UNIVERSITY OF CALIFORNIA

OFFICE OF THE GENERAL COUNSEL

Health Sciences Research Advisory: *Electronic Records and Signatures in Human Subjects Research*

May 2012

Q. May we create, maintain, and transmit electronic records in connection with clinical trials or other human subjects research? May we use electronic signatures in documents associated with clinical trials or other human subjects research? If so, what requirements apply?

A. Yes. Federal and state law both prescribe standards for use of electronic documents and signatures in research and other contexts. Compliance with these standards is mandatory if electronic documents and signatures are expected to be the sole means of addressing mandatory documentation requirements.

Background/Executive Summary

The Federal Electronic Signatures in Global and National Commerce Act ("eSIGN") and California's adoption of the Uniform Electronic Transactions Act ("UETA") were both intended to facilitate the use of electronic systems to document legal transactions and other activities. These laws were critical to the development of online shopping, banking, insurance, and other services.

Use of electronic tools to facilitate documentation of human subjects research activities and, in particular, informed consent, has not been widespread at academic and other research institutions. These tools, however, may be employed if appropriate precautions are taken to assure compliance with relevant regulatory standards.

This advisory describes the requirements for implementation of electronic systems and signatures in clinical trials and other human subjects research. The first sections address general requirements for informed consent and for creation and retention of records in electronic format. The last summarizes more detailed requirements applicable to FDA-regulated clinical investigations. In brief, all of these standards seek to assure that documents created, maintained, or transmitted electronically are attributable, legible, contemporaneous, original, and accurate. Some of these standards also focus on consumer (in this case, research participant) rights including opt-in and notification rights.

Use of Electronic Signatures to Document Informed Consent

The Federal Policy for the Protection of Human Subjects ("Common Rule") was first adopted in 1991 and therefore predates the advent of modern technologies that can facilitate electronic collection and documentation of informed consent. Thus, while the regulation addresses the substantive requirements for informed consent and requirements for documentation of consent, it is silent with regard to use of electronic signatures.[1] The Common Rule requires only that consent be documented by use of a written form approved by the IRB and signed by the subject or subject's legally authorized representative (e.g., parent or legal guardian); and that a copy be provided to the person signing the form. An Institutional Review Board overseeing the project may waive documentation requirements in limited circumstances not relevant here.

[1] California's Protection of Human Subjects in Medical Experimentation Act is also silent on this subject.

Substantively, nothing in the Common Rule prohibits use of electronic signatures, so long as a copy is given to the person signing the form. Indeed, the Office for Human Research Protections, which is responsible for implementation and enforcement of the Common Rule for research supported by the National Institutes of Health and other DHHS agencies, has issued guidance expressly acknowledging that electronic signatures may be used if: (1) legally valid in the jurisdiction where the research is to be conducted; and (2) the IRB has made the necessary determinations, such as whether the signature can be validated and whether the consent can be produced in hard copy for a subject who wishes to see it. OHRP's guidance is reproduced in full immediately below:

> Can an electronic signature be used to document consent or parental permission?
>
> Yes, under certain circumstances. First, the investigator and the IRB need to be aware of relevant laws pertaining to electronic signatures in the jurisdiction where the research is going to be conducted.
>
> Unless the IRB waives the requirement for the investigator to obtain a signed consent or permission form based on the HHS regulations at 45 CFR 46.117(c), a written consent or permission form, which may be an electronic version, must be given to and signed by the subjects or the subjects' legally authorized representatives or the parents of subjects who are children. Some form of the consent document must be made available to the subjects or the parents of subjects who are children in a format they can retain. **OHRP would allow electronic signature of the document if such signatures are legally valid within the jurisdiction where the research is to be conducted.**
>
> OHRP does not mandate a specific method of electronic signature. Rather, **OHRP permits IRBs to adopt such technologies for use as long as the IRB has considered applicable issues such as how the electronic signature is being created, if the signature can be shown to be legitimate, and if the consent or permission document can be produced in hard copy for review by the potential subject.** One method of allowable electronic signatures in some jurisdictions is the use of a secure system for electronic or digital signature that provides an encrypted identifiable "signature." If properly obtained, an electronic signature can be considered an "original" for the purposes of recordkeeping.

DHHS Office for Human Research Protections, Informed Consent FAQs (Reviewed January 2011). One may presume that the referenced IRB determination may be made with respect to any given system – or even to all electronic systems employed by the relevant research institution if they meet the relevant standards – rather than on a case-by-case basis for each individual research study.

We turn, then, to eSIGN and UETA for guidance. Under these laws, an electronic signature is valid if the subject agrees to utilize the electronic format (for example, by clicking an "I agree" icon) and a clear statement of the subject's rights with respect to the electronic document is provided. These rights include:

- The right to obtain electronic records in non-electronic form;
- The right to withdraw the subject's agreement to have the record provided or made available in an electronic form and of any conditions, consequences or fees in the event of such withdrawal;
- An explanation of whether the agreement applies only to the subject's consent to participate in the study or to other categories of records that may be provided and executed electronically;
- A description of any procedures that must be followed to withdraw the subject's agreement to use an electronic record;
- Information about how, after agreeing to an electronic record, a subject may, upon request, obtain a paper copy and whether any fee will be charged.

Regulations promulgated pursuant to Government Code Section 16.5 and issued by California's Secretary of State ("SOS") also describe technical requirements for use of electronic signatures by government entities including the University of California. These technology-specific regulations[2] are preempted by eSIGN, which requires that state laws be technologically neutral (*i.e.*, state laws may not "require, or accord greater legal status or effect to, the implementation or application of specific technology").[3] By providing legal status only to digital signatures that meet specific technology requirements, Section 16.5 and the regulations promulgated thereunder accord "greater legal status" to certain acceptable technologies. That "specific technology" requirement is, therefore, preempted.

Notably, if an electronic signature is intended to document a subject's authorization for use or disclosure of protected health information under HIPAA, that law's privacy and security rules will apply to the transaction. Unfortunately, DHHS has failed so far to issue a final rule on electronic signatures.[4] In another context, however, the DHHS Office for Civil Rights, which is charged with implementation and enforcement of HIPAA's privacy and security rules, has, like OHRP, advised that electronic signatures are permitted to document compliance with regulatory signature requirements if the signatures meet the requirements of applicable state law. More recently, the agency noted in connection with rulemaking efforts under the HITECH Act, that "the Privacy Rule allows for electronic documents to qualify as written documents for purposes of meeting the Rule's requirements, as well as electronic signatures to satisfy any requirements for a signature, to the extent the signature is valid under applicable law." 75 Fed. Reg. 40868, 40902 (Jul. 14, 2010).

Thus, compliance with eSIGN and UETA standards should assure compliance with the Common Rule and HIPAA for purposes of documenting informed consent and authorization.

Documentation and Retention of Other Records in Electronic Format

The Common Rule and Protection of Human Subjects in Medical Experimentation Act are also silent with respect to electronic creation, transmission, and retention of research administration records such as records of an IRB's deliberations and approval of a research study or records of study visits or procedures performed in connection with the study, including case report forms and associated source documentation. Under eSIGN and UETA, however, electronic documentation of these research activities is permissible if the records "accurately reflect" what occurred and access is assured to those who would be entitled to access to paper records. This applies both to records originally created in electronic format and to retention of records originally created on paper. Accuracy can be assured in numerous ways but compliance with FDA regulations for electronic systems and records should satisfy any eSIGN and UETA requirements.

FDA-Regulated Research

When electronic signatures or recordkeeping systems are utilized to support research involving drugs, biologics, and devices regulated by the U.S. Food and Drug Administration, the research is subject to a specialized set of requirements found at 21 C.F.R. Part 11 ("Part 11").

