INDIANA UNIVERSITY

59 – Health Care Data Confidentiality

Action Item Template Response

General Action Item Information

Lead Division/Office: IUSM information Services and Technology Management
Action Item Number: 59
Action Item Short Name: Health Care Data Confidentiality
Dependencies with other EP Action Items: 22
Implementation leader (name & email): Vince Sheehan (vsheehan@iupui.edu)

I. DESCRIBE YOUR PLANS FOR IMPLEMENTING THIS ACTION.

Policies are in place to protect data in transit. SSL is currently used to protect sensitive data communications wherever possible. A new strategy to protect sensitive data in all communications is required. While policies are in place to require full disk encryption on all laptops and PDAs, we will investigate technologies to protect data stored on other mobile devices.

The University Compliance Office recently certified the High Performance Computing environment (managed by Research Technologies) as HIPAA-compliant. Likewise, the UITS Intelligent Infrastructure needs to be certified as a qualified environment for managing healthcare data so that the IUSM can require all departments to eliminate local servers and transition to that environment. Currently, all ISTM servers are located in the UITS Data Center behind the Data Center firewall, and all remaining departmental servers located in the Data Center will be moved behind the firewall as well.

Sensitive data in school-developed applications are encrypted at the database field level and a secure communications protocol has been established between the IU and Clarian Messaging Systems.

II. WHAT ARE THE POLICY AND PRACTICE IMPLICATIONS OF YOUR PLANS?

New policies and procedures for the use of the Intelligent Infrastructure environment need to be developed. These will be done as part of Action Item 22.

The IUSM will explore new tools to facilitate encryption of mobile devices.

III. IDENTIFY STAKEHOLDERS.

- IUSM
- Indiana Clinic
- Clarian
- Regenstrief
- VA
- Wishard

- IIA