August 21, 2017
Division of Dockets Management (HFA-305)
Food and Drug Administration
5630 Fishers Lane, Rm 1061
Rockville, Maryland 20852
via electronic submission

Attention: **Docket Number: FDA-2017-D-1105**

Subject: FDA draft guidance **Use of Electronic Records and Electronic Signatures in Clinical Investigations Under 21 CFR Part 11 – Questions and Answers**

Dear Sir or Madam:

ISPE (the International Society for Pharmaceutical Engineering) would like to submit comments for the FDA draft guidance Use of Electronic Records and Electronic Signatures in Clinical Investigations Under 21 CFR Part 11 – Questions and Answers. The draft was reviewed by ISPE's technical sub-committee known as the Good Automated Manufacturing Practice (GAMP®) Community of Practice, which is comprised of individuals from pharmaceutical companies, suppliers, and consultants.

Overall, the ISPE members found the draft guidance to be a useful document and applaud FDA's effort to update recommendations for applying and implementing part 11 requirements in the current environment of electronic systems. We offer these general observations for your consideration:

- The document addresses the changing technological environment used in the provision of medical care, mobile technology, and telecommunication systems, with the possible exception of the concept where the sponsor's EDC system is a sort of platform where all clinical data are finally generated and/or transferred. This is a simplified logical construct of many collaborative processes, which eliminate the sponsor's sole control on the clinical data and shifts the responsibilities to the clinical investigators. This does not represent the current industry environment and changing it to match the FDA's concept of the sponsor's EDC system depicted in the guidance would require a significant re-engineering of most existing computerized systems. Therefore, we would like to encourage the Agency to carefully consider and provide additional clarity.
- The guidance does not address the scenario of having a technology service provider database as part of the data flow (ref FDA Guidance "Electronic Source Data in Clinical Investigations"), leading to conflicting interpretation of full control by the sponsor. In this scenario, the sponsor does not have full control of the data until it is transferred to their EDC system without addressing the expectation of the clinical investigators' control over the clinical data.

  The guidance should provide directions on how to meet the fundamental expectations that 1) the sponsor does not have exclusive control until the data is in their EDC, and 2) the clinical investigator must appropriately control the data prior to that transfer since they typically have continuous access to the data. The current language seems to allow the direct transfer of mobile

data to the sponsor's EDC system without mentioning how clinical investigators should be ensuring proper controls over that data.

These and other specific comments are included in the following pages. We appreciate the opportunity to submit these comments for your consideration.

ISPE is a not-for-profit organization of individual members leading scientific, technical and regulatory advancement throughout the entire pharmaceutical lifecycle. The 18,000 members of ISPE are building solutions in the development and manufacture of safe and effective pharmaceutical and biologic medicines and medical delivery devices in more than 90 countries around the world. ISPE does not take political positions or engage in lobbying activities or legislative agendas.

Please do not hesitate to contact me if you have any questions.

Sincerely,

John E. Bournas
ISPE CEO and President.

Proposed Regulation/Guidance Document:

FDA Draft Guidance for Industry: "Use of Electronic Records and Electronic Signatures in Clinical Investigations under 21 CFR Part 11-- Questions and Answers."

Comments from: ISPE (International Society for Pharmaceutical Engineering)

GENERAL COMMENTS ON THE DOCUMENT
Overall a useful document. It addresses the changing technological environment used in the provision of medical care, mobile technology, and telecommunication systems, with the possible exception of the concept where the sponsor's EDC system is a sort of platform where all clinical data are finally generated and/or transferred. This is actually a simplified logical construct of many collaborative processes, which eliminate the sponsor's sole control on the clinical data and shifts the responsibilities to the clinical investigators. This does not represent the current industry environment and changing it to match the FDA's concept of the sponsor's EDC system depicted in the guidance would require a significant re-engineering of most existing computerized systems. Therefore, we would like to encourage the Agency to carefully consider and provide additional clarity.
The guidance does not address the scenario of having a technology service provider database as part of the data flow (ref FDA Guidance "Electronic Source Data in Clinical Investigations"), leading to conflicting interpretation of full control by the sponsor. In this scenario, the sponsor does not have full control of the data until it is transferred to their EDC system without addressing the expectation of the clinical investigators' control over the clinical data. The guidance should provide directions on how to meet the fundamental expectations that 1) the sponsor does not have exclusive control until the data is in their EDC, and 2) the clinical investigator must appropriately control the data prior to that transfer since they typically have continuous access to the data. The current language seems to allow the direct transfer of mobile data to the sponsor's EDC system without mentioning how clinical investigators should be ensuring proper controls over that data.