FDA-regulated clinical trials are subject to a series of regulations governing FDA applications and approvals, human subjects protections, institutional review board operations, conflict of interest, and mandatory recordkeeping and reporting (collectively the "predicate rules"). A system such as a medical record system designed to comply with HIPAA's information security requirements very likely can be configured to comply with Part 11's core electronic signatures and records standards. Proper configuration, however, is a key to compliance and for this reason it is advisable to perform a focused Part 11 review of any electronic system intended to be utilized as the sole means to

[2] These regulations permit the use of electronic signatures *only if* one of two "acceptable technolog[ies]" are used by public entities, *i.e.*, public key cryptography (PKC) and signature dynamics. *See* 22 CCR 22003 ("List of Acceptable Technologies"); *see also* http://www.sos.ca.gov/digsig/digital-signature-faq.htm#choose (FAQ "How should we choose between…").

[3] eSIGN, Section 7002.

[4] The agency proposed electronic signature standards in August 1998 but a promised final rule has never materialized.

collect consent signatures or document other research activities (including retention of source documentation, such as relevant medical records) consistent with the predicate rules. The documents attached at Appendices A-D below can be utilized to facilitate such a review and certify compliance to industry sponsors who sometimes demand it. Unfortunately, although Part 11 itself seems on its face to be relatively straightforward, FDA has released a series of guidance documents since the regulation was first promulgated that can render compliance a complex undertaking but that nevertheless should be consulted in performing a Part 11 review.[5]

First, FDA has advised that when computers are used solely to produce physical records (for example, to generate forms or other documents that will be "wet signed" by researchers or authorized staff), or when certain legacy systems are utilized, the agency will exercise enforcement discretion and not subject the resulting records to Part 11 standards or will subject them only to limited requirements. *See* 2003 Guidance. The agency also has published practical guidance on steps that should be taken to assure compliance with Part 11 when employing computerized systems to facilitate clinical trials in those cases where Part 11 controls. *See* 2007 Guidance.

More recently, FDA published a *draft* guidance document titled Electronic Source Documentation in Clinical Trials. The draft guidance defines *eSource documents* and *eSource data*, and identifies three principal "tiers" of data management: (1) data entry, (2) data review, and (3) data processing and transmission. Among other things, the draft guidance suggests that research investigators should review completed portions of the eCRF *for each subject* before data are archived and released to sponsors or FDA; and specifies that in those rare instances where the investigator is not privy to certain data elements (*e.g.*, to maintain a blind), prior FDA concurrence with the plan should be secured. It also recommends that the investigator maintain control over at least one copy of any source data as reported to sponsors or FDA and retain that copy throughout the standard retention period (generally at least two years following study termination and notification to FDA). The guidance clearly reflects FDA's position that the investigator is ultimately responsible for the accuracy and integrity of reported research results, even in those instances where research staff have primary responsibility for documenting the information.

Although the source documentation guidance exists only in draft form and even when finalized will not theoretically represent a new mandate, it does provide insight into inquiries FDA inspectors may make or data they may review during routine and for-cause inspections even today, including:

- Information on the reliability and integrity of any software or equipment used to record or transmit data elements directly from EHRs or other clinical records or sources to eCRFs, including information on the ability of the software to ensure that data elements are entered for the correct subject. FDA advises that algorithms for automated data extraction be described in study protocols or other documents that include "data management details." For example, some information, such as concomitant medications or weight, may change with time. FDA expects the protocol or other documents to describe the procedure for selecting the appropriate data element in these cases.
- Documents (*e.g.*, hospital or clinic records, whether electronic or written) relied upon by clinical trial staff in manually transcribing clinical information to eCRFs and other research records, including the original source documents and information that identifies the transcriber.
- Documentation of key "data element identifiers" for each recorded data element, including: (1) data element originators, whether human or machine; (2) date and time of entry to eCRF; and (3) the study subject to which the data element belongs. Modified or amended data elements should, according to the draft guidance, include at least original (and write-protected) data elements/identifiers; the date, time, and originator of the change; and a text field to describe the reason for the change. The guidance specifically recommends that clinical data be entered electronically by study site personnel at the time of the subject visit in order to avoid transcription errors.

[5] Strict compliance with FDA guidance is not mandated, even in FDA-regulated clinical trials. However, the agency's published guidance serves as a means to understand its interpretation of controlling laws and regulations, as well as its enforcement approach. Where full compliance is not feasible for any reason, it is advisable to document an alternative mechanism of assuring compliance with the underlying regulations.

