AHIMA
American Health Information
Management Association®

233 N. Michigan Ave.,21st Fl.
Chicago, IL 60601-5800

phone » (312) 233-1100
fax » (312) 233-1090
web » www.ahima.org

August 21, 2017

Dr. Scott Gottlieb
Commissioner
Food and Drug Administration
10903 New Hampshire Avenue
Silver Spring, MD 20993

Docket No. FDA-2017-D-1105, Use of Electronic Records and Electronic Signatures in Clinical Investigations Under 21 CFR Part 11—Questions and Answers; Draft Guidance

Submitted via www.regulations.gov

Dear Commissioner Gottlieb:

Thank you for the opportunity to submit comments on the Use of Electronic Records and Electronic Signatures in Clinical Investigations under 21 CFR Part 11 draft guidance.

AHIMA is the national non-profit association of health information management (HIM) professionals. Serving 52 affiliated component state associations including the District of Columbia and Puerto Rico, AHIMA represents over 103,000 health information management professionals dedicated to effective health information management, information governance, and applied informatics. AHIMA's credentialed and certified HIM members can be found in more than 40 different employer settings in 120 different job functions—consistently ensuring that health information is accurate, timely, complete, and available to patients and providers. AHIMA provides leadership through education and workforce development, as well as thought leadership in continuing HIM research and applied management for health information analytics.

Although the draft guidance covers a number of topics, we offer general comments on the draft guidance, followed by more specific comments below.

Risk-Based Approach

AHIMA supports the FDA's intent under the draft guidance to expand its risk-based approach described in its 2003 21 CFR part 11 guidance to validation, audit trails and archiving of records. We believe that a risk-based approach is the most appropriate method to ensuring the quality, authenticity, and reliability of electronic records and electronic signatures throughout their lifecycle while ensuring that sponsors, clinical investigators, institutional review boards, contract research organizations, and other interested parties are not unduly burdened in complying with 21 CFR part 11.

Information Governance

As stewards of health information, AHIMA believes that information governance—an organizational framework for managing information throughout its lifecycle which supports an organization's strategy, operations, regulatory, legal and risk requirements—can play an important role in developing processes and procedures that assure compliance with 21 CFR part 11 while improving the overall quality, integrity, and trustworthiness of the data held in the electronic record and/or system.

AHIMA has developed an Information Governance Adoption Model (IGAM™) that assesses and scores a health organization using 10 information governance organizational competencies. Each competency includes several maturity markers that identify critical requirements that must be met to optimize maturity in information governance that ensures the trustworthiness of a healthcare organization's information. A detailed description of AHIMA's IGAM™ competencies may be found in **Appendix A**. We welcome the opportunity to share our information governance expertise with the FDA and demonstrate how AHIMA's information governance framework could assist stakeholders in meeting the FDA's guidance concerning 21 CFR part 11.

Audit Trails

AHIMA believes that the use of audit trails under 21 CFR part 11 can play an important role in ensuring the reliability, authenticity, and quality of electronic records during their lifecycle. However, a number of our members have expressed concern that some vendors' audit trails lack the functionality required to comply with 21 CFR part 11. For example, a number of our members have noted that while their vendor's audit trail may indicate when data has been deleted and/or added, it may or may not indicate whether such information has been edited. The audit trail also may not indicate whether the information has been copied and pasted into the system. As one member noted, "you may know an event took place but not the details of the event." We recommend that the FDA consider recommending as part of this guidance the use of government and industry standards. A list of recommended standards may be found in **Appendix B**. These standards could play a critical role in ensuring that vendors can provide the audit trail functionality required to comply with 21 CFR part 11.

FDA Inspection of Electronic Systems

AHIMA supports the FDA's intention under the draft guidance to focus on source data transferred to another data format or system to ensure that checks are in place and that critical data are not altered in value or meaning during the migration process. However, our members are concerned as to how the FDA would know whether critical data has been altered in value or meaning during the migration process, particularly when the audit trail begins when the data is transmitted to the EDC. We request that further guidance be provided as to how the FDA would determine or what aspects the FDA would consider in determining whether critical data had been altered during the migration process as to ensure that the appropriate materials and systems are documented and/or archived for FDA inspection.

