Guidance on the Protection of CRITICAL Data in IU Health Sciences

This document provides guidance on establishing appropriate system security for computer systems that may contain CRITICAL data within IU Health Sciences organizations. This guidance is based on university and school policies and also the requirements of the Health Information Portability and Accountability Act (HIPAA).

Indiana University IT policy IT-12, Security of University IT Resources states that organizational units (campuses, departments, offices, affiliated agencies, etc.) operating technology resources are responsible for ensuring that those systems are managed securely. Among other things, IT-12 requires that "... functional unit technicians must fully understand the sensitivity of the function or operation being supported by the system and the data being stored and/or manipulated on the system."

The HIPAA security rule also provides guidance related to the security of technology resources where ePHI may be present. Specifically, §164.310(c), Workstation Security states "Implement physical safeguards for all workstations that access electronic protected health information, to restrict access to authorized users."

Based on the above policies, IU health science organizations must ensure appropriate security protections are in place for all computer systems that may contain CRITICAL data. If data volumes are so large that available resources cannot appropriately audit individual data stores for proper classification, it is recommended that organizations treat all data they manage as CRITICAL.

Any further questions can be directed to this office by calling 317-278-8751 or email erschmid@iu.edu.