Guidance: Additional Requirements for U.S. Department of Energy (DOE) Sponsored Research

1. Introduction

DOE has adopted the Common Rule at 10 CFR Part 745 and has published additional requirements for research it supports or conducts as described in DOE Order 443.1B Chg1, Protection of Human Research Subjects. Researchers are responsible for reviewing these documents to understand the applicable requirements and should check with their DOE Program Officer to ensure that all DOE requirements are met prior to beginning research.

2. Special Considerations for DOE-supported Research

2.1 Expansion of Definition of Research with Human Subjects for Research Involving Intentional Modification of the Human Environment

DOE has expanded the definition of human subjects research found at 45 CFR 46 as follows:

a. Research involving human participants also includes studies that involve the intentional modification of the human environment; generalizable includes the study of tracer chemical, particles, or other materials to characterize airflow.

b. Generalizable also includes studies in occupied homes or offices that:
   - Manipulate the environment to achieve research aims.
   - Test new materials
   - Involve collecting information on occupants' views of appliances, materials, or devices installed in their homes or their energy-saving behaviors through surveys and focus groups.

2.2 IRB Review of Research Involving Expanded Definition

Even if the IRB does not view a project as meeting the literal definition of human subjects research as defined in 45 CFR Part 46, DOE requires initial review of the application and supporting materials by the IRB to determine whether the individuals included in the research will be **properly informed and protected.** The IRB must consider if additional protections are required for research involving DOE employees and contractors.

- The chair decides the level of review.
- The IRB assesses risks associated with the research and whether the individuals to be included in the research will be properly informed and protected.
- The chair sends a letter to the researcher indicating that the research has been approved in accordance with DOE expectations and will be monitored and tracked by the IRB.

2.3 Research involving Personally Identifiable Information (PII)

For research that involves PII, investigators must complete and comply with the requirements outlined in "Checklist – Reviewing Protocols that Use PII" developed in coordination with the National Nuclear Security Administration (see attached). The IRB must verify compliance with those requirements in its review of the project.

2.4 Research Involving DOE Employees and Contractors

Requirements for human participant protections and their accompanying Contractor Requirements Documents (CRDs) apply to all research conducted at DOE institutions regardless of funding source, or by DOE employees/contractor personnel regardless of funding source or location conducted, and whether done domestically or in an international environment, and including Human Terrain Mapping research.

DOE employees and contractors are considered vulnerable subjects and shall be afforded additional protections as determined by the IRB.

2.5 Informed Consent Disclosure of Sponsoring Agency

Informed consent documents must contain the identity of the sponsoring agency unless the sponsor requests that it not be done, because doing so could compromise intelligence sources or methods; the research involves no more than minimal risk to participants; and the IRB determines that by not disclosing the identity, the investigators will not adversely affect the participants.

2.6 Notifications to the DOE Human Subjects Protection Manager (HSP)

The HSP should be notified within 48 hours of any:

- Significant adverse events, unanticipated problems or complaints about the research, with a description of any corrective actions taken or to be taken.
- Study suspensions or terminations of IRB approval of research.
- Significant noncompliance with HRPP procedures or other requirements.

The HSP should be notified immediately when there is a breach of PII.

- The time frame for immediately is defined as upon discovery.

2.7 Periodic HRPP Self-Assessment

Organizations that conduct DOE regulated research are required to conduct periodic self-assessments to ensure compliance with DOE Human Subjects Protection Program requirements.

The purpose of this checklist is to provide support for IRB members or the Designated Reviewer to verify that the following items are addressed in all protocols that use PII or PHI. For the IRB, this checklist must be used for all reviews (initial, continuing, modification, review by the convened IRB, and review using the expedited procedure).

- For initial review using the expedited procedure and modifications and CRs where the determinations relevant to this checklist made on the previous review have changed, the Designated Reviewer completes this checklist to document determinations required by the regulations along with protocol specific findings justifying those determinations. The Designated Reviewer attaches this checklist to "Submit Designated Review" activity.
- For initial review using the convened IRB and for modifications and CRs where the determinations relevant to this checklist made on the previous review have changed, one of the following two options may be used:
  1. The convened IRB complete the corresponding section of the meeting minutes to document determinations required by the regulations along with protocol specific findings justifying those determinations, in which case this checklist does not need to be completed or retained.
  2. The convened IRB complete this checklist to document determinations required by the regulations along with protocol specific findings justifying those determinations and the IRB uploads this checklist in the "Submit Committee Review" activity.

