Section 25. **Information Security**

The medical school has established standards and safeguards to protect patient information and to ensure compliance with federal and state information security regulations. There may be additional requirements of an external research site (eg, a hospital or other covered entity), and the sponsor, depending on the study and type of data (eg, PHI) being stored or transmitted. It is the responsibility of investigators and research staff to understand and comply with all required standards for information security.

Medical school information security standards and requirements must be met if the medical school IRB is the IRB of record, or if the research is conducted at, under the auspices of, or using the services or resources of the medical school.

The use of personal computers and devices (eg, laptops, desktops, tablets, smartphones, portable/USB drives) for storing research data is prohibited.

The use of computers and devices owned and managed by another entity (eg, Borgess Health, Bronson Healthcare) for storing, even temporarily, or transmitting PHI or PII (Personally Identifiable Information) for research requires that medical school Information Technology verify the safeguards of the computer or device, and also that a User Agreement is completed.

Any potential or known breach of a device used in the research study, whether the device is owned by the medical school or not, or breach of study data must be immediately reported to both the IRB and the medical school Research Integrity Officer, who is also part of corporate compliance, so that appropriate steps can be taken to assess the situation, protect the information, and comply with regulations and reporting requirements.

Lost or stolen devices that are used for research, whether owned by the medical school or not, must be reported immediately to Information Technology.

Research data that is shared or transmitted between devices or covered entities must be encrypted when transmitted.

Provisions for data security must be described in the study application to the IRB and updated as necessary. When information containing PHI or direct identifiers such as Social Security numbers, including sensitive data that may not be PHI, is to be transferred outside of medical school or computers or devices that have been approved by the IRB, the provisions for data security for the study are subject to further review and approval by medical school Information Technology and the IRB

Investigators and research staff working with or at Borgess Health, Bronson Healthcare, and other covered entities are subject to the separate HIPAA privacy and security policies of the covered entity. Thus, a study may be subject to policies of the medical school and also other covered entities. Regardless of the site or the owner of the computer or device, the storage and transmission of research data must meet medical school security standards and requirements at all times.

Medical School Information Technology staff provide extensive guidance to assist investigators and research staff with standards and safeguards to protect patient information and to ensure compliance with federal and state information security regulations.

25.1 NIH GRANTS

The NIH has specific requirements about ensuring data security when collecting identifiable research data, as described in NIH Grants Policy Statement section 2.3.12, *Protecting Sensitive Data and Information in Research*.

> “Recipients of NIH funds are reminded of their vital responsibility to protect sensitive and confidential data as part of proper stewardship of federally funded research, and take all reasonable and appropriate actions to prevent the inadvertent disclosure, release or loss of sensitive personal information. NIH advises that personally identifiable, sensitive and confidential information about NIH-supported research or research participants not be housed on portable electronic devices. If portable electronic devices must be used, they should be encrypted to safeguard data and information. These devices include laptops, CDs, disc drives, flash drives, etc. Researchers and institutions also should limit access to personally identifiable information through proper access controls such as password protection and other means. Research data should be transmitted only when the security of the recipient's system is known and is satisfactory to the transmitter.”