Specific Comments on the Text

ISPE indicates text proposed for deletion with ~~strikethrough~~ and text proposed for addition with **bold and underlining**.

Line Number	Current Text	Proposed Change	Rationale or Comment
113-114	Records required for clinical investigations of medical products that are maintained in electronic format in place of paper format, including all records that are necessary for FDA to reconstruct a study	…all records required by the predicate rule as discussed herein	The last phrase has unlimited scope
139	For electronic systems that fall under the scope of part 11 regulations, the regulations distinguish the systems as closed or open (see §§ 11.10 and 11.30, respectively).[13] This distinction is seldom relevant because of the pervasive use of the internet and web-based systems.	For electronic systems that fall under the scope of part 11 regulations, the regulations distinguish the systems as closed or open (see §§ 11.10 and 11.30, respectively).[13] This distinction is seldom relevant**, and no longer typically applied by the Agency or wider industry.** ~~**, partly** because of the pervasive use of the internet and web-based systems.~~ If access to electronic systems through use of the internet (for example) is permitted, if may be prudent, based on risk, to implement additional security measures for such systems above and beyond those controls for closed systems described in § 11.10, such as document encryption and the use of appropriate electronic signature standards to ensure the authenticity, integrity, and confidentiality of records (see § 11.30).	The Open /closed distinction is not helpful, and is seldom or not typically used by either Agency or industry. An appropriate justified and documented risk-based approach to selection and application of controls will lead to appropriate security and integrity without the need for the distinction. Suggest clearly stating that the distinction is no longer actively applied by industry or Agency. The definition of closed vs. open systems states that the difference is related to whether system access is controlled by persons responsible for the content, which is generally controlled primarily by logical security controls, so the relationship to the restriction of physical access is not clear. Also, the relationship of encryption and electronic signature to system access controls is not clear. It may be helpful to simply follow the direction of the text of the Part 11 regulation in suggesting that (without

Line Number	Current Text	Proposed Change	Rationale or Comment
			applying the open/closed distinction) additional measures such as encryption and digital signature standards should be considered, based on risk and as necessary under the circumstances, to ensure record authenticity, integrity, and confidentiality.
155-162	Examples of electronic systems used in clinical investigations that are owned or managed by sponsors and other regulated entities (e.g., CROs, IRBs) include electronic case report forms (eCRFs); electronic data capture (EDC) systems, electronic trial master files (eTMFs), electronic Clinical Data Management System (eCDMS), electronic Clinical Trial Management System (eCTMS), Interactive Voice Response System (IVRS), Interactive Web Response System (IWRS), centralized, web-based electronic patient-reported outcomes (ePRO) portals, and electronic IRB human subject application systems (eIRBs). Requirements and recommendations for these systems are described in this section.	Examples of electronic systems used in clinical investigations that are owned or managed by sponsors and other regulated entities (e.g., CROs, IRBs) include electronic case report forms (eCRFs); electronic data capture (EDC) systems, electronic trial master files (eTMFs), **mobile applications (e.g. ……),** electronic Clinical Data Management System (eCDMS), electronic Clinical Trial Management System (eCTMS), Interactive Voice Response System (IVRS), Interactive Web Response System (IWRS), centralized, web-based electronic patient-reported outcomes (ePRO) portals, and electronic IRB human subject application systems (eIRBs). **In some cases, the sponsor relies on Information Technology (IT) suppliers, which are generally not regulated entities, to provide software and/or data hosting services. In these instances, the sponsor is accountable for assuring that applicable regulatory requirements are met.** Requirements and recommendations for these systems are described in this section.	Please clarify and differentiate between software or data hosting providers that are performing activities on behalf of the sponsor vs. CROs and which entities are considered to be regulated. Also, the guidance covers mobile apps but there are no examples to refer to.
189	For COTS office utilities software in general use, such as word processing, spreadsheets,	For COTS office utilities software in general use, such as word processing,	The suggestion that office utilities such as word processors may potentially require

