Investigator Checklist for Verification of Compliance with the Department of Energy (DOE) Requirements for the Protection of Personally Identifiable Information (PII) or Protected Health Information (PHI)

Investigators conducting human subject research supported or regulated by the DOE **and** involving collection of PII or PHI, complete the following to address compliance with DOE requirements and include with IRB submission.
For technical assistance with encryption, etc, please consult departmental Information Technology (IT) or University of Kentucky IT Security. For a summary of requirements for DoE supported research, see ORI's summary document [PDF].

Instructions: Review and check to indicate criteria are evident and have been met for items applicable to your proposed research.

□ The research protocol and/or IRB submission (i.e. research description) includes information on how the research team will keep PII/PHI confidential.

I agree to:

□ release PII/PHI, where required, only under a procedure approved by the IRB and DOE;

□ use PII/PHI only for purposes of the study protocol;

□ handle and mark documents containing PII/PHI as "**containing PII or PHI**;"

□ establish reasonable administrative, technical, and physical safeguards to prevent unauthorized use or disclosure of PII/PHI;

□ make no further use or disclosure of the PII/PHI except when approved by the IRB and DOE, where applicable, and then only under the following circumstances:

(a) in an emergency affecting the health or safety of any individual;
(b) for use in another research project under these same conditions and with DOE written authorization;
(c) for disclosure to a person authorized by the DOE program office for the purpose of an audit related to the project;
(d) when required by law; or
(e) with the consent of the participant;

□ protect PII/PHI stored on removable media (CD, DVD, USB Flash Drives, etc.) using encryption products that are Federal Information Processing Standards (FIPS) 140-3 certified;

□ use passwords to protect PII/PHI used in conjunction with FIPS 140-3 certified encryption;

□ send removable media containing PII/PHI, as required, by express overnight service with signature and tracking capability, and shipping hard copy documents double wrapped;

□ encrypt data files containing PII/PHI that are being sent by e-mail with FIPS 140-2 certified encryption products;

□ send passwords that are used to encrypt data files containing PII/PHI separately from the encrypted data file, i.e. separate e-mail, telephone call, separate letter;

□ use FIPS 140-2 certified encryption methods for websites established for the submission of information that includes PII/PHI;

□ use two-factor authentication for logon access control for remote access to systems and databases that contain PII/PHI. (Two-factor authentication is contained in the National Institute of Standards and Technology (NIST) Special Publication 800-63 Version 1.0.2 [https://csrc.nist.gov/publications/detail/sp/800-63/3/final];

□ report the loss or suspected loss of PII/PHI **immediately** upon discovery, **(as soon as aware of incident),** to: 1) DOE Program manager or the DOE funding office HSP Program Manager or the DOE-CIRC (1-866-941-2472) if the DOE Program manager is unreachable; and 2) the IRB.

Your signature below indicates your understanding and intention to comply with the Department of Energy's requirements as stated above:

____ ______________________
Signature of Principal Investigator Date

Source: http://humansubjects.energy.gov/other-resources/documents/IRB-template-for-reviewing-PII-protocols-2010_ac.pdf