21 CFR 11 - Electronic Records; Electronic Signatures Assessment Worksheet

System Name:		**System Location:**	
System ID #:		**System Owner:**	
Assessment Type *(check all that apply after completing pg. 3)*	☐ Electronic Records ☐ Electronic Signatures ☐ Closed System ☐ Open System	**Assessor(s):**	
Start Date:		**End Date:**	

APPROVAL OF ELECTRONIC RECORDS ASSESSMENT RESULTS

The approval signatures below mean that the signers:

- Have diligently read this document, and based upon their understanding of this document and the signer's education, training, and experience, can find no substantive errors or omissions, and
- Attest that the assessment described by this worksheet accurately summarizes the current capability of the computerized system described in this assessment to fulfill the applicable requirements of 21 CFR Part 11.

_____	_____	_____	_____
System Owner	Date	Lead Assessor	Date

PURPOSE:

The purpose of this worksheet is to:

- Specify the criteria under which electronic records, electronic signatures, and handwritten signatures executed to electronic records are considered equivalent to paper records and handwritten signatures executed on paper in accordance with 21 CFR Part 11 (the Regulation),
- Evaluate a computerized system versus the established requirements, and
- Document the evaluation of the computerized system.

SCOPE:

This worksheet is designed to assist with the assessment of computerized systems that create, modify, maintain, archive, retrieve, or transmit electronic record(s) that are required to demonstrate compliance with FDA regulations, and that are used in lieu of paper records.

This worksheet does not apply to those electronic records that are:

- not required to be maintained, or
- not used in lieu of paper records, or
- transmitted fax or scanned paper records, or
- required to be submitted to the FDA.

PROCEDURES / INSTRUCTIONS FOR USE OF THIS TEMPLATE:

1. Assemble a cross-functional team to conduct the assessment. (It is strongly recommended that more than one individual perform the assessment.) Recommended members include the system supervisor or a very knowledgeable user, the IS Project Leader or a systems support person, and a Validation representative.
2. Classify the assessed system by completing the CLASSIFICATION SECTION. (Guidance for completing this section is included in the GUIDANCE SECTION, item numbers CG.1 - CG.7.) If 21 CFR 11 applies to the system (C.2 - C.3) and the system is a closed system (C.4) complete this worksheet. Otherwise return this incomplete worksheet to the Computer Validation Group.
3. Table 1 includes references to which sections of 21 CFR 11 are applicable to which classes of computer systems. Working from Table 1 and the scenario number(s) selected so far, mark as non-applicable (“N/A”) all line items (“R” numbers) in the ASSESSMENT SECTION that correspond to the specified N/A 21 CFR 11 paragraph numbers.
4. Complete the ASSESSMENT SECTION. (Guidance for completing this section is included in the GUIDANCE SECTION, item numbers RG.1 - RG.14.5.) Assess the ability of the systems to fulfill the specified 21 CFR 11 Requirement. Record “C” (Conforming), “NC” (Non-conforming), or “N/A” (Not Applicable) for the results of the assessment in the Assessment Results column. Each NC or N/A response requires a clarification in the Comments column or the OBSERVATIONS SECTION.
5. Complete the OBSERVATIONS SECTION at the same time as the ASSESSMENT evaluation. Note: recommendation for system remediation will be given at a later phase of the project.
6. Approve the Assessment Worksheet on Page 1.
7. Forward the completed ASSESSMENT (hard copy) to the Computer Validation group to be archived. Place the completed electronic copy (MS Word) of the assessment into the **21CFR11 Assessment** folder (path: QAdomain/Common/1999Projects/21cfr11/Assessment).

SYSTEM CLASSIFICATION SECTION:

Determine if the computerized system is required to comply with 21 CFR 11 and the applicable sections, if any.

