MEMORANDUM

TO: SAM Administrator
Sponsored Awards Management

FROM: PI
Department
College/Center/Institute/School

DATE:

PROJECT PERIOD:

RE: HIPAA Compliance (including use of portable devices)

In accordance with the HIPAA Omnibus Rule (January 2013), the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009, and other applicable federal regulations, I and all persons working on the project entitled: ***Title of Proposal, (USCeRA Proposal Number)*** agree to implement administrative, physical and technical safeguards that reasonably and appropriately protect the confidentiality, integrity and availability of the Protected Health Information (PHI) and Electronic Protected Health Information (ePHI) obtained in connection with the project and as defined in the contract and/or Business Associate Agreement.

As required by HIPAA, I will implement written procedures addressing the applicable HIPAA Security Rule specifications. I understand that my procedure manual must be reviewed by the Office of General Counsel prior to accessing and/or obtaining PHI or ePHI. Such procedures will address the security of all PHI and ePHI stored on electronic storage material including, but not limited to, CDs, DVDs, external hard drives, USB flash drives, laptop/tablet computers, external hard drives, PDAs, portable audio/video devices (e.g. MP3 players, smartphones, digital pens, etc.). This definition includes photocopiers and scanners with internal hard drives that can be used to store information, and data that is transmitted over intranets. PHI and ePHI should not be put in any unsecure data storage format.

To store PHI or ePHI in a cloud-based service, including but not limited to Amazon, Dropbox or Google Drive, a Business Associate Agreement (BAA) with the provider must be in place. The University recommends Microsoft One Drive for secure storage and data transfer of PHI or ePHI. **Information stored on Departmental Servers should be secured per the standards set forth in Information Technology Policy 3.00.** The Omnibus Rule also replaces the term "electronic media" with "electronic storage material" to align with the definition with the NIST standards for technology.

I am aware of the security requirements associated with accessing, using, or disclosing PHI and ePHI. Further, I am responsible for training all personnel who are working with PHI or ePHI on this project and will retain records of annual HIPAA training. A copy of this memorandum will be given to all personnel who are working with PHI or ePHI on this project.

_____

Principal Investigator Date

_____

Department Chair/Director Date

_____

Department IT Director Date