24. Information Security

University of Virginia has established standards and safeguards to protect patient's information and to ensure compliance with federal and state information security regulations. It is the responsibility of investigators to familiarize themselves with and comply with these standards which may be found on the Information Security (InfoSec) website. The use of individual use devices such as personal laptops, desktops, portable/USB drives, or other non-University of Virginia devices for storage of research data is discouraged. In the instances when an individual use device or a non-University of Virginia computer or device must be used for the purposes of storing, even temporarily, or transmitting PHI or PII (Personally Identifiable Information) for research, the safeguards of the device must be verified by InfoSec and the study team must submit the Highly Sensitive Data Storage Request form. This form requires the signatures of a Department Manager or Chair and a VP or Dean. Additionally, any potential or known breach of a device or of research data must be immediately reported according to the Information Security Incident Reporting Policy so that appropriate steps can be taken to assess the situation, protect the information, and comply with regulations. Any data breach will also be reported to the IRB of Record if the report meets the criteria of an Unanticipated Problem.

Provisions for Data Security must be described in Data Security Plan to the IRB and updated as necessary. When information containing direct identifiers such as Social Security numbers or PHI including data considered sensitive is to be transferred outside of the institution, the provisions for data security may be subject to further review by InfoSec.