Question #	Question	Answer	Observation / Recommen-dation #
C.1	Does this computerized system create, modify, maintain, archive, retrieve, or transmit any electronic record(s) that are required to demonstrate compliance with FDA regulations? *(**NOTE:** Even if "parallel" paper records exist, answer "yes." All electronic records that are maintained in viewable condition must comply.)*	☐ No Stop here, Part 11 compliance is not required. ☐ Yes Continue with next question.	
C.2	Is this computerized system used exclusively to transmit paper records by electronic means, such as FAX's and scanned images?	☐ Yes Stop here, Part 11 compliance is not required. ☐ No Continue with next question.	
C.3	Do FDA regulations permit the use of electronic records for this required documentation? If the answer is "No", indicate the specific CFR reference requiring these records to be maintained in paper format only. ____ CFR Part(s) _____	☐ No Stop here, Part 11 compliance is not required. ☐ Yes Continue with next question.	
C.4	Is the computerized system an "Open System" or a "Closed System"? ***NOTE:** For systems deemed to be "open systems" **stop work here** and forward this assessment to the Computer Validation Group.*	☐ Open System Stop here. ☐ Closed System Continue with next question.	
C.5	Does the computerized system requires electronic signatures on the electronic records? Q1 - "If the records are printed out, would or do you need to sign them?" Q2 - "Do you save 'John Smith' as a field in the file / database and expect it to be right on the form, printout, and/or archive?" Q3 - "If I sign 'John Smith' does that mean I have attested that I did or saw something, or that I'm authorizing some action?" If any of these answers is yes, e-sigs are required.	☐ No Scenario #1 Applies Skip to C.7 ☐ Yes Continue with next question	
C.6	Classify the electronic signature that this system uses: (Check all that apply.) • Handwritten signature executed to electronic record • Biometric • Identification code / password • Token / password *If system doesn't have any of the above capabilities then complete section 11.10 (pages 5 & 6 ONLY) and forward the assessment to the Computer Validation Group.*	☐ Scenario #2 Applies ☐ Scenario #3 Applies ☐ Scenario #4 Applies ☐ Scenario #5 Applies Continue with next question	
C.7	Update the "Assessment Type" on the cover sheet. Update the "ASSESSMENT SECTION" to indicate which 21 CFR 11 sections are N/A according to the chosen Scenario Number and Table 1. Complete the "ASSESSMENT SECTION".		

TABLE 1 - Applicable Sections of 21 CFR 11?

Scenario #	ATTRIBUTES	21 CFR 11 Sections (✓ = applicable / N/A = not applicable)									
		11.1; 11.2; 11.3	11.10	11.30	11.50	11.70	11.100	11.200 (a)	11.200 (b)	11.300 (a), (b), (d)	11.300 (c), (e)
	CLOSED SYSTEMS										
1	Electronic Record Only (without signature)	✓	✓	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
2	Handwritten Signature Executed to Electronic Record	✓	✓	N/A	✓	✓	N/A	N/A	N/A	N/A	N/A
3	Electronic Signature Based upon Biometrics	✓	✓	N/A	✓	✓	✓	N/A	✓	N/A	N/A
4	Electronic Signature Based upon ID Code & Password	✓	✓	N/A	✓	✓	✓	✓	N/A	✓	N/A
5	Electronic Signature ID Code & Token	✓	✓	N/A	✓	✓	✓	✓	N/A	N/A	✓
NOTES:	The applicable parts of 21 CFR Part 11 for each type of system are check-marked in the table above.										
	OPEN SYSTEMS										
Forward all "open system" assessments to the Computer Validation Group.											

ASSESSMENT SECTION:

1. Ensure that all non-applicable parts have been marked "N/A" before beginning this assessment. (Ref. CLASSIFICATION SECTION)
2. "21 CFR 11 Requirements" are listed as detailed line items R.1 through R.14.5. Review the structure and function of the computerized system and assess its compliance with these against these requirements. (Note: The GUIDANCE SECTION includes guidance in interpreting 21 CFR 11 and suggestions for assessing the system. The guidance information is listed by corresponding requirement number.)
3. Record "Assessment Results" as conformances or non-conformances. Record observations or recommendations (abbr. OBS/REC) in the OBSERVATIONS AND RECOMMENDATIONS SECTION. Record the Requirement and OBS/REC numbers in their corresponding sections.
   Each non-conformance requires an Observation or Recommendation.

Key: **C** = *Conforms to Requirement*; **NC** = *Non-Conformance*; **N/A** = *Not Applicable;*