1 Protocols that Use PII. The protocol includes provisions for:
(Check if **"Yes"**. All must be checked or completed.)

☐	Keeping PII/ PHI confidential. *Provide any supporting comments*:
☐	Protecting PII/PHI during storage and transmission. *Provide any supporting comments*:
☐	Releasing PII/PHI, where required, only under a procedure approved by the responsible IRB and DOE. *Provide any supporting comments*:
☐	Using PII/PHI only for purposes of this project. *Provide any supporting comments*:

☐	Handling and marking documents containing PII or PHI as "containing PII or PHI. *Provide any supporting comments*:
☐	Establishing reasonable administrative, technical, and physical safeguards to prevent unauthorized use or disclosure of PII/PHI. *Provide any supporting comments*:
☐	Making no further use or disclosure of the PII/PHI except when approved by the responsible IRB and DOE, where applicable, and then only under the following circumstances: (a) in an emergency affecting the health or safety of any individual; (b) for use in another research project 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 project, as required by Office of Management and Budget Circular No. A-133; (d) when required by law; or (e) with the consent of the participant/guardian. *Provide any supporting comments*:
☐	Protecting PII/PHI data stored on removable media (CD, DVD, USB Flash Drives, etc.), network drives, and stand-alone computers using encryption products that are FIPS 140-2 certified. *Provide any supporting comments*:
☐	Using passwords to protect PII/PHI used in conjunction with FIPS 140-2 certified encryption products that meet the following current DOE password requirements[1]: • Minimum of twelve (12) non-blank characters • Must contain a lowercase letter • Must contain an uppercase letter • Must contain a number or special character • Must contain a nonnumeric in the first and last position • Must not contain the user ID *Provide any supporting comments*:

[1] The following are good practice guidelines to follow:

- Password does not include the user's own or, to the best of his/her knowledge, close friends' or relatives' names, employee serial number, Social Security number, birth date, phone number, or any information about him/her that the user believes could be readily learned or guessed;
- Password does not, to the best of the user's knowledge, include common words that would be in an English dictionary or from another language with which the user has familiarity;
- Password does not, to the best of the user's knowledge, employ commonly used proper names, including the name of any fictional character or place; and
- Password does not contain any simple pattern of letters or numbers, such as "qwertyxx" or "xyz123xx".

☐	Sending removable media containing PII, as required, by express overnight service with signature and tracking capability, and shipping hard copy documents double wrapped. *Provide any supporting comments*:
☐	Encrypting data files containing PII that are being sent by e-mail with FIPS 140-2 certified encryption products. *Provide any supporting comments*:
☐	Accessing data via a secure, encrypted internet connection or through an Electronic Data Interface using TLS 1.1 or newer. *Provide any supporting comments*:
☐	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. *Provide any supporting comments*:
☐	Using TLS 1.1 encryption methods or higher for websites established for the submission of information that includes PII. *Provide any supporting comments*:
☐	Using two-factor authentication for logon access control for remote access to systems and databases that contain PII/PHI. (Two-factor authentication is contained in the NIST Special Publication 800-63.) *Provide any supporting comments*:
☐	Reporting the loss or suspected loss of PII/PHI immediately upon discovery to: 1. The DOE funding office Program Manager or, if funded by a DOE laboratory, the DOE laboratory Program Manager; and 2. The DOE HSP Program Manager and the NNSA HSP Program Manager. If these individuals are unreachable, immediately notify the DOE-CIRC by phone at 1-866-941-2472, by fax at 702-932-0189, or by e-mail at circ@jc3.doe.gov. For additional information, see: http://energy.gov/cio/office-chief-information-officer/services/incident-management/jc3-incident-reporting. *Provide any supporting comments*:
☐	Classified projects that use PII/PHI must also comply with all requirements for conducting classified research. *Provide any supporting comments*: