In accordance with the Privacy Act, the DOE has established requirements for the protection of Personally Identifiable Information (PII) with the DOE Privacy Program (DOE Order 206.1), DOE Manual (M) for Identifying and Protecting Official Use Only Information (DOE M 471.3-1) and DOE Cyber Security Incident Management Manual (DOE M 205.18-8).

***Personally Identifiable Information (PII):*** Any information collected or maintained about an individual, including but not limited to, education, financial transactions, medical history and criminal or employment history, and information that can be used to distinguish or trace an individual’s identity, such as his/her name, Social Security number, date and place of birth, mother’s maiden name, biometric data, and any other personal information that is linked or linkable to a specific individual.

**Research Protocols Must Include Description of Processes for:**

* Keeping PII confidential
* Releasing PII only under a procedure approved by the responsible IRB(s) and DOE, where required
* Using PII only for purposes of the DOE-approved research
* Handling and marking documents containing PII as “containing PII” or “containing 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:
* 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
* 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 FIPS 140-2 certified encryption that meet the current DOE password requirements cited in DOE Guide 205.3-1
* Shipping removable media containing PII, as required, by express overnight service with signature and tracking capability, and shipping hard copy documents double wrapped via express overnight service
* 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 found at:

<http://csrc.nist.gov/publications/nistpubs/800-63-1/SP-800-63-1.pdf>)

In addition to other reporting requirements, reporting the loss or suspected loss of PII *immediately* upon discovery to: 1) the DOE Project Officer; and 2) the applicable IRBs.

(\*Adapted from: <http://humansubjects.energy.gov/other-resources/09hswg-mtg/associated_files/WhiteExpectationsofDOESiteIRBsPII_ac.ppt>)