Require-ment #	21 CFR 11 Requirements	Assessment Results	OBS/REC Number(s)
	SUB-PART B: ELECTRONIC RECORDS		
	11.10: CONTROLS FOR CLOSED SYSTEMS		
R.1	**Validation -** The computerized system shall be validated in accordance with applicable Corporate Standards and regulatory requirements to ensure....		
R.1.1	• Accuracy. [11.10 (a)]	☐ C ☐ NC ☐ N/A	
R.1.2	• Reliability. [11.10 (a)]	☐ C ☐ NC ☐ N/A	
R.1.3	• Consistent intended performance. [11.10 (a)]	☐ C ☐ NC ☐ N/A	
R.1.4	• Ability to discern invalid or altered records. [11.10 (a)]	☐ C ☐ NC ☐ N/A	
R.2	**Inspectability -** Procedures and controls shall be designed and implemented to include the ability to...		
R.2.1	• Generate accurate and complete copies of records in both human and electronic form for inspection, review, and copying by the FDA. [11.10 (b)]	☐ C ☐ NC ☐ N/A	
R.2.2	• Protect records to enable their accurate and ready retrieval throughout the records retention period. [11.10 (c)]	☐ C ☐ NC ☐ N/A	
R.3	**Security -** Security procedures and controls shall be designed and implemented to include:		
R.3.1	• System access shall be limited to authorized individuals. [11.10 (d)] (Physical access)	☐ C ☐ NC ☐ N/A	
R.3.2	• Operational system checks shall enforce the proper sequencing of steps in a process (as appropriate). [11.10 (f)]	☐ C ☐ NC ☐ N/A	
R.3.3	• Authority checks shall ensure that only authorized individuals can:		
R.3.3.1	• Use the system. [11.10 (g)] (Logical access)	☐ C ☐ NC ☐ N/A	
R.3.3.2	• Electronically sign a record. [11.10 (g)]	☐ C ☐ NC ☐ N/A	
R.3.3.3	• Access the operation or computer system input or output device. [11.10 (g)]	☐ C ☐ NC ☐ N/A	
R.3.3.4	• Alter a record. [11.10 (g)]	☐ C ☐ NC ☐ N/A	
R.3.3.5	• Perform the specified operation. [11.10 (g)]	☐ C ☐ NC ☐ N/A	

Requirement #	21 CFR 11 Requirements	Assessment Results	OBS/REC Number(s)
R.3.4	• Device or terminal checks shall determine validity of the source of input or operation (as appropriate). [11.10 (h)]	☐ C ☐ NC ☐ N/A	
R.4	**Audit Trails -** Procedures and controls shall be designed and implemented for audit trails to:		
R.4.1	• Be secure. [11.10 (e)]	☐ C ☐ NC ☐ N/A	
R.4.2	• Be computer-generated. [11.10 (e)]	☐ C ☐ NC ☐ N/A	
R.4.3	• Be time- and date-stamped. [11.10 (e)]	☐ C ☐ NC ☐ N/A	
R.4.4	• Independently record the date/time of operator entries and actions that... (Journal function)		
R.4.4.1	• create electronic records. [11.10 (e)]	☐ C ☐ NC ☐ N/A	
R.4.4.2	• modify electronic records. [11.10 (e)]	☐ C ☐ NC ☐ N/A	
R.4.4.3	• maintain electronic records. [11.10 (e)]	☐ C ☐ NC ☐ N/A	
R.4.4.4	• delete electronic records. [11.10 (e)]	☐ C ☐ NC ☐ N/A	
R.4.5	• Ensure that changes to electronic records shall not obscure previously recorded information. [11.10 (e)]	☐ C ☐ NC ☐ N/A	
R.4.6	• Ensure that audit trail records shall be maintained for at least as long as the retention of the underlying records. [11.10 (e)]	☐ C ☐ NC ☐ N/A	
R.4.7	• Ensure that audit trail records shall be available for FDA review and copying. [11.10 (e)]	☐ C ☐ NC ☐ N/A	
R.5	**Personnel Qualifications -** Determination that the following persons have the education, training, and experience to perform their assigned tasks:		
R.5.1	• Developer(s) of the computerized system. [11.10 (i)]	☐ C ☐ NC ☐ N/A	
R.5.2	• Maintainer(s) of the computerized system. [11.10 (i)]	☐ C ☐ NC ☐ N/A	
R.5.3	• User(s) of the computerized system. [11.10 (i)]	☐ C ☐ NC ☐ N/A	
R.6	**Accountability and Responsibility for Actions -** Establishment of, and adherence to, written policies and/or procedures that hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification. [11.10 (j)]	☐ C ☐ NC ☐ N/A	
R.7	**Systems Documentation Controls -** Establishment and use of appropriate controls over systems documentation including:		
R.7.1	• Adequate controls over the documentation for system operation and maintenance, to include:		
R.7.1.1	• distribution of documentation. [11.10 (k)(1)]	☐ C ☐ NC ☐ N/A	
R.7.1.2	• access to documentation. [11.10 (k)(1)]	☐ C ☐ NC ☐ N/A	
R.7.1.3	• use of documentation. [11.10 (k)(1)]	☐ C ☐ NC ☐ N/A	
R.7.2	• Revision and change control procedures to maintain an audit trail that documents the time-sequenced development and modification of the systems documentation. [11.10 (k)(2)]	☐ C ☐ NC ☐ N/A	

