Title: Personally Identifiable Information (PII) Standard Operating Procedure: #14
Department: Human Research Protection Program/Institutional Review Board
Original Publication Date: March 22, 2010
Revision Date: September 2017

Subject: Department of Energy Requirements for Protecting PII at National Laboratories

Definitions:

Personally Identifiable Information (PII): The U.S. Department of Energy, Office of Management and Budget, has defined Personally Identifiable Information (PII) as

> ". . . any information collected or maintained by the Department 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 identify, such as his/her name, Social Security number, date and place of birth, mother's maiden name, biometric data, and including any other personal information that is linked or linkable to a specific individual."

(1) The DOE HSP Program Manager (and when an NNSA element is involved, the NNSA HSP Program Manager) shall be notified immediately upon a finding of a suspected or confirmed data breach involving Personally Identifiable Information (PII) in printed or electronic form and reported to the DOE-Cyber Incident Response Capability in accordance with the requirements of DOE O 206.1. The appropriate HSP Program Manager shall also be informed of any corrective actions taken and shall concur on the plan for any remaining corrective actions.

... the Contractor shall ... Ensure notification of the DOE HSP Program Manager (and, when and NNSA element is involved, the NNSA HSP Program Manager):

Within 48 hours of the following, and, provide a description of corrective actions taken immediately following the incident, as well as corrective actions to be taken for concurrence by the appropriate HSP Program Manager:

...Immediately, of a finding of a suspected or confirmed data breach involving PII in printed or electronic form and to the DOE-Cyber Incident Response Capability immediately in accordance with the requirements of CRD associated with DOE O 206.1, and provide a description of any corrective actions taken within 48 hours and a description of corrective actions to be taken for concurrence by the appropriate HSP Program Manager.

Reference:

DOE O.206.1, *Department of Energy Privacy Program*, dated 1-16-09, which ensures compliance with privacy requirements;-establishes a Departmental training and awareness program for all DOE Federal and contractor employees to ensure personnel are cognizant of their responsibilities for safeguarding Personally Identifiable Information (PII) and complying with the Privacy Act; and provides Departmental oversight to ensure compliance.

IRB-approved Protocols: The Human Research Protection Office (OHRP) shall examine and verify that protocol(s) have clear and detailed plan(s) for protecting PII in accordance with federal/DOE requirements, including safe storage of PII (file cabinets, computers), encryption of data to be transferred, and immediate notification of incident(s) involving potential compromise or loss of PII data.

New protocols: The Human Research Protection Office shall verify that there are clear and detailed plan(s) for protecting PII in accordance with federal and DOE requirements.

Policy:
In accordance with federal and DOE requirements, PII transferred from one organization to another as part of a human research project [when/as authorized by the approving IRB(s), the responsible DOE Program Office, and the research participant] must first be encrypted consistent with PII protection requirements stated in DOE M 205.1-7 using a program such as Entrust.

Code of Federal Regulations 45 CFR 46 calls for prompt reporting of violations to the IRB, appropriate institutional and agency officials, and the OHRP.

OHRP guidance recommends that the PI report an unanticipated problem to the IRB within two (2) weeks and that the PI or PI's organization report the unanticipated problem to OHRP within six (6) weeks [or within one (1) month of notifying the IRB].

DOE Order 443.1B also requires prompt reporting to the DOE Human Subjects Research (HSR) Program Manager, SC-23 and the DOE Program Manager, National Nuclear Security Administration (NNSA) for NNSA sites, and coordination with and approval from the HSR Program Manager(s) in determining plans to correct the unanticipated problem.

While DOE Order 443.1B does not define "prompt," the DOE Program Manager requests that the HSR Program Manager(s) receive notification within 48 hours of learning of any unanticipated problem that *does not involve* PII.

If potential loss or compromise of PII *is involved*, as soon as investigator learns of the incident he/she shall report the incident:

- To the IRB Office within the Human Research Protection Office

The IRB Office shall then report the incident to the:

- DOE-Cyber Incident Response Capability (DOE-CIRC) at doecirc@doecirc.energy.gov or 866-941-2472; *and* The DOE HSR Program Manager(s).

Procedures:

Department of Energy Headquarters Expectations Regarding Unanticipated Problems at Site IRBs.

In accordance with the Privacy Act[1], the DOE has established requirements for the protection of PII with the:

[1] The Privacy Act of 1974, as amended at Title 5 United States Code (U.S.C.) 552a, governs a federal agency's ability to maintain, collect, use, or disseminate a record about an individual. Information collected under the Privacy Act must be stored in a Privacy Act System of Records (SOR).

- DOE Privacy Program (DOE Order 206.1).
- DOE Manual for Identifying and Protecting Official Use Only Information (DOE M 471.3-1).
- DOE Cyber Security Incident Management Manual (DOE M 205.1-8).

Research protocols must include description of processes for:

- Keeping PII confidential.
- Releasing PII only under a procedure approved by the responsible IRB and DOE, where required.
- Using PII only for purposes of the DOE-approved research and/or Energy Employees Occupational Illness Compensation Program Act (EEOICPA).
- Handling and marking documents containing PII as "containing PII" or "containing Protected 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:

- 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.

The following guidelines need to be followed to assure both the safety and integrity of PII:

- Protect 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.
- Use FIPS 140-2 certified encryption that meets the current DOE password requirements cited in DOE Guide 205.3-1.
- Ship 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.
- Encrypt data files containing PII that are being sent by e-mail with FIPS 140-2 certified encryption products.
- Send passwords that are used to encrypt data files containing PII separately from the encrypted data file (i.e., separate e-mail, telephone call, or separate letter).
- Use FIPS 140-2 certified encryption methods for websites established for the submission of information that includes PII.

- Use 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 on the NIST Computer Security Resource Center Website

In addition to other reporting requirements, reporting the loss or suspected loss of PII ***immediately upon discovery*** to the DOE Project Office and the applicable IRB.

References:

DOE Order 206.1
DOE M 471.3-1
DOE M 205.1-7
DOE M 205.1-8
DOE IRB Template for Reviewing Former Worker Medical Screening Program Protocols LLNL/IRB – A. Dake & J. Knezovich (12/28/09)