- A complete, accurate, and continuously updated list of prospectively determined originators (persons, devices, and instruments) of data elements authorized to transmit data elements to the eCRF.
- Archived copies of eCRFs and other electronic documents and records pertinent to the study, in read-only format, write-protected at the time of investigator sign-off.

FDA states that its review divisions are available to review with *sponsors* their plans for the handling of electronic source data before deployment of a computerized system. The draft guidance is silent on any assistance that may be available to research sites. Comments on the draft guidance were due April 7, 2011. No date has been set for issuance of a final guidance document.

Notwithstanding its complexity, the draft guidance can be understood as simply a means for FDA to emphasize its concerns with data quality, which is essential to assure that only safe products reach and stay on the market.

Incident Preparedness and Response

Among the risks inherent in adopting electronic systems to facilitate electronic transactions and documentation are: (1) false or otherwise incorrect identity authentication; and (2) communication failures that result in substantive informed consent or authorization deficiencies. These risks can be mitigated with:

- Appointment of a single individual who is clearly delegated primary accountability for systems integrity and serves as the first point of contact when an incident occurs (typically a Chief Information Officer, Program Manager, or person in a similar role)
- Development and implementation of a comprehensive incident response plan; and
- Empaneling of an incident response and remediation committee that represents different stakeholders whose job it is to investigate, report on, and correct any acute or systemic errors or deficiencies that may have contributed to an identified incident.

These issues may be addressed through broadly applicable information security policies adopted by each campus.

Conclusion

Electronic signatures and records may be used to satisfy documentation requirements under federal and state laws and regulations governing human subjects research. Compliance with FDA standards to assure that electronic records are "trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper," 21 C.F.R. § 11.1(a), should be adequate to assure compliance with eSIGN and UETA technical standards. Assuring that subjects receive proper notice of their rights with respect to electronic signatures when electronic signatures are used to document informed consent should address any remaining needs.

Attachments

Appendix A – Model Part 11 Compliance Survey Instrument
Appendix B – Model Compliance Statement
Appendix C – Model Non-Repudiation Statement
Appendix D – Model Non-Repudiation Letter

Links

U.S. Food and Drug Administration:
- Regulations: 21 CFR Part 11; *see also* Federal Register Notice – 62 Fed. Reg. 13430 (Mar. 20, 1997)
- Inspections Notice (July 2010)
- Bioresearch Monitoring Program – CPGM 7348.811 (see p. 9)

- Computerized Systems Used in Clinical Investigations (May 2007); *see also* April 1999 Guidance
- Part 11, Electronic Records; Electronic Signatures – Scope and Application (August 2003); *see also* 2002 DRAFT
- DRAFT Guidance on Electronic Source Documentation (December 2010); *see also* Presentation and Presentation
- FDA Bioresearch Monitoring Compliance Program - Inspections
- Certification Instructions
- Presentation (March 2009); Webinar (January 2012)

Other Federal Rules:

- Federal Electronic Signatures in Global and National Commerce Act, 15 USC 7000-7006 (eSIGN)
- NIST eSIGN Guidance (for Federal agencies)
- NIST Authentication Guidelines (and here)
- NIST Privacy and Security Controls Guidance (see Special Publication 800-53)
- FTC Report on Consumer Consent Provisions in eSIGN
- Health Insurance Portability and Accountability Act (HIPAA)

State Laws

- Uniform Electronic Transactions Act, Cal. Civ. Code 1633.1 *et seq.* (UETA)
- National Conference of State Legislators (UETA Website)

More Information

Contact: Rachel Nosowsky, OGC (510) 987-9407
Rani Singh, OGC (510) 987-9729

Subpart A – General Provisions

Sec. 11.1 Scope.

(a) The regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper.

(b) This part applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted, under any records requirements set forth in agency regulations. This part also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act and the Public Health Service Act, even if such records are not specifically identified in agency regulations. However, this part does not apply to paper records that are, or have been, transmitted by electronic means.

(c) Where electronic signatures and their associated electronic records meet the requirements of this part, the agency will consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations, unless specifically excepted by regulation(s) effective on or after August 20, 1997.