	11.30: CONTROLS FOR OPEN SYSTEMS		
R.8	**Controls for Open Systems -** Open systems used to create, modify, maintain, or transmit electronic systems shall employ procedures and controls designed to ensure the following attributes for those electronic records from the point of their creation to the point of their receipt:		
R.8.1	• Authenticity. [11.30]	☐ C ☐ NC ☐ N/A	
R.8.2	• Integrity. [11.30]	☐ C ☐ NC ☐ N/A	
R.8.3	• Confidentiality, as appropriate. [11.30]	☐ C ☐ NC ☐ N/A	
	Such procedures and controls shall include:		
R.8.4	• Those identified in 11.10, as appropriate. [11.30]	☐ C ☐ NC ☐ N/A	
R.8.5	• Document encryption, as appropriate. [11.30]	☐ C ☐ NC ☐ N/A	
R.8.6	• Use of digital signature standards, as appropriate. [11.30]	☐ C ☐ NC ☐ N/A	
	11.50: SIGNATURE MANIFESTATIONS		
R.9	**Signature Manifestations -** Signed electronic records shall contain information associated with the signing that clearly indicates all of the following:		
R.9.1	• The printed name of the signer. [11.50 (a)(1)]	☐ C ☐ NC ☐ N/A	
R.9.2	• The date and time when the signature was executed. [11.50 (a)(2)]	☐ C ☐ NC ☐ N/A	
R.9.3	• The meaning of the signature. [11.50 (a)(3)]	☐ C ☐ NC ☐ N/A	
	All items identified in 11.50 (a)(1), 11.50 (a)(2), and 11.50 (a)(3) above shall be:		
R.9.4	• Subject to the same controls as for electronic records. [11.50 (b)]	☐ C ☐ NC ☐ N/A	
R.9.5	• Included as part of any human readable form of the electronic record (such as electronic display and/or printout or report). [11.50 (b)]	☐ C ☐ NC ☐ N/A	
	11.70: SIGNATURE/RECORD LINKING		
R.10	**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. [11.70]	☐ C ☐ NC ☐ N/A	
	SUB-PART C: ELECTRONIC SIGNATURES		
	11.100: GENERAL REQUIREMENTS FOR ELECTRONIC SIGNATURES		
R.11	**General Requirements**		
R.11.1	• Each electronic signature shall be unique to one individual and shall not be reused by, or reassigned to, anyone else. [11.100 (a)]	☐ C ☐ NC ☐ N/A	
R.11.2	• The identity of the individual shall be verified prior to the organization establishing, assigning, certifying, or otherwise sanctioning that individual's electronic signature. [11.100 (b)]	☐ C ☐ NC ☐ N/A	

R.11.3	• Persons using electronic signatures shall, prior to or at the time of such use, certify to the FDA that the electronic signatures used in the computerized system on or after August 20, 1997 are intended to be the legally binding equivalent of traditional handwritten signatures. [11.100 (c)]	☐ C ☐ NC ☐ N/A	
R.11.4	• The certificate shall be submitted in paper form and signed with a traditional handwritten signature to the appropriate FDA Office specified in the Regulation. [11.100 (c)(1)]	☐ C ☐ NC ☐ N/A	
	11.200: ELECTRONIC SIGNATURE COMPONENTS AND CONTROLS		
R.12	**Electronic Signatures Not Based On Biometrics -** Electronic signatures that are not based on biometrics shall:		
R.12.1	• Employ at least 2 distinct identification components such as an identification code and password. [11.200 (a)(1)]	☐ C ☐ NC ☐ N/A	
R.12.2	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 singings shall be executed using at least one electronic signature component that is only executable by, and designed to be used only by the individual. [11.200 (a)(1)(i)]	☐ C ☐ NC ☐ N/A	
R.12.3	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. [11.200 (a)(1)(ii)]	☐ C ☐ NC ☐ N/A	
R.12.4	• Be used only by their genuine owners. [11.200 (a)(2)]	☐ C ☐ NC ☐ N/A	
R.12.5	• Be administered and executed to ensure that attempted use of an individual's electronic signature by anyone other that its genuine owner requires collaboration of two or more individuals. [11.200 (a)(3)]	☐ C ☐ NC ☐ N/A	
R.13	**Electronic Signatures Based On Biometrics**		
R.13.1	Electronic records based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners. [11.200 (b)]	☐ C ☐ NC ☐ N/A	
	11.300: CONTROLS FOR IDENTIFICATION CODES/PASSWORDS		
R.14	**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, including:.		
R.14.1	• The combination of identification code and password shall be unique. [11.300 (a)]	☐ C ☐ NC ☐ N/A	
R.14.2	• Identification code and password issuances shall be periodically checked, recalled, or revised (e.g., to cover such events as password aging). [11.300 (b)]	☐ C ☐ NC ☐ N/A	
R.14.3	• Procedures and controls shall be designed and implemented for devices which bear or generate identification code or password information to:		
R.14.3.1	• Electronically deauthorize devices that have been lost, stolen,	☐ C ☐ NC ☐ N/A	

