AAMC

Association of
American Medical Colleges
655 K Street, N.W., Suite 100, Washington, D.C. 20001-2399
T 202 828 0400
www.aamc.org

August 21, 2017

Food and Drug Administration
Division of Dockets Management (HFA-305)
5630 Fishers Lane, Rm. 1061
Rockville, MD 20852

RE: Use of Electronic Records and Electronic Signatures in Clinical Investigations Under 21 CFR Part 11—Questions and Answer; Draft Guidance for Industry; Availability (Docket No. FDA-2017-D-1105

The Association of American Medical Colleges (AAMC) appreciates the opportunity to comment on the FDA's additional guidance on the use of electronic records and electronic signatures in clinical investigations of medical products. The AAMC is a not-for-profit association representing all 147 accredited U.S. medical schools, nearly 400 major teaching hospitals and health systems, and more than 80 academic and scientific societies. Through these institutions and organizations, the AAMC represents nearly 160,000 faculty members, 88,000 medical students, 124,000 resident physicians, and thousands of graduate students and postdoctoral trainees in the biomedical sciences.

The AAMC is pleased with the FDA's decision to release additional guidance on the use of electronic records and signatures in clinical investigations and agrees that the use and capabilities of electronic systems have expanded significantly since the Agency issued the 2003 *Guidance for Industry, Part 11, Electronic Records; Electronic Signatures—Scope and Application.* We support the FDA's commitment to engage key stakeholders in the development of new processes and frameworks to ensure the quality and reliability of electronic records and electronic signatures and encourage the FDA to continue seek public feedback as electronic systems and technologies develop. We offer these comments and suggestions for this and future guidance documents.

1) **Electronic Systems Owned or Managed by Sponsors and Other Regulated Entities Inspected by FDA (Q. 2)**

   As noted in the draft guidance, the FDA conducts inspections of electronic systems that fall under the scope of 21 CFR part 11, focusing primarily on implementation of the electronic system and validation of system functionality after implementation. During inspection, the FDA ensures that checks are in place for the reformatting and transfer of "source data" and that the value or meaning of "critical data" have not been altered during the migration process. Further, for each clinical investigation, FDA recommends that sponsors and other regulated entities develop prospective monitoring activities to uphold trial integrity by preventing error in the collection and reporting of

critical data and processes. Citing section IV.A (Identify Critical Data and Processes to be Monitored) of the 2013 *Guidance for Industry, Oversight of Clinical Investigations—A Risk-Based Approach to Monitoring*, the draft guidance provides several examples of critical data that sponsors and other regulated entities *may* use during the review process, identifying the documentation of informed consent as one example. **Recognizing the importance of informed consent, the FDA could suggest that sponsors and other regulated entities make reasonable efforts to verify whether the obtaining of informed consent was properly documented each time a monitoring review is conducted. Routine monitoring of practices around informed consent better ensures the protection of trial participants and integrity of the study conduct.** This is particularly important in light of the quickly-changing research environment which includes novel methods for data collection and data transfer (e.g., wearable biosensors, mobile devices, and telecommunication systems).

The AAMC also appreciates that the FDA will focus its inspections on the exchange of source data between electronic systems to ensure checks are in place. In our response to the Agency's July 2016 draft guidance for industry on the *Use of Electronic Health Record Data in Clinical Investigations*, AAMC supported the development of frameworks and processes to increase the use of electronic health record (EHR) data in clinical investigations and agreed with the FDA that "[…] the interoperability of data systems, such as an Electronic Data Capture (EDC) system, can benefit the clinical investigation, patients, and other healthcare providers." As discussed in this draft document, data transferred between multiple electronic systems or trial sites require sponsors or other regulated entities to develop specific mechanisms or processes to ensure its protection **We further recommend that additional guidance on how to manage and protect data transferred across multiple sites may be needed in addition to clarify the respective roles of sponsors, clinical investigators, and clinical trial personnel.**[1]

2) FDA's Expectations Regarding the Use of Internal and External Security Safeguards (Q.4)

The AAMC supports FDA's expectation that sponsors and other regulated entities implement specific procedures and safeguards to protect the "authenticity, integrity, and, when appropriate, the confidentiality of electronic records […]." **Given the speed at which technology is advancing, we encourage consistent stakeholder engagement to identify ways sponsors and other regulated entities can better utilize access controls and safeguards to prevent potentially harmful impacts on electronic systems and data.** Failure to appropriately guard against external threats such as computer viruses or worms, threatens the integrity of the study, poses risks to research subjects, and jeopardizes public trust in biomedical research.

3) Use and Retention of Electronic Copies of Source Documents in Place of the Original Paper Source Documents (Q. 6)

If a sponsor or other regulated entity intends to destroy the paper source data and use an electronic copy in its place, the FDA recommends that sponsors or other regulated entities certify that the electronic copy accurately represents the original paper document and verify that the copy contains the same attributes and information as the original document. The draft guidance references part 11

[1] AAMC Comment Letter, July 18, 2016 (available at https://www.aamc.org/download/463634/data/aamccommentletterontheuseofehrdatainclinicalinvestigations.pdf).

