Michigan State University
Human Research Protection Program

Subject: U.S. Department of Energy

Section: 2-2-E

This policy and procedure supersedes those previously drafted.

Approved by: Vice President of Research and Graduate Studies, 7-19-2011.

Related Sections: 3-3, 4-8, 8-1, 8-10, 9-1, 9-2, 9-3


Unless otherwise required by department or agency heads, research activities in which the only involvement of human subjects will be in one or more of the exempt categories, outlined in the Human Research Protection Program (HRPP) Manual 8-1 “Exemptions,” are exempt from this policy.

No human subject research conducted with DOE funding may be initiated without both a Federalwide Assurance (FWA) and approval by the Institutional Review Board (IRB) in accordance with 10 CFR 745.103 and 45 CFR 46.

MSU periodically conducts self-assessments to ensure compliance with the HRPP procedures and requirements. The HRPP monitors the effectiveness of the program through routine, for-cause, internal, and self-assessment evaluations. See HRPP Manual 3-3 “Evaluation and Quality Improvement” and 8-10 “Project Audits” for policy and procedures on self-assessments.

Investigators must submit the “Checklist for IRBs to Use in Verifying that HS Research Protocols Are in Compliance with DOE requirements.” The IRB must review and approve the checklist submitted by the investigators to verify compliance with the DOE requirements for the protection of personally identifiable information. Investigators are required to follow DOE requirements for the protection of personally identifiable information.

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 for Identifying and Protecting Official Use Only Information (DOE M 471.3-1); and DOE Cyber Security Incident Management Manual (DOE M 205.1-8).
Research protocols must include a description of the processes for the following:

1. Keeping PII confidential.
2. Releasing PII only under a procedure approved by the responsible IRB(s) and DOE, when required.
3. Using PII only for purposes of the DOE-approved research.
4. Handling and marking documents containing PII as “containing PII” or “containing 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:
   a. In an emergency affecting the health or safety of any individual;
   b. For use in another research study 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 study; or
   d. When required by law.
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 FIPS 140-2 certified encryption that meet the current DOE password requirements cited in DOE Guide 205.3-1.
9. 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.
10. Encrypting data files containing PII that are being sent by e-mail with FIPS 14—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/publications/nistpubs/800-63/SP800-63V1_0_2.pdf).

In addition to other reporting requirements, reporting the loss or suspected loss of PII immediately upon discovery to the DOE Project Officer; and the applicable IRB(s).

Types of breaches that must be reported include, but are not limited to the following
- Loss of control of DOE employee information consisting of names and social security numbers;
- Loss of control of Department credit card holder information;
- Loss of control of PII pertaining to the public;
- loss of control of security information (e.g., logons passwords);
- incorrect delivery of PII;
- theft of PII; and
- unauthorized access to PII stored on Department-operated web sites.

While DOE order 443.1A does not define “prompt”, the DOE requests that the HSR Program Manager(s) are notified within 48 hours of learning of any unanticipated problem that does not involve PII.

Researchers must promptly report the following to the human subject research program manager:
- Any significant adverse events, unanticipated risks; and complaints about the research, with a description of any corrective actions taken or to be taken.
- Any suspension or termination of IRB approval of research.
- Any significant noncompliance with HRPP procedures or other requirements.
- Any compromise of personally identifiable information must be reported immediately.

See the following sections of the HRPP Manual for specific requirements (e.g., timeframes): 4-8 “Reporting,” 9-1 “Unanticipated Problems Involving Risks to Subjects or Others,” 9-2 “Noncompliance,” and 9-3 “Termination or Suspension of Research.”