Regulations and directives that specifically address the protection of human subjects include 10 CFR Part 745; 45 CFR Part 46, Subparts B, C, and D; Department of Health and Human Services Regulation on Protection of Human Subjects; and DOE O 443.1A, Protection of Human Subjects, dated 12-20-07. The requirements of all applicable regulations and directives must be met before any research involving human subjects is initiated.

In addition to traditional biomedical and clinical studies, the DOE considers human subjects research to include but is not limited to studies that:

- use humans to examine devices, products, or materials with the express purpose of investigating human-machine interfaces or evaluating environmental alterations when humans are the subjects being tested;
- use personally identifiable bodily materials such as cells, blood, tissues, urine, or hair, even if the materials were collected previously for a purpose other than the current research;
- collect and use personally identifiable information such as genetic information or medical and exposure records, even if the information was collected previously for a purpose other than the current research;
- collect personally identifiable data, surveys, or questionnaires through direct intervention or interaction with individuals; and
- search for generalizable knowledge about categories or classes of subjects (e.g., linking job conditions of worker populations to hazardous or adverse health outcomes).

The DOE does not consider the following human subject research:

- studies to improve the safety or execution of procedures that apply to routine occupational activities;
- occupational health surveillance of DOE Federal and contractor employees to determine apparent departures from typical health status and not for the purpose of obtaining generalizable knowledge; and
- employee surveys used as management tools to improve worker or contractor performance as long as the identity of the participant is protected.

Research protocols must include a description of processes for:

- Keeping (Personally Identifiable Information) PII confidential;
• Releasing PII only under a procedure approved by the IRB and DOE, where required;

• Using PPII only for purposes of the DOE-approved research and/or EEOICPA;

• Handling and marking documents containing PII

• Establishing reasonable administrative, technical, and physical safeguards to prevent unauthorized use or disclose of PII;

• Marking no further use or disclose of the PII except when approved by the IRB and DOE, where applicable, and then only:
  o In an emergency affecting the health or safety of any individual;
  o For use in another research project under these same conditions and with (Department of Energy) DOE written authorization;
  o For disclosure to a person authorized by the DOE program office for the purpose of an audit related to the project; or
  o When required by law.

• Protecting PII data stored on removable media (CD, DVD, Flash Drives, etc.) using encryption products that are Federal Information Processing Standards (FIPS) 140-2 certified;

• Using FIPS 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 certified encryption methods for web sites established for the submission of information containing PII;

• Using two-factor authentication for logon access control for remote access to systems and database that contain PII (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:
  o The DOE Project Officer; and
  o IRB

DOE Order 443.1A requires prompt reporting to the DOE HSR Program Manager, and coordination with and approval from the HSR Program Managers in determining plans to correct the unanticipated problem. While DOE 443.1A does not define “prompt,” they request that the HSR Program Manager(s) be notified within 48 hours of learning of any unanticipated problem that does not involve personally identifiable information (PII). However, if potential loss or compromise of personally identifiable
information is involved, the incident should be reported immediately (as soon as you learn about the incident) to the Departmental Element; the DOE Cyber Incident Response Capability at doecirc@doecirc.energy.gov or 8660941-2472 and to the DOE HSR Program Manager(s).

References:

10 CFR 745 – “Protection of Human Subjects”

Checklist for IRBs to Use in Verifying that HS Research Protocols are in Compliance with DOE Requirements

HQ Expectations of DOE Site IRBs- “Reporting Unanticipated Problems and Review/Approval of Projects that Use Personally Identifiable Information” – May 7, 2009

DOE Order 443.1A