Line Number	Current Text	Proposed Change	Rationale or Comment
	and portable document format (PDF) tools or for electronic systems that process non critical procedural records, the extent of validation should be guided by the organization's internal business practices and needs.	spreadsheets, and portable document format (PDF) tools or for electronic systems that process non critical procedural records, the extent of ~~validation~~ **control and/or any required qualification** should be guided by the organization's internal business practices and needs.	validation is unhelpful and may be misleading. Previous and subsequent paragraphs in the Draft Guide outline the need to validate electronic systems (applications) for their intended use, and it is suggested that the term validation is best reserved for such activities. This is in line with GAMP and PIC/S Annex 11 usage and terminology (i.e. Validation of GxP applications, and qualification of IT Infrastructure. Office utilities would be considered as part of the infrastructure.
194 - 207	For COTS systems that perform functions beyond office utilities, such as COTS EDC systems, validation should include a description of standard operating procedures and documentation from the vendor that includes, but is not limited to, results of their testing and validation to establish that the electronic system functions in the manner intended. For COTS systems that are integrated with other systems or for customized systems that are developed to meet a unique business need of a user, sponsors and other regulated entities should develop and document a validation plan, conduct the validation in accordance with the plan, and document the validation results. Such documentation may be reviewed and copied during an FDA inspection. Validation for these systems may	For COTS systems that perform functions beyond office utilities, such as COTS EDC systems, ~~validation should include a description of standard operating procedures and documentation from the vendor that includes~~**, the sponsor is responsible for assessing the vendor's software development practices and relevant standard operating procedures** ~~but is not limited to, results of their testing and validation to establish~~ **to assure** that the electronic system functions in the manner intended. For COTS systems that are integrated with other systems or ~~for~~ customized ~~systems that are developed~~ to meet a unique business need of a user **(e.g., execution of specific clinical studies), sponsors and other regulated entities are responsible for validating the integration and**	For COTS systems, the sponsor is responsible for evaluating the validation conducted by the COTS software vendor as well as their operating procedures to ensure that the system is validated for their intended use and that the vendor has procedures in place to support a regulated system. When COTS systems (e.g. EDC) are customized for specific clinical studies, is this section expressing that additional validation by the sponsor is required? If so, recommend using this as an example for clarity.

Line Number	Current Text	Proposed Change	Rationale or Comment
	include, but is not limited to, user acceptance testing, dynamic testing, and stress testing. Sponsors and other regulated entities should perform the validation before the use of these systems, in addition to initial testing of the electronic system, to ensure that the system functions in the manner intended.	**customization based on their intended use.** Sponsors and other regulated entities should develop and document a validation plan, conduct the validation in accordance with the plan, and document the validation results. Such documentation may be reviewed and copied during an FDA inspection. Validation for these systems may include, but is not limited to, user acceptance testing, dynamic testing, and stress testing. **All validation activities outlined in the validation plan (e.g., requirements, testing) should be completed before using the system.** ~~Sponsors and other regulated entities should perform the validation before the use of these systems, in addition to initial testing of the electronic system, to ensure that the system functions in the manner intended.~~	
204	dynamic testing, and stress testing.	Provide definition of these testing	These are not common terms in the clinical area. Either in the body of the guidance or in the glossary, a concise operational definition would ensure common understanding of the expectations. For example: *Stress Testing (ISO 24765) - Testing conducted to evaluate a system or component at or beyond the limits of its specified requirements.*

Line Number	Current Text	Proposed Change	Rationale or Comment
			Dynamic testing (Derived from FDA Glossary of Computer System Software Development Terminology) – testing that is performed by executing the program code.]
209-221	Recommend using the term regression analysis and regression testing instead of re-validation (reference *General Principles of Software Validation)*	**When changes are made to the electronic system (e.g., system and software upgrades, including security and performance patches, equipment or component replacement, or new instrumentation), sponsors and other regulated entities should perform regression analysis and testing using a risk-based approach in addition to testing the specific changes to re-establish the validated state of the system.** **The extent of validation and testing should be based on the level of risk.**	Suggested terminology is aligned with FDA *General Principles of Software Validation* and better aligned with general industry usage. Also, one current sentence implies that there is a specific document with the title risk assessment, while for changes the impact evaluation considers also risks associated with the change.
234	FDA will also review standard operating procedures and support mechanisms in place, such as training, technical support, and auditing to ensure that the system functioning and is being used in the manner intended.	add footnote after auditing FDA review of auditing will be consistent with FDA's Compliance Policy Guide to no normally review internal audits except in specific for cause instances	As stated in FDA's CPG to be sure audits are as thorough and frank as possible. This does not preclude verifying there is an audit system procedure in place and verification audits have been performed.
383	N/A	N/A	Although 11.10 (b) defines 'The ability to generate accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency', the scope and application mentions that FDA intends to exercise enforcement discretion