	or potentially compromised. [11.300 (c)]		
R.14.3.2	• Issue temporary or permanent replacements using suitable, rigorous controls. [11.300 (c)]	☐ C ☐ NC ☐ N/A	
R.14.4	• Transaction safeguards shall be implemented to:		
R.14.4.1	• Prevent unauthorized use of identification codes and passwords. [11.300 (d)]	☐ C ☐ NC ☐ N/A	
R.14.4.2	• Detect any attempt at unauthorized use of identification codes and/or passwords. [11.300 (d)]	☐ C ☐ NC ☐ N/A	
R.14.4.3	• Report in an immediate and urgent manner any attempt at unauthorized use of identification codes and passwords to the system security unit, and, as appropriate, organizational management. [11.300 (d)]	☐ C ☐ NC ☐ N/A	
R.14.5	• Initial and periodic testing of devices that bear or generate identification code or password information. [11.300 (e)]	☐ C ☐ NC ☐ N/A	

GUIDANCE SECTION

Question #	Classification Guidance
Cover Sheet	Discuss the definition of the "system" in terms of its logical and physical boundaries. It is probably best to accept the specification of what comprises the "system" that is included in the validation documentation.
CG.1	The Regulation applies to a wide variety of computerized systems, not just those systems that use electronic signatures. The Regulation also applies to new and existing systems. No "grandfathering" provisions exist. See Preamble Comment #9 for a discussion of grandfathering. "Dual" sets of records, (e.g., one paper record system that is the "official" record and one electronic record system that is "for reference only") are strongly discouraged. According to the "Washington Drug Letter" of Sept. 29, 1997, "...one FDA'er said such practice can give the appearance of evading regulations, at least from an investigator's perspective. That source said existence of two sets of records would be taken 'very seriously' during an inspection..." also "...FDA expects a single record to be kept. **But if dual records, or even a hybrid paper and electronic system are maintained, agency rules apply to the electronic records...**" *[ed: emphasis added]* Answer "Yes" to this question if any of the following questions have a "Yes" answer. See Preamble Comments #22 and 26 for a full discussion of which systems fall within the scope of the Regulation. • Does any user rely on use of the computerized system to make decisions impacting the Quality System? • If asked to produce information for an inspector, will any of the submitted information be obtained from the computerized system? • If asked to produce custom or ad-hoc information for an inspector, will ANY part of that information be generated through or by the computerized system (e.g., trending reports, summary reports, exception reports)?
CG.2	Paper records transmitted by electronic means, such as FAX's and scanned images are exempt.
CG.3	Some regulations specifically paper records or documents. For these cases electronic records are prohibited. One example of this is that physical copies of master labels and package inserts must be retained.
CG.4	CCPI's corporate information security policies specify procedures and methods that ensure confidentiality, integrity, and authenticity of information assets. These policies include systems with modem / Internet access. Assume that all computerized systems solely under CCPI physical control meet the FDA-specified requirements for a "Closed" system. *"...the most important factor in classifying a system as open or closed is whether the persons responsible for the content of the electronic records control access to the system containing those records....If those persons do not control such access, then the system is open because the records may be read, modified, or compromised by others...Hence, those responsible for the records would need to take appropriate additional measures in an open system to protect those records from being read, modified, destroyed, or otherwise compromised by unauthorized and potentially unknown parties." Preamble Comment #41.* *"...where an organization's electronic records are stored on systems operated by third parties, such as commercial online services, access would be under control of the third parties and the agency would regard such a system as being open."* *(See Preamble Comment #44.)* Note the exception here. It's not users that have to be "under control" but administrators, DBA's etc. *"...dial-in access over public phone lines could be considered part of a closed system where access to the system that holds the electronic records is under the control of the persons responsible for the content of those records." Preamble Comment #44.* Assume that all computerized systems solely under CCPI control meet the specified requirements for a "Closed" system. This includes systems with modem access. Again CCPI corporate INFOSEC policies must be in place.
CG.5	Differentiate between "signature" and "identification". If the intent is to use the applied identification to authenticate the electronic record, then the identification is an

