposal.*

**4. Will data be extracted and stored on a mobile device (e.g., flash drive, laptop, PDA)?**

**No**

**Yes. Please describe the security measures.**

*Note: Mobile devices must be stored in a physically secured manner and the user must take additional security precautions such as encryption or password protection. In addition, no data may be extracted and shared with people not listed on the IRB application without the express approval of the IRB.*

**5. Will research data containing confidential information be available via the internet?**

**No**

**Yes**

*Note: Research data containing confidential information cannot be placed on a public website as it is in violation of HIPPA laws. Access to this data must be granted through a secure technical method set in place by OU ITS.*

**6. Will you use a wireless computer?**

**No**

**Yes**

*Note: Wireless is approved for OU use only if installed by OU ITS in order to avoid data interception.*

**7. Will this research involve transfers of information (files) outside the organization?**

**No**

**Yes**

*Note: When files need to be transferred outside of the campus network, a secure file transfer methodology (as determined by the type of equipment and operating system used) must be used. ITS will provide additional help upon request.*

**8. Will sponsor or others not associated with OU require remote access to the research database?**

**No**

**Yes**

*Note: Direct inbound modems should never be used as they provide unsecured access to the OU Network. VPN access and secure ID connection can be requested through OU ITS.*

**9. Does this study involve transfer of data between standalone networks and the OU network?**

**No**

**Yes**

*Note: Secure methods must be in place to transfer data between standalone networks and the OU network in order to ensure protection against introduction of viruses and worms into the OU network.*

**10. Is the computer you are using updated regularly with current operating system patches, Microsoft Office patches, and anti-virus software?**

**No**

**Yes**

*Note: Most workstations on the OU network utilizing the Windows operating system have the “auto update” feature activated. When a user receive the message that patches are available for install it is important that the patches be installed as quickly as possible.*

**11. In this research are all operating and application software that you are using appropriately licensed and in compliance with copyright laws?**

**No**

**Yes**