(d) Electronic records that meet the requirements of this part may be used in lieu of paper records, in accordance with 11.2, unless paper records are specifically required.

(e) Computer systems (including hardware and software), controls, and attendant documentation maintained under this part shall be readily available for, and subject to, FDA inspection.

(f) This part does not apply to records required to be established or maintained by 1.326 through 1.368 of this chapter. Records that satisfy the requirements of part 1, subpart J of this chapter, but that also are required under other applicable statutory provisions or regulations, remain subject to this part.

Sec. 11.2 Implementation.

(a) For records required to be maintained but not submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that the requirements of this part are met.

(b) For records submitted to the agency, persons may use electronic records in lieu of paper records or electronic signatures in lieu of traditional signatures, in whole or in part, provided that:

(1) The requirements of this part are met; and

(2) The document or parts of a document to be submitted have been identified in public docket No. 92S-0251 as being the type of submission the agency accepts in electronic form. This docket will identify specifically what types of documents or parts of documents are acceptable for submission in electronic form without paper records and the agency receiving unit(s) (e.g., specific center, office, division, branch) to which such submissions may be made. Documents to agency receiving unit(s) not specified in the public docket will not be considered as official if they are submitted in electronic form; paper forms of such documents will be considered as official and must accompany any electronic records. Persons are expected to consult with the intended agency receiving unit for details on how (e.g., method of transmission, media, file formats, and technical protocols) and whether to proceed with the electronic submission.

Sec. 11.3 Definitions.

(a) The definitions and interpretations of terms contained in section 201 of the act apply to those terms when used in this part.

(b) The following definitions of terms also apply to this part:

(1) *Act* means the Federal Food, Drug, and Cosmetic Act (secs. 201-903 (21 U.S.C. 321-393)).

(2) *Agency* means the Food and Drug Administration.

(3) *Biometrics* means a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable.

(4) *Closed system* means an environment in which system access is controlled by persons who are responsible for the content of electronic records that are on the system.

(5) *Digital signature* means an electronic signature based upon cryptographic methods of originator authentication, computed by using a set of rules and a set of parameters such that the identity of the signer and the integrity of the data can be verified.

(6) *Electronic record* means any combination of text, graphics, data, audio, pictorial, or other information representation in digital form that is created, modified, maintained, archived, retrieved, or distributed by a computer system.

(7) *Electronic signature* means a computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the legally binding equivalent of the individual's handwritten signature.

(8) *Handwritten signature* means the scripted name or legal mark of an individual handwritten by that individual and executed or adopted with the present intention to authenticate a writing in a permanent form. The act of signing with a writing or marking instrument such as a pen or stylus is preserved. The scripted name or legal mark, while conventionally applied to paper, may also be applied to other devices that capture the name or mark.

(9) *Open system* means an environment in which system access is not controlled by persons who are responsible for the content of electronic records that are on the system.

Subpart B – Electronic Records

Sec. 11.10 Controls for closed systems.

Persons who use closed systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity, and, when appropriate, the confidentiality of electronic records, and to ensure that the signer cannot readily repudiate the signed record as not genuine. Such procedures and controls shall include the following:

(a) Validation of systems to ensure accuracy, reliability, consistent intended performance, and the ability to discern invalid or altered records.

Is [NAME OF SYSTEM] compliant? ☐ Yes ☐ No
Briefly summarize why or why not:

(b) 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. Persons should contact the agency if there are any questions regarding the ability of the agency to perform such review and copying of the electronic records.

Is [NAME OF SYSTEM] compliant? ☐ Yes ☐ No
Briefly summarize why or why not:

(c) Protection of records to enable their accurate and ready retrieval throughout the records retention period.

Is [NAME OF SYSTEM] compliant? ☐ Yes ☐ No
Briefly summarize why or why not:

(d) Limiting system access to authorized individuals.