(sect. 10 and 30) which outlines procedures and controls for closed and open systems. **In addition to those recommended procedures and controls referenced in the draft guidance and part 11, FDA could recommend that sponsors and other regulated entities employ appropriate safeguards to detect, prevent, and mitigate the potential risks associated with software updates or software changes to ensure that the electronic system's supported software has the capability to store and retrieve electronic documents without jeopardizing the context, content, or structure of the data.**

4) **Implementation of Access Controls for Mobile Technology Accessed by Study Participants for use In Clinical Investigations (Q. 17)**

The AAMC agrees that when mobile technology is used to capture, record, or transmit data from study participants, sponsors and other regulated entities should implement basic user access controls (e.g., ID codes, usernames, electric thumbprints) to ensure that the data entries originate from the intended study participant. **For clinical investigations that allow for remote data to be captured from a study participant's mobile application, the FDA should consider recommending that sponsors and other regulated entities address potential barriers to effective access controls that result from deficiencies in reading comprehension or lack of familiarity with or access to mobile technology.** The use of an electronic format such as graphics or videos in addition to interactive questions may allow for trial participants to demonstrate their understanding of the purpose of the clinical investigation and how specific access controls will be used to protect their private information throughout the study.

The FDA also recommends that when access controls are impractical or difficult to implement, sponsors should consider obtaining a signed declaration from the study participant indicating that the device will solely be used by the participant. **We recommend that sponsors and other regulated entities also clearly communicate the purpose of the declaration in the context of the clinical investigation. Additionally, the participant should be informed about the reasonably foreseeable security and privacy risks that arise when a mobile device is also used by someone other than the intended study participant**.

5) **Mobile Technology and Source Data (Q. 19)**

As recognized by the FDA, source data collected from a study participant are "data that are first recorded in a permanent manner" which may temporarily pass through electronic hubs or gateways before reaching the sponsor's EDC system and may make it difficult to determine the location of the source data.

We agree that the first designated permanent recording of the source data collected from a participant's device is the data located in the sponsor's EDC or EHR system, and not the mobile technology used by the study participant. Thus, an individual's mobile device should not be subject to the inspection (e.g., audit) and validation that may be conducted by the FDA after the data are transmitted and stored in the sponsor's EDC system. Appropriate safeguards or controls should be implemented to ensure the integrity and reliability of the data collected from a participant's mobile device during transmission to the sponsor's electronic system, but the FDA's

inspection of those controls should be limited to the safeguards implemented by the sponsor, not the controls as used by each study participant.

6) **Implementation of Security Safeguards to Ensure Security and Confidentiality of Data When Mobile Technology is Used to Capture, Record, and Transmit Data from Study Participants (Q. 22)**

The AAMC supports the recommendation that data transmitted wirelessly to the sponsor's EDC system should be encrypted at rest and in transit to prevent access or malicious use by intervening parties. **When considering additional safeguards to ensure the confidentiality of data collected from mobile technology, the FDA could recommend that sponsors or other regulated entities implement protections to ensure the security of collateral data such as the participant's personal information (e.g., contacts, geographic location, web searches) that may be collected from the mobile device during the course of the clinical investigation, especially if a participant is using his/her personal device.**

As acknowledged in the draft guidance, the standards and capabilities of electronic systems have greatly improved and expanded to include the use of wearable biosensors and other portable electronic implantable devices to transmit participant data. **The FDA should continue to engage stakeholders to determine what additional security and confidentiality measures are sufficient to safeguard the data captured, transmitted, and recorded using new technologies.**

7) **Sponsor, Study Personnel, and Study Participant Training on the Use of Mobile Technology in a Clinical Investigation (Q. 23)**

The AAMC agrees with the FDA that clinical investigators, study personnel, and study participants should be adequately trained on the use of mobile technology used in clinical investigations. Investigators and study personnel should also conduct periodic reassessments and retrain study participants on systems that are complex or pose a higher risk to the conduct of the study. **We recommend that periodic assessments to determine the need for study participant retraining take place for all systems and technology used by study participants, and not solely on systems or technology that are more complex or pose a higher risk to the conduct of the study**.

The ability for study participants to interact with clinical investigators and study personnel during the course of the clinical investigation is equally paramount. Ensuring opportunities for participant interaction allows for the ongoing exchange of information between the study participant and investigator and creates opportunities for the investigator to answer questions or address concerns that may arise during the course of the clinical investigation.

8) **Methods Used to Create Valid Electronic Signatures (Q. 24)**

As noted in the draft guidance, the FDA does not mandate or identify a specific method or biometric upon which an electronic signature must be based. However, when electronic documents are signed, the FDA requires that electronic signatures must be accompanied by a computer-generated, time stamped audit trail and investigators should ensure that participants understand the legal significance

of the signature. **We encourage the FDA to engage a diverse cross section of the research community to identify the most appropriate and effective format for a participant's comprehension of the legal significance of their digital signature. We note that this document does not reference the possibility that an electronic signature may come from a participant's legally authorized representative and not from the participant himself or herself. The FDA should consider providing additional guidance in this document to address the situation when consent for participation in a clinical study that uses mobile technology is provided by an individual who is the legally authorized representative for the study participant.**

The AAMC appreciates the opportunity to comment on this topic and would be happy to provide additional information on any of the issues discussed in our letter. If you have any questions regarding our comments, please feel free to contact Heather Pierce, Senior Director for Science Policy and Regulatory Counsel at hpierce@aamc.org or (202) 478-9926.

Sincerely,

Ross McKinney, MD
Chief Scientific Officer