

**Overview:**

The IRB will 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.

Per DOE O 4431C:

*As directed by the contracting officer, the contractor must—*

*1. Notify the DOE HSP Program Manager (and, when an NNSA element is involved, the NNSA HSP Program Manager):*

*1 c. Immediately, upon finding of a suspected or confirmed data breach involving PII in printed or electronic form, and additionally immediately notify the DOE-Cyber Incident Response Capability, in accordance with the requirements of the CRD associated with DOE O 206.1. The HSP Program Manager(s) shall also be notified of any corrective actions taken and consulted regarding the plan for any remaining corrective actions.*

**Procedures:**

**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). (The Energy Employees Occupational Illness Compensation Program Act (EEOICPA) was enacted to provide compensation and medical benefits to employees who worked at certain Department of Energy (DOE) facilities, including contractors and subcontractors at those locations, and certain of its vendors.)
- 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.

**Research protocols should ensure that there will be 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.
- 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 Program Managers and the applicable IRB.

**References:**

DOE Order 206.1, Change 1 [Department of Energy Privacy Program](#)

DOE Order 205.1C [Department of Energy Cyber Security Program](#)

## Document Review History

Revision Number	Date	Author	Summary of Changes
01	September 2017	Ann-Marie Dake	Complete Revision
02	November 2018	Dawn Whalen	Document control process added
03	November 2019	IRB Office	Complete Revision
04	October 2020	Ann-Marie Dake	Revisions and updates