Electronic Copy of Source Documents in Place of Paper Source Data

AHIMA supports the FDA's statement in the draft guidance that the electronic copy of source documents should be an accurate representation and contain the same attributes and information as the original paper record. However, often there are instances where in the conversion of original paper records to electronic copies, an HIM department (which is often charged with validating the record) may not see the original paper source data prior to it being converted into an electronic copy. For example, clinic staff may convert the record into electronic format or any and all of the original record may be given to the patient. In such instances, it is difficult for an HIM department to verify that the electronic copy has all the same attributes and information as the original record. Having documented policies and procedures in place concerning how documents are incorporated into the record are critically important to ensure that the electronic copy of the record retains the same attributes and information as the original paper source data. This is particularly true in certain facilities where critical data, such as informed consent documentation, does not move to a central location like an HIM department for validation. We recommend that the FDA consider providing additional guidance as to what appropriate processes and procedures should be in place in such instances as to ensure the integrity of the record.

Mobile Technology

Again, we appreciate the FDA's risk-based approach with respect to the access controls around mobile technologies under 21 CFR part 11. For mobile apps that rely on a study participant's data entry, we suggest that the FDA consider recommending that sponsors utilize government and industry standards when applying access controls to ensure the standardization of such controls. In particular, the FDA may want to review the standards found in **Appendix B**.

Electronic Signatures

AHIMA supports the FDA's intention under the draft guidance to not mandate or specify a particular method for electronic signatures, including biometric methods that may be relied upon as a form of electronic signature. We support the recommendation in the draft guidance that suggests when biometric methods are utilized as a form of electronic signature, the biometric method be performed using government and industry standards. As the ANSI-appointed Secretariat to the ISO/Technical Committee 215 on Health Informatics (ISO/TC215), and as Administrator of the United States Technical Advisory Group (US TAG), the delegation representing the US to ISO/TC215, AHIMA appreciates that the FDA has included entities such as the ISO/IEC Joint Technical Committee 1/Subcommittee 37 and the American National Standards Institute as standards development organizations (SDOs) that develop biometric standards that sponsors could utilize. We believe that such standards will help ensure the administration and execution of biometric methods while helping to preserve the confidentiality of the electronic record.

Along these lines, for electronic signatures obtained via a non-biometric method, we recommend that the FDA suggest in its guidance that they also should be performed using government and industry standards. We believe the "IHE ITI Technical Framework Supplement – Document Digital Signature" could minimize the risk of fraudulent use and safeguard the identity of the individual.

We thank you for the opportunity to submit comments on the Use of Electronic Records and Electronic Signatures in Clinical Investigations under 21 CFR Part 11 draft guidance. Should you or your staff have questions or concerns, please contact Lauren Riplinger, Senior Director, Federal Relations, at lauren.riplinger@ahima.org or at (202) 839-1218.

Sincerely,

Pamela L Lane

Pamela L. Lane, MS, RHIA
Interim Chief Executive Officer

Appendix A:

AHIMA's Information Governance Adoption Model (IGAM™)

AHIMA created the Information Governance Adoption Model (IGAM™) which is the healthcare industry standard for measuring the maturity of an organization's information governance program. The model assesses and scores a healthcare organization using 10 IG organizational competencies. Each competency includes several key maturity markers that identify critical requirements that must be met to optimize maturity in information governance.

AHIMA IGAM™ Competencies

Privacy and Security Safeguards IG Competency: The Privacy and Security Safeguards competency encompasses the processes, policies, and technologies necessary to protect data and information across the organization from breach, corruption, and loss. Protection also ensures information is kept private, confidential, and secret as required based on its classification.

Information Technology Governance (ITG) IG Competency: ITG is a sub-domain of information governance and is seen as essential for any organization employing information technology. Organizations in healthcare must have certainty that information technology (IT) serves as a vehicle to achieve organizational strategy, goals, and objectives. IT governance establishes a construct for aligning IT strategy with the strategy of the business, and a means of fostering success in achieving those strategies. In addition to this alignment, IT governance includes use of best practices in technology solution selection and deployment, ensuring and measuring the value/benefit created through IT investments, management of resources, mitigating risks, measuring the performance of the IT function, and ensuring stakeholder input is incorporated into IT strategy.