Question #	Classification Guidance
	electronic signature. If the intent is to merely identify who did something, that is not an electronic signature. From Preamble Comment 28: *"The agency stresses that part 11 does not require that any given electronic record be signed at all. The requirement that any record bear a signature is contained in the regulation that mandates the basic record itself. Where records are signed, however, by virtue of meeting a signature requirement or otherwise, part 11 addresses controls and procedures intended to help ensure the reliability and trustworthiness of those signatures."* In other words, if you would have to sign the paper copy, you have to sign the electronic copy. IMMEDIATE NOTE: Don't accept the dodge, "We save a signed paper copy, so we don't have to have electronic signatures on the electronic copy." According to the "Washington Drug Letter" of Sept. 29, 1997: *"...one FDA'er said such practice can give the appearance of evading regulations, at least from an investigator's perspective. That source said existence of two sets of records would be taken 'very seriously' during an inspection..." also "...FDA expects a single record to be kept. But if dual records, or even a hybrid paper and electronic system are maintained, agency rules apply to the electronic records..."* In other words, whether or not to use electronic signatures **is not the system owner's (or CCPI's) choice.** The choice is whether or not to use electronic records, and that choice (plus the other FDA regs.) dictates the requirement (or lack thereof) for electronic signatures. Based on this, the questioning of a system owner, to find out if e-sigs are required, is pretty straightforward. Q1 - "If these were or are printed out, would or do you need to sign them?" Q2 - "Do you save 'John Smith' as a field in the file / database and expect it to be right on the form, printout, and/or archive?" Q3 - "If I sign 'John Smith' does that mean I have attested that I did or saw something, or that I'm authorizing some action?" If any of these answers is yes, e-sigs are required.
CG.6	Indicate the current electronic signature method(s) being used, or those most likely to be used if an electronic signature requirement is established.

Guidance #	Assessment Guidance
	SUB-PART B: ELECTRONIC RECORDS
	11.10: CONTROLS FOR CLOSED SYSTEMS
	GENERAL GUIDANCE FOR ELECTRONIC RECORDS
	Legislative Intent: The agency is concerned with assuring that an individual cannot readily repudiate any electronic record and/or electronic signature attributable to that person. The agency considers authenticity of records and signatures vital to their goal of protecting the public health, so this Regulation should be carefully interpreted and applied. While assessing compliance, carefully consider the impact of each requirement on this overall goal.
	Electronic signature are, by definition, applied to electronic records. Therefore, all electronic signature systems must comply with the electronic records portions of 21 CFR 11.
	Portions of computerized system functionality should not be assessed outside the context of the entire system. This differs from the assessment of multiple, coordinated, peer-to-peer systems which will have selected transactions, screens, or functions that are included in the assessment.
RG.1	Was the system validated? Locate and examine the validation documentation for the system. Was the system adequately challenged for:
RG.1.1	• Accuracy?
RG.1.2	• Reliability? What were the reliability criteria against which the system was qualified? How long has it been operating? Any crashes or outages?
RG.1.3	• Consistent intended performance? Any deviations or unexplained data corruption?
RG.1.4	This requirement can be addressed by: • Abnormal case testing vs. verification of impact through the audit trail (or other system functionality). For example, conduct add/change/delete transactions and observe whether the audit trail can accurately discern the changes. • Tests to determine that, if tools outside of the application software can be used to add, change, or delete records, that these actions can be detected. Be very careful to check for ad-hoc database maintenance tools, and who has access to them. • Review of the system design/implementation to determine if there is some combination of edit checks, security, and or data validation that prevents or detects record altering. Be particularly diligent in reviewing inter-process communication between upstream and downstream applications that has been implemented in custom code. See Preamble Comment #68 and Preamble Comment #4. Also see RG.3.3.4 and R.4.
RG.2	Hardware, software, audit trails, and documentation all need to be available for inspection.
RG.2.1	The computerized system should be able to extract **only** the relevant electronic records upon request. It is strongly discouraged that an inspector be given an entire database or table unless it is specifically requested. *"Electronic copies can be accurate and complete without being in the same computer file format as the original." "..if you encounter an electronic...record that is not in a file format you can copy for off-line review, you'll need to work with the firm to ensure that the conversion file used for the copy...preserves the record content and integrity of meta data (data, such as time stamps, that describe a file), so as to be both accurate and complete."* Human Drug CGMP Notes, December 1997 edition, author Paul Motise (FDA) Key Questions to consider in assessing compliance include: • Can CCPI supply copies of a single record (in electronic format) to an inspector? In paper format? • Can CCPI supply all or any part of the audit trail (in electronic format) to an inspector? In paper format?