Is [NAME OF SYSTEM] compliant? ☐ Yes ☐ No
Briefly summarize why or why not:

(e) Use of secure, computer-generated, time-stamped audit trails to independently record the date and time of operator entries and actions that create, modify, or delete electronic records. Record changes shall not obscure previously recorded information. Such audit trail documentation shall be retained for a period at least as long as that required for the subject electronic records and shall be available for agency review and copying.

Is [NAME OF SYSTEM] compliant? ☐ Yes ☐ No
Briefly summarize why or why not:

(f) Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.

Is [NAME OF SYSTEM] compliant? ☐ Yes ☐ No
Briefly summarize why or why not:

(g) Use of authority checks to ensure that only authorized individuals can use the system, electronically sign a record, access the operation or computer system input or output device, alter a record, or perform the operation at hand.

Is [NAME OF SYSTEM] compliant? ☐ Yes ☐ No
Briefly summarize why or why not:

(h) Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction.

Is [NAME OF SYSTEM] compliant? ☐ Yes ☐ No
Briefly summarize why or why not:

(i) Determination that persons who develop, maintain, or use electronic record/electronic signature systems have the education, training, and experience to perform their assigned tasks.

Is [NAME OF SYSTEM] compliant? ☐ Yes ☐ No
Briefly summarize why or why not:

(j) The establishment of, and adherence to, written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification.

Is [NAME OF SYSTEM] compliant? ☐ Yes ☐ No
Briefly summarize why or why not:

(k) Use of appropriate controls over systems documentation including:

(1) Adequate controls over the distribution of, access to, and use of documentation for system operation and maintenance.

(2) Revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation.

Is [NAME OF SYSTEM] compliant? ☐ Yes ☐ No
Briefly summarize why or why not:

Sec. 11.30 Controls for open systems.

Persons who use open systems to create, modify, maintain, or transmit electronic records shall employ procedures and controls designed to ensure the authenticity,

integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt. Such procedures and controls shall include those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure, as necessary under the circumstances, record authenticity, integrity, and confidentiality.

Is [NAME OF SYSTEM] compliant? ☐ Yes ☐ No
Briefly summarize why or why not:

Sec. 11.50 Signature manifestations.

(a) Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:

(1) The printed name of the signer;

(2) The date and time when the signature was executed; and

(3) The meaning (such as review, approval, responsibility, or authorship) associated with the signature.

Is [NAME OF SYSTEM] compliant? ☐ Yes ☐ No
Briefly summarize why or why not:

(b) The items identified in paragraphs (a)(1), (a)(2), and (a)(3) of this section shall be subject to the same controls as for electronic records and shall be included as part of any human readable form of the electronic record (such as electronic display or printout).

Is [NAME OF SYSTEM] compliant? ☐ Yes ☐ No
Briefly summarize why or why not:

Sec. 11.70 Signature/record linking.

Electronic signatures and handwritten signatures executed to electronic records shall be linked to their respective electronic records to ensure that the signatures cannot be excised, copied, or otherwise transferred to falsify an electronic record by ordinary means.

Is [NAME OF SYSTEM] compliant? ☐ Yes ☐ No
Briefly summarize why or why not:

Subpart C – Electronic Signatures

Sec. 11.100 General requirements.

(a) Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else.

Is [NAME OF SYSTEM] compliant? ☐ Yes ☐ No
Briefly summarize why or why not:

(b) Before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.

Is [NAME OF SYSTEM] compliant? ☐ Yes ☐ No
Briefly summarize why or why not:

(c) Persons using electronic signatures shall, prior to or at the time of such use, certify to the agency that the electronic signatures in their system, used on or after August 20, 1997, are intended to be the legally binding equivalent of traditional handwritten signatures.

(1) The certification shall be submitted in paper form and signed with a traditional handwritten signature, to the Office of Regional Operations (HFC-100), 5600 Fishers Lane, Rockville, MD 20857.

(2) Persons using electronic signatures shall, upon agency request, provide additional certification or testimony that a specific electronic signature is the legally binding equivalent of the signer's handwritten signature.

Is [NAME OF SYSTEM] compliant? ☐ Yes ☐ No
Briefly summarize why or why not:

Sec. 11.200 Electronic signature components and controls.