Enterprise Information Management (EIM) IG Competency: EIM, a sub-domain of information governance, includes the policies and processes for managing information across the organization, throughout all phases of its life including: creation/capture, processing, use, storing, preservation, and disposition. EIM also includes management of enterprise practices for information sharing with patients, clients, residents, and their representatives, release and exchange practices, patient portal, chain of custody, and long-term digital preservation. Enterprise information management incorporates identity management to ensure patients see their information as well as automation of patient request processing.

Strategic Alignment IG Competency: Strategic alignment of information governance (IG) with the organization's strategy demonstrates valuation of information as a strategic asset and communicates that IG is an organizational imperative. Strategic alignment supports an information-driven, decision-making culture and ensures its workforce at all levels has access to

the information they need to make good decisions in real time, and it supports the expectation that information is used appropriately and strategically.
Strategic alignment encourages organizations to assign ownership, assess current state, and create a go forward strategy to engage consumers in the continuum of care through a consumer centric enablement strategy.

Strategic alignment also includes a maturity marker specific to the healthcare ecosystem and an organization's ability to interact with health information exchange in support of continuity of care for at risk populations, accountable care, and population health.

Data Governance (DG) IG Competency: Data governance is the sub-domain of information governance that provides for the design and execution of data needs planning and data quality assurance in concert with the strategic information needs of the organization. Data governance includes data modeling, data mapping, data audit, data quality controls, data quality management, data architecture, and data dictionaries. DG collaborates with EIM in functional components essential to the enterprise plans for information organization and classification. Best practices for data governance are included in the model as well as coaching to move organizations along.

Regulatory and Legal IG Competency: This competency focuses not only on the organization's ability to respond to regulatory audits, e-discovery, mandatory reporting, and releases to patients upon requests, but also on compliance with information-related requirements of any/all regulatory and other bodies of authority.

Analytics IG Competency: The ability to use data and information to achieve its strategy, goals, and mission, or, in short, to realize the value of its information is critical to success with information governance. An organization's competence is essential to moving from data to intelligence to knowledge. Competency in data analytics is therefore seen as essential to mature information governance.

IG Structure: The IG structure competency defines and connects the organizational structure, programmatic structures, and supporting structures for information governance. It ties together the three core programmatic structures of Enterprise Information Management, IT Governance, and Data Governance.

Awareness and Adherence: This competency aims to ensure the IG program principles, processes, practices, and procedures are learned and understood by the workforce, consistent with respective roles. Guidance is provided on compliant behaviors with respect to information creation, use, handling, access, sharing, storage, retention, and disposition. Beyond awareness, this competency includes adherence to, or compliance with, required policies and practices. Formal documentation, training, and strategy are utilized to shift workforce behaviors.

IG Performance: This competency enables development of a methodology for measuring the performance and impact of an IG program. IG performance assessment and management is essential to ensuring its effectiveness, ongoing improvement, and alignment with the organization's strategy. Performance management includes addressing capability for mandatory business, regulatory reporting, reliability of information, and measures for each of the areas of IG organizational competence.

Appendix B:

AHIMA Suggested Standards for FDA Draft Guidance on Use of Electronic Records and Electronic Signatures in Clinical Trials

Data Provenance Standards:

1. HL7 CDA® Release 2 Implementation Guide Data Provenance, Release 1 - US Realm
2. ISO/TR 21548:2010(en) Health informatics — Security requirements for archiving of electronic health records — Guidelines

Electronic Signature

1. HL7 Implementation Guide for CDA® Release 2: Digital Signatures and Delegation of Rights, Release 1
2. ISO 17090-4:2014(en) Health informatics — Public key infrastructure — Part 4: Digital Signatures for healthcare documents
3. ISO/TS 14441:2013(en) Health informatics — Security and privacy requirements of EHR systems for use in conformity assessment
4. ISO 22600-3:2014(en) Health informatics — Privilege management and access control — Part 3: Implementations
5. ISO 13606-2:2008(en) Health informatics — Electronic health record communication — Part 2: Archetype interchange specification
6. ISO/TS 21547:2010(en) Health informatics — Security requirements for archiving of electronic health records — Principles
7. ISO/TR 21548:2010(en) Health informatics — Security requirements for archiving of electronic health records — Guidelines
8. NIST: Digital Signature Standard (DSS)
   URL: http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.186-4.pdf
9. IHE ITI Technical Framework Supplement Document Digital Signature, Trial Implementation
   URL: https://www.ihe.net/uploadedFiles/Documents/ITI/IHE_ITI_Suppl_DSG.pdf