Guidance #	Assessment Guidance
	• Can CCPI supply copies of the entire database (in electronic format) to an inspector? • Are procedures in-place to describe HOW to accomplish these inspection tasks? • Are procedures in-place to define in what format the electronic records will be provided? For example, all records will be provided in the native database format, ASCII text, PDF, converted to a "standard" database format, etc.? • Are procedures in-place to assure that all electronic records requested by FDA are marked "Confidential" in order to avoid release of sensitive information into the public domain through FOI disclosures, etc.? • If requested, is it possible for an inspector to review the hardware, software, system-related documentation, and/or audit trail information? • Can all electronic records be reviewed in both electronic format and in paper format? Are there exceptions? • If this computerized system consists of geographically dispersed parts, does CCPI have procedures or policies to address the potential for multi-site inspections? (See Preamble Comment #3R.) See [11.1 (e)] for a full discussion. See Preamble Comments #69, 70, 30, and 33 for a full discussion.
RG.2.2	Has CCPI implemented a records retention policy? Is this system compliant, or is there a records retention SOP for this system? Note that electronic records and their audit trails must both follow these retention requirements. Questions related to this requirement might include: • Are the records in this system classified as to retention period? What is (are) the retention period(s)? • Have the records been saved in a format that can read by newer systems, or is there a plan to roll them forward? • Has CCPI made written provisions to maintain the capability at some point in the future to electronically read all electronic records associated with this computerized system throughout the entire records retention period? • For example, will supplanted hardware, software, configurations, and procedures be archived to read data? • Will all previously collected data (Note this says "DATA" not just records.) be converted for use in future revisions / replacements of this computerized system? (Note: As long as "accurate and complete copies" can be generated, there is no requirement to maintain supplanted hardware / software.) • -Is there a refreshment procedure for magnetic media? (Magnetic media deteriorates over time and must be periodically "refreshed" in order to remain readable.) See Preamble Comments #30 & # 71 for a full discussion
RG.3	Again, the corporate INFOSEC policies must be in place.
RG.3.1	Only persons who have a legitimate business requirement to use the system should be allowed physical access to the server / mainframe, systems console, or any critical component. Since this requirement [11.10 (d)] is virtually the same as [11.10(g)] these generally interpreted to refer to physical and logical access respectively. There is no specific Preamble Comment for this requirement. Ensure that Corporate INFOSEC policies are applied.
RG.3.2	This requirement is typically "Not Applicable". *"The agency advises that the purpose of performing operational checks is to ensure that operations (such as manufacturing production steps and signings to indicate initiation or completion of those steps) are not executed outside of the predefined order established by the operating organization."* See Preamble Comments #79 - #81 for a full discussion.
RG.3.3	Ensure that there is a definition of "authorized individuals," and a list of these individuals is published or maintained on the computer system. (Usually in the form of an access list) *"System access control is a basic security function because system integrity may be impeached even if the electronic records themselves are not directly accessed." "...it is unlikely that a firm would permit any unauthorized individuals to access its computer systems."*