(a) Electronic signatures that are not based upon biometrics shall:

(1) Employ at least two distinct identification components such as an identification code and password.

(i) When an individual executes a series of signings during a single, continuous period of controlled system access, the first signing shall be executed using all electronic signature components; subsequent signings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual.

(ii) When an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing shall be executed using all of the electronic signature components.

(2) Be used only by their genuine owners; and

(3) Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals.

Is [NAME OF SYSTEM] compliant? ☐ Yes ☐ No
Briefly summarize why or why not:

(b) Electronic signatures based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners.

Is [NAME OF SYSTEM] compliant? ☐ Yes ☐ No
Briefly summarize why or why not:

Sec. 11.300 Controls for identification codes/passwords.

Persons who use electronic signatures based upon use of identification codes in combination with passwords shall employ controls to ensure their security and integrity. Such controls shall include:

(a) Maintaining the uniqueness of each combined identification code and password, such that no two individuals have the same combination of identification code and password.

Is [NAME OF SYSTEM] compliant? ☐ Yes ☐ No
Briefly summarize why or why not:

(b) Ensuring that identification code and password issuances are periodically checked, recalled, or revised (e.g., to cover such events as password aging).

Is [NAME OF SYSTEM] compliant? ☐ Yes ☐ No
Briefly summarize why or why not:

(c) Following loss management procedures to electronically deauthorize lost, stolen, missing, or otherwise potentially compromised tokens, cards, and other devices that bear or generate identification code or password information, and to issue temporary or permanent replacements using suitable, rigorous controls.

Is [NAME OF SYSTEM] compliant? ☐ Yes ☐ No
Briefly summarize why or why not:

(d) Use of transaction safeguards to prevent unauthorized use of passwords and/or identification codes, and to detect and report in an immediate and urgent manner any attempts at their unauthorized use to the system security unit, and, as appropriate, to organizational management.

Is [NAME OF SYSTEM] compliant? ☐ Yes ☐ No
Briefly summarize why or why not:

(e) Initial and periodic testing of devices, such as tokens or cards, that bear or generate identification code or password information to ensure that they function properly and have not been altered in an unauthorized manner.

Is [NAME OF SYSTEM] compliant? ☐ Yes ☐ No
Briefly summarize why or why not:

Statement on University of California, [CAMPUS] Compliance with 21 CFR Part 11

University of California faculty and staff sometimes use electronic applications to maintain records and create signatures necessary to support human research activities, some of which are governed by FDA regulations.

Sponsors occasionally request certification of compliance with 21 C.F.R. Part 11 (" Part 11") or alternatively certification that systems covered by Part 11 will not be used for these activities. This notice provides information about the University's use of electronic applications and the compliance of those systems with Part 11 requirements.

[DESCRIBE ANY ELECTRONIC SYSTEMS USED BY THE CAMPUS FOR PROTOCOL APPLICATIONS, APPROVALS, AND OTHER REGULATORY DOCUMENTATION THAT IRBs AND/ OR INVESTIGATORS ARE REQUIRED TO MAINTAIN. PROVIDE WEBSITE LINKS IF PUBLIC. ASSUMING THE CAMPUS HAS PERFORMED THE REQUISITE VALIDATION AND ISSUED A NON-REPUDIATION LETTER TO FDA, ADD THE REMAINING LANGUAGE IN THIS PARAGRAPH.] UC___ believes that [SYSTEM NAME], together with the University's electronic authentication system, is substantially compliant with Part 11 requirements and neither the University's institutional review board nor, to our knowledge, any individual University researcher functioning as a sponsor and/ or investigator has been cited for non-compliance with Part 11. However, the University is unable to provide any absolute representation or warranty of compliance.

Sponsors or others seeking certification of compliance may be provided with a copy of this letter. UC___ researchers performing FDA-regulated studies may rely on this substantial compliance certification or may print out and physically sign required documents and maintain these with other required research records. FDA has specified that it will exercise " enforcement discretion" where electronic records and signature are committed to physical writings and appropriately countersigned to assure security and non-repudiation.

