DOE INSTITUTIONAL REVIEW BOARD TEMPLATE FOR REVIEWING HUMAN SUBJECTS RESEARCH PROTOCOLS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION (PII)

The following items must be addressed in all protocols:

1. Keeping PII confidential;
2. Releasing PII, where required, only under a procedure approved by the responsible IRB(s) and DOE;
3. Using PII only for purposes of this project;
4. Handling and marking documents containing PII as "containing PII or PHI;"
5. Establishing reasonable administrative, technical, and physical safeguards to prevent unauthorized use or disclosure of PII;
6. 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: (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;
7. 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;
8. 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;
9. Sending removable media containing PII, as required, by express overnight service with signature and tracking capability, and shipping hard copy documents double wrapped;
10. Encrypting data files containing PII that are being sent by e-mail with FIPS 140-2 certified encryption products;
11. 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;
12. Using FIPS 140-2 certified encryption methods for websites established for the submission of information that includes PII;
13. 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 found at: http://csrc.nist.gov/publication/nistpubs/800-63/SP800-63V 1 0 2.pdf);
14. Reporting the loss or suspected loss of PII immediately upon discovery to: 1) the DOE funding office Program Manager; and 2) 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, www.doecirc.energy.gov).