Office of Health, Safety and Security

Checklist for IRBs to Use in Verifying that Human Subject Research Protocols are in Compliance with Department of Energy (DOE) Requirements

The following items must be addressed in all protocols:

Keeping Personal Identifiable Information (PII) Confidential:

- Releasing PII only under a procedure approved by the responsible IRB(s) and Department of Energy (DOE), where required;
- Using PII only for purposes of this program, assisting participants filing claims under the Energy Employees Occupational Illness Compensation Program (EEOICP), or with the consent of the participant;
- Handling and marking documents containing PII as "containing PII or Personal Health Information (PHI)."
- Establishing reasonable administrative, technical, and physical safeguards to prevent unauthorized use or disclosure of PII;
    - Making no further use or disclosure of the PII except when approved by the responsible IRB(s) and DOE, where applicable, and then only under the following circumstances:
        - in an emergency affecting the health or safety of any individual;
        - for use in another research project under these same conditions and with DOE written authorization;
        - for disclosure to a person authorized by the DOE program office for the purpose of an audit related to the project;
        - when required by law; or
        - with the consent of the participant.
    - Protecting PII data stored on removable media (CD, DVD, USB Flash Drives, etc.) using encryption products that are Federal Information Processing Standards (FIPS) 140-2 certified;
    - Using passwords to protect PII used in conjunction with FIPS 140-2 certified encryption that meet the current DOE password requirements cited in DOE Guide 205.3-1;
    - Sending removable media containing PII, as required, by express overnight service with signature and tracking capability, and shipping hard copy documents double wrapped;
    - Encrypting data files containing PII that are being sent by E-mail with FIPS 140-2 certified encryption products;
    - Sending passwords that are used to encrypt data files containing PII separately from the encrypted data file, i.e., separate e-mail, telephone call, separate letter;

- Using FIPS 140-2 certified encryption methods for websites established for the submission of information that includes PII;
- Using two-factor authentication for logon access control for remote access to systems and databases that contain PII. Two-factor authentication is contained in the *National Institute of Standards and Technology (NIST) Special Publication 800-63 Version 1.0.2.* (http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf)
- Reporting the loss or suspected loss of PII immediately upon discovery to:
  - The DOE funding office Program Manager; and
  - The applicable IRBs (as designated by the DOE Program Manager).
  - If the DOE Program Manager is unreachable, immediately notify the DOE-CIRC (1-866-941-2472), http://www.doecirc.energy.gov/

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