Questions about this statement may be directed to: [PROVIDE APPROPRIATE CONTACT INFORMATION]

Attachment:

> Statement of [TITLE OF RELEVANT CAMPUS OFFICIAL – TYPICALLY THE INSTITUTIONAL OFFICIAL] on non-repudiation of electronic signatures in [SYSTEM NAME].

Additional Resources:

- [LIST – AND ATTACH COPIES OF IF NOT ACCESSIBLE ON PUBLIC WEBSITES – SYSTEM AND CAMPUS POLICIES AND GUIDELINES APPLICABLE TO ANY OF THE ELECTRONIC SYSTEMS LISTED ABOVE ADDRESSING DELEGATION OF AUTHORITY TO BIND THE UNIVERSITY (OR THE CAMPUS), INFORMATION RESOURCES POLICIES THAT ADDRESS APPROPRIATE USE, IDENTITY MANAGEMENT/ USER ID AND PASSWORD ADMINISTRATION, IT SECURITY, EMPLOYEE TRAINING ON IT SECURITY, ETC.]

Statement of [DESIGNATED CAMPUS OFFICIAL] On Non-Repudiation of Electronic Signatures in [SYSTEM NAME]

To: Members of the University of California, [CAMPUS NAME] Research Community

From: [NAME], [TITLE]

Re: Non-Repudiation of Electronic Signatures

Date: [TBD]

Researchers and research staff who are involved with FDA-regulated studies are asked from time to time to certify compliance with 21 C.F.R. Part 11 (" Part 11" for short) – the regulations promulgated and enforced by FDA on the development, implementation, and use of electronic records and signatures.

[WHO] has reviewed the [SYSTEM NAME] and validated that it is substantially compliant with Part 11 requirements. One of those requirements is the submission to FDA of a letter promising that any electronic signatures used in [SYSTEM NAME] are intended to be the legally binding equivalent of hand-written, or " wet," signatures. A copy of the letter we are submitting to FDA is attached for your information.

A variety of University policies and procedures require faculty and staff to secure their usernames and passwords (" ID/ PW") against unauthorized use. It is important to remember that **any submission to [SYSTEM NAME] using your ID/PW is assumed to be a submission by you personally.** Because the signature is legal and binding, it is critical for you to comply with UC___ policies and assure the integrity of your ID/ PW. Simple steps you can take to do so include:

- *Never, ever share your password with anyone, including family members, students, supervisors, support staff, or others.*
- *Never keep your password in a computer file, on your desk, or in other obvious or easily accessible locations.*
- *When developing passwords, do not use dictionary words, foreign words, simple transformations, repeated words, names of people, keyboard sequences, phone numbers, or words with vowels removed, even if the system might allow this. Do use a line from a song or verse together with mixed cases, punctuation marks, and numbers (e.g., " Mary had a little lamb" would convert to m!h!a!l!!! or m1h3a5171 or, best yet, M!h1ll!).*
- *Change your password frequently, at least every three (3) months, even if not prompted or required to do so by the system.*

[LETTERHEAD]

[Date]

Office of Regional Operations (HFC-100)
5600 Fishers Lane
Rockville, MD 20857

Michael Fauntleroy
Office of the Director (HFM-25)
Center for Biologics Evaluation and Research
Food and Drug Administration
11400 Rockville Pike, Room 4119
Rockville, MD 20857.

Re: Electronic Signature Certificate Statement

To Whom It May Concern:

Pursuant to Section 11.100 of Title 21 of the Code of Federal Regulations, this is to certify that The University of California, [CAMPUS NAME] intends that all electronic signatures executed in the following electronic record system(s) by our officers, directors, employees, students or contractors, located anywhere in the world, are the legally binding equivalent of traditional hand-written signatures, subject to applicable University policies including [CITE RELEVANT CAMPUS POLICY ON NON-REPUDIATION/ BINDING NATURE OF SIGNATURES IN ELECTRONIC SYSTEMS]:

- [LIST INDIVIDUAL VALIDATED SYSTEMS HERE]

Sincerely yours,

_____

[NAME]
[TITLE – E.G., CHIEF INFORMATION OFFICER]
[CAMPUS]