Line Number	Current Text	Proposed Change	Rationale or Comment
			with regard to part 11 requirements for validation, audit trails, record retention, and record copying. Please address if FDA intends to exercise enforcement discretion for coping records?
391	Secure, computer-generated, time-stamped audit trails of users' actions and changes to data	Secure, computer-generated, time-stamped **data** audit trails of ~~users' actions and changes to data user~~ **user entries and actions that delete or modify records**	To bring in line with usage in the Part 11 regulation, and also the definition of Audit Trail in Appendix II: Glossary of Terms. To clarify that not all user actions are typically or required to be recorded in a data audit trail, only those actions related to data changes.
454	What should sponsors and other regulated entities consider when deciding to validate outsourced electronic services that are used in clinical investigations?	N/A	It would be helpful to clarify FDAs expectations on Change Management on outsourced services like cloud or Single-Instance Multitenant (SIMT) systems are. As these systems are often updated without the explicit approval by the sponsor by the technology providers, it is difficult for Sponsors and CROs to meet the expectations as laid out.
517	In cases where access controls are impractical, sponsors should consider obtaining a signed declaration from the study participant confirming that the device will only be used by the study participant.	Either removal or refer to the informed consent being signed the study participants. In cases where access controls are impractical, sponsors should **consider adding in the informed consent to be signed by study participant , a statement confirming** that the device will only be used by the study participant.	It is highly recommended to not introduce such declaration since it is not required for many other activities performed by the study participants (e.g. as paper diaries) and it is not required by Good Clinical Practices. The informed consent and the instructions for the proper use of the instrument/tool etc. might be used in lieu of an additional

Line Number	Current Text	Proposed Change	Rationale or Comment
			document that will add unnecessary complexity.
536	the study participant should be identified as the data originator	the study participant should be identified as the data originator **using unique identifiers that will protect the confidentiality and privacy rights of the study participant**, as appropriate	Add clarification to ensure confidentiality and privacy expectations are met.
571	FDA considers source data as data that are first recorded in a permanent manner.	Recommend deleting this sentence and retaining the remaining content to state the agency's position on mobile technology records – lines 572 – 578.	This sentence does not align with expectations and statements regarding what is considered source data, including the definition within this guidance (i.e. all information in original records and certified copies of original records of clinical findings, observations, or other activities (in a clinical investigation) used for the reconstruction and evaluation of the trial). This could lead to confusion regarding interpretation of what is considered source data with respect to other records.
590	In addition, the date and time that the measurement was made should be recorded and available to FDA at the time of inspection if it differs from the date and time the data enter the EDC system.	In addition, the date and time that the measurement was made and **the date and time of the transfer being made** should be recorded and available to FDA……	The audit trail of the sponsor's EDC system will provide the exact date and time of when the data arrived/populated the sponsor's EDC system. However, for full traceability, there are 3 sets of date/time to be made available: - When the measurement was made - When the measurement was transferred

Line Number	Current Text	Proposed Change	Rationale or Comment
			- When the measurement was acquired in the sponsor's EDC system
593-597	In cases where the study participant actively participates in the performance measure and manually enters the data into the mobile platform (e.g., tablet computers, smart phones) or other portable device, the mobile technology should be designed to prevent unauthorized modifications to the data before those data are transmitted to the sponsor's EDC system.	In cases where the study participant actively participates in the performance measure and manually enters the data into ~~the~~ **a** mobile platform (e.g., tablet computers, smart phones) or other portable device **provided by the sponsor**, the mobile technology should be designed to prevent unauthorized modifications to the data before those data are transmitted to the sponsor's EDC system.	Differentiate the expected controls for sponsor provided devices (e.g., phone or tablet) vs. BYOD where the device belongs to the study participant. In the BYOD case, the sponsor has minimal control over the design of the device. In addition to the access controls in Q17, please provide examples of expected controls on the mobile device that would prevent unauthorized modifications to the data before transmission to the EDC system (e.g., an application time-out). In line 596, there is emphasis on preventing unauthorized modifications **before** data is transmitted to the sponsor's EDC system. We would like to request clarification why the Agency is taking such a position since normally modifications using the mobile technology are not allowed after the data are transmitted vs. emphasizing only before the data are transmitted.
605-606	N/A	N/A	When study participants are asked to sign a handwritten signature using a smart device, we concur that such a signature would be regarded as equivalent to a wet-ink signature We believe that it may be determined from Part 11 and the associated Preamble that handwritten signatures captured by a

