MUSC
Medical University
of South Carolina

IRB Reviewer Checklist Federal Funding
Department of Energy

Reviewer: **PRO:** **PI:**

This checklist is designed to support the IRB reviewer in evaluation of protocols funded by the Department of Energy (DoE):				
1.	Is there a system in place to keep the Personally Identifiable Information (PII) confidential?	○Yes	○No	
2	If releasing PII, where required, does the PI have the required procedure approval from the IRB(s) and DoE?	○Yes	○No	
3	Is the PI using PII only for the purpose of this project?	○Yes	○No	
4.	Has the PI established a plan for handling and marking documents containing PII as "containing PII or PHI?"	○Yes	○No	
5	Has the PI established reasonable administrative, technical, and physical safeguards to prevent unauthorized use or disclosure of PII?	○Yes	○No	
6	Has the PI addressed when making no further use or disclosure of the PII except when approved by the responsible IRB and DoE, where applicable, and then only a) in an emergency affecting the health and 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 d) when required by law?	○Yes	○No	
7	Has the PI established a plan to protect PII data stored on removable media (CD, DVD, USB Flash Drives, etc.) and to use encryption products that are Federal Information Processing Standards (FIPS) 140-2-certified?	○Yes	○No	
8	Has the PI established a plan to use passwords to protect PII used in conjunction with FIPS 140-2 certified encryption that meet the current DoE password requirements cited in DoE Guide 205.3-1?	○Yes	○No	
9	Has the PI addressed the sending of removable media containing PII, as required, by express overnight services with signature and tracking capability, and shipping hard copy documents double wrapped?	○Yes	○No	
10	Has the PI established a plan to use encrypting data files containing PII that will be sent by e-mail with FIPS 140-2 encryption products?	○Yes	○No	
11	Has the PI established a plan when sending passwords that are used to encrypt data files containing PII separately from the encrypted data file, i.e. separate e-mail, telephone call, and separate letter?	○Yes	○No	
12	Has the PI addressed FIPS 140-2 certified encryption methods for websites established for the submission of information that includes PII?	○Yes	○No	
13	Has the PI addressed using two-factor authentication for logon access control for remote access to systems and databases that contain PII?	○Yes	○No	
14	Has the PI addressed reporting the loss or suspected loss of PII immediately upon discovery to: 1) the DoE Project Manager and 2) the IRB?	○Yes	○No	
15	When using Classified projects that use PII, is the PI complying with all requirements for conduction Classified research?	○Yes	○No	
If the answer to any question is No, the research is not allowable under DoE guidelines				

NOTE: MUSC uses PGP encryption for all removable media containing PII data. PGP is validated to the standards set forth by the FIPS PUB 140-2 Security Requirements for Cryptographic Modules document published by the National Institute of Standards and Technology (NIST).