University of Missouri Position on 21 CFR Part 11 Compliance

Policies

Business Policy Manual: BPM-210, Sponsored Programs
Memo: University of Missouri Position on 21 CFR Part 11 Compliance (attached)

Forms

None

Overview

MU Health Care (MUHC) has made the determination that it cannot provide certification of electronic records or electronic signatures or complete a questionnaire as it relates to 21 CFR Part 11 as these do not apply to the MUHC records maintained for patient care purposes. The attached memo provides information about how records for patient care are maintained in accordance with applicable state and federal requirements.

Need Help?

Contact OSPA at muresearchospact@missouri.edu or 882-7560.

Effective Date

01/29/2014

Office of Sponsored Program Administration
115 Business Loop 70W, 5th Floor | Columbia, MO 65211
573-882-7560 | grantsdc@missouri.edu

MU Sponsored Programs Administration
University of Missouri

UNIVERSITY *of* MISSOURI

MU Health Care (MUHC) has made the determination that we cannot provide the requested certification of our electronic records or electronic signatures or complete a questionnaire as it relates to 21 CFR Part 11 as these do not apply to the MUHC records maintained for patient care purposes. The Food and Drug Administration (FDA) has confirmed this in the recently issued *"Guidance for Industry: Electronic Source Data in Clinical Investigations"* (found at http://www.fda.gov/downloads/Drugs/GuidanceComplianceRegulatoryInformation/Guidances/UCM328691.pdf, page 8, section IV, *Use and Description of Computerized Systems in Clinical Investigations.*)

Records for patient care are maintained in accordance with other state and federal requirements but not specifically in accordance with the requirements of the Federal Food, Drug, and Cosmetic Act (the Act), Public Health Service Act (the PHS Act), or other FDA regulations. In addition, our patient records (electronic or paper) are not submitted to the FDA by our health care providers. However, data may be abstracted by researchers and then submitted to the FDA or drug sponsors by the principal investigators as a result of a research investigation. For this purpose we provide the following information.

MUHC provides the following electronic medical record system(s) that is also accessed for research and clinical studies:

- Cerner Millennium PowerChart

This system is not required to be compliant with the FDA regulations for research systems, but, as required, it is in compliance with the HIPAA Privacy and Security Rules. In addition, the Cerner system is certified for the purposes of the Meaningful Use incentive program. Under the Meaningful Use requirements of the HITECH Act passed in 2009, electronic health record (EHR) technology must be tested and certified by an Office of the National Coordinator (ONC) Authorized Testing and Certification Body (ATCB). The Cerner system was tested and certified by the Certification Commission for Healthcare Information Technology (CCHIT), an ATCB, meaning that the following requirements are being met:

- Provides the ability to produce a human-readable copy of data (which includes audit trails and the translation of coded data)
- Includes an audit trail that records date, time, and author of any data created, changed, or deleted
- Prevents new audit trail information from over-writing existing or previous information
- Provides the ability to create, maintain, and apply the roles, access permissions, and capabilities of each user that accesses the system so that users have access
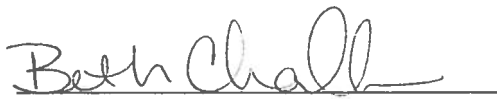
only to those system features and functions to which they have been granted access

- Ensures that data used for clinical research source records are retained for the legal period

As specified in the HITECH legislation, in order for a provider or hospital to qualify for incentive payments, they must prove through an attestation process that the system has the specified capabilities and that they are being used. (Our health system) has completed this attestation of meaningful use. In addition to the above system features, the Chief Information Officer (CIO) has also attested to having or providing the following:

- Documented standard operating procedures
- Appropriate education and training for individuals who develop, maintain, and use the systems
- Data integrity due to appropriate lifecycle practices for both hardware and software from the standpoint of both the vendor and the IT Services department.

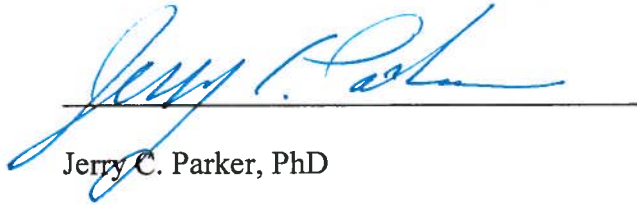Thank you for the opportunity to provide this information.

Beth Chancellor

Chief Information Security Officer

University of Missouri System

Jerry C. Parker, PhD

Associate Dean for Research

University of Missouri Health System