Line Number	Current Text	Proposed Change	Rationale or Comment
			device, where the act of signing with a writing or marking instrument such as a pen or stylus is preserved are regarded as handwritten signatures, and not electronic signatures.
637	the data must be encrypted at rest and in transit to prevent access	the data must be encrypted at rest **(e.g. ……..)** and in transit **(e.g……)** to prevent access	In order to clarify the expectations, it is recommended to define what are those types of encryptions, either by adding examples or operational definition in the glossary of the guidance.
640-654	On the other hand, additional controls may be important when using mobile apps and mobile platforms. In addition to having encryption and basic user access controls in place (see 644 section IV.D.Q17), sponsors should consider implementing additional security safeguards as follows: Remote wiping and remote disabling • Remote wiping and remote disabling • Disable function for installing and using file-sharing applications • Firewalls • Procedures and processes to delete all stored health information before discarding or reusing the mobile device	On the other hand, additional controls may be important when using mobile apps and mobile platforms. In addition to having encryption and basic user access controls in place (see 644 section IV.D.Q17), **for sponsor provided mobile devices,** sponsors should consider implementing additional security safeguards as follows: Remote wiping and remote disabling • Remote wiping and remote disabling • ~~Disable function for installing and using file-sharing applications~~ • ~~Firewalls~~ • Procedures and processes to delete all stored health information before discarding or reusing the mobile device	Unclear what the following requirements mean relative to mobile devices: • Disable function for installing and using file-sharing applications • Firewalls For example, firewalls are not applicable to mobile devices and not aware of a way to disable installing a particular type of application on a mobile device.
662-664	Training should occur before the use of the mobile technology and whenever changes are made (e.g., software or system upgrades) to	Training should occur before the use of the mobile technology and whenever changes **to the initial functionalities** are made (e.g., software or system upgrades,	There are changes that would not require training or re-training.

Line Number	Current Text	Proposed Change	Rationale or Comment
	the mobile technology during the course of the clinical investigation.	**according to impact evaluation)** to the mobile technology during the course of the clinical investigation.	
665-667	In addition, clinical investigators and study personnel should periodically reassess and retrain study participants, as necessary, on systems that are more complex or that pose a higher risk to the conduct of the study	In addition, clinical investigators and study personnel should ~~periodically~~ reassess and retrain study participants, as necessary, on systems that are more complex or that pose a higher risk to the conduct of the study	This is not an activity done periodically, but only is necessary in front of signals like compliance, quality of the data etc.
746	Q26. When an individual executes a series of signings during a single, continuous period of controlled system access, could the initial logging into an electronic system using a unique username and password be used to perform the first signing and satisfy the requirements found in 21 CFR 11.200(a)?	Q26. When an individual executes a series of signings during a single, continuous period of controlled system access, could the initial logging into an electronic system using a unique username and password be ~~used to perform the first signing~~ **regarded as equivalent of using all signature component,** and satisfy the requirements found in 21 CFR 11.200(a), **such that subsequent signatures during the same controlled session can be executed using only the private component?**	The intention of the Question and Answer (751-771) is clear, and welcomed, but the current wording in the Question suggests that the initial login is actually a first signature event. It is essential and extremely helpful to maintain a distinction between various events, e.g. a login on to a system (which is a security and privilege management aspect), vs. a signature event (i.e. application of a signature required by a predicate rule). The current FDA Part 11 Scope and Application Guidance very usefully makes the Narrow Scope distinction between signature events proper, and other uses of components such as user-ids and passwords in other contexts., such as logins, acknowledgements, or identification of individuals. It is important for regulated entities to clearly distinguish between signature events and other events, in order to ensure that Electronic signatures required for

Line Number	Current Text	Proposed Change	Rationale or Comment
			clinical investigations are truly regarded as the equivalent of handwritten signatures, initials, and other general signings. Absent this clarity, the accuracy, integrity, and non-repudiation of signatures and records are at risk.
Appendix II - Glossary	Certified copy	Add "…by a dated signature **or by generation through a validated process**……"	Align this definition with other harmonized guidance documents – e.g. ICH E6 R2
Appendix II - Glossary	Critical Data	The current definition provides examples only. Recommend providing the criteria to be considered when determining if data are critical. Are these criteria the same as found in other guidance documents related to data integrity (e.g. WHO, MHRA, PIC/S, EMA Q&A, FDA Q&A)?	The criteria will provide clearer expectations in determining which data is critical.
845 - 846	Audit Trail is a process that captures details of information, such as additions, deletions, or alterations, in an electronic record without obscuring the original record.	N/A	In "Data Integrity and Compliance With CGMP Guidance for Industry", audit trail is defined as an "electronic record". Here it is defined as "process", which is helpful as it provides more flexibility in implementation. Consider aligning the CGMP Guidance for Industry with this document (or alternatively aligning all guidance with the Part 11 regulation)