Guidance #	Assessment Guidance
	See Preamble Comments #82-84 for a full discussion.
RG.3.3.1	This is generally interpreted to mean logical access, i.e. data separation, password protection, etc. Verify that Corporate INFOSEC policies are applied.
RG.3.3.2	This requirement does not apply unless the computerized system uses electronic signatures. If it does, refer to RG.14.* which covers rule section 11.300 and password controls.
RG.3.3.3	Verify that Corporate INFOSEC policies are applied.
RG.3.3.4	Verify that Corporate INFOSEC policies are applied.
RG.3.3.5	Verify that Corporate INFOSEC policies are applied.
RG.3.4	This requirement is typically "Not Applicable". *"The agency believes that these checks are warranted where only certain devices have been selected as legitimate sources of data input or commands....The device check would typically interrogate the source of the command to ensure that only the authorized workstation, and not some other device, was, in fact, issuing the command."* See Preamble Comment # 85. If the computerized system does not require device or terminal checks, then state in the "Notes" section that "All workstations are legitimate sources of data input." Examples of when device/terminal checks are appropriate include: • Console commands for a server are limited to the console station • Certain commands may be disallowed for RF devices vs. Terminals • Modem access may be verified to ensure the identity of the caller See Preamble Comment # 85 for a full discussion.
RG.4	One very important discussion to have around audit trails is that of the requirement for audit trails of changes made directly to data structure for "maintenance" or corrections. System administrators and DBA's typically make these changes. If these changes have audit trails, for example through the operating system level auditing features; you're OK. If those changes do not have audit trails, then procedural controls over use of such outside tools should be implemented to maintain data integrity. (If CCPI accepts that procedural control are sufficient.) See Preamble Comments # 72 - 78 for a full discussion.
RG.4.1	When assessing compliance, use the following questions: • Are audit trails secured at the "system administrator" level, i.e., not available as a user function? • Are audit trail records updatable manually in order to, for example, delete individual audit trail entries and compromise audit trail integrity? • Are audit trails capable of undetected add/change/delete by using the application software or application software-related maintenance utilities? • Are audit trails capable of undetected add/change/delete by using external tools (such as debuggers, database maintenance utilities, etc.)? See Preamble Comment #73.
RG.4.2	Does the computer system automatically generate and record the audit trail? *"To maintain audit trail integrity, the agency believes it is vital that the audit trail be created by the computer system independently of operators."* *"...audit trail information may be contained as part of the electronic record itself or as a separate record."* See Preamble Comment #73.
RG.4.3	The FDA expects both time and date stamps. Date and time recorded should be the user's local date/time. The units of time chosen should be "meaningful in terms of documenting human actions" for the process being controlled in order to create a meaningful audit trail of who did what, who changed what, and when it was done. For example, for a high-speed data acquisition system, it would be inappropriate to record the date, the hour and

Guidance #	Assessment Guidance
	the minute of an operator action. *"The element of time becomes vital to establishing an electronic record's trustworthiness and reliability."* (Preamble Comment #74.) See Preamble Comments #72 - #78.
RG.4.4	Consider the following points when assessing compliance: • *"It is the agency's intent that the audit trail provide a record of essentially who did what, who wrote what, and when."* (Preamble Comment #72.) • The Regulation is not intended to cover non-human "background" operations such as writing to a buffer or swap file; it is intended to assure the "integrity of human actions". (Preamble Comment #72.) • The audit trail entries should be made at the time the actions/operations are conducted. See Preamble Comment #72.) • Not every operator action (such as switching screens) requires an audit trail; however, limiting audit trails to only "critical" fields and/or operations does not thoroughly document events. See Preamble Comment #72. • *"The agency believes that, in general, the kinds of operator actions that need to be covered by an audit trail are those important enough to memorialize in the electronic record itself. These are actions which, for the most part, would be recorded in corresponding paper records according to existing recordkeeping requirements."* (Preamble Comment #72.) • *"The need for validating audit trails does not diminish the need for their implementation."* (Preamble Comment #73.) • *"The agency does not intend that new technologies, such as cryptographic technologies, will be needed to comply with this requirement."* (Preamble Comment #74.)
RG.4.4.1	Verify that record creation is logged.
RG.4.4.2	Verify that record modification is logged.
RG.4.4.3	Verify that maintenance (refreshing) record is logged.
RG.4.4.4	Verify that record deletion is logged.
RG.4.5	The intent of an audit trail is not met unless it is possible at some time in the future to re-create a previously recorded value that has been altered. For example, it should be possible to completely re-construct a deleted record to any point in time by only using the audit trail information. An audit trail should ideally record "before and after data" (or "delta" data in some cases) to ensure this traceability, though other means of reconstruction are also suitable. (See Preamble Comment #72.) *"All changes to existing records need to be documented, regardless of the reason, to maintain a complete and accurate history, to document individual responsibility, and to enable detection of record falsifications*." (Preamble Comment #76.)
RG.4.6	Audit trails should be covered as part of the records retention program for the computerized system.
RG.4.7	Same guidance as in RG.2.1 above.
RG.5	Consider the following when assessing compliance: *"The agency regards this requirement as fundamental to the proper operation of a facility...documentation of such training is also customary and not unreasonable."* (Preamble Comment #87.) • This requirement can be satisfied for internal persons if there are current, accurate job descriptions, training records, and a training procedure that is followed. Training in systems operation, database administration, application software administration, etc. is now considered part of GMP training. • For external persons, obtain or inspect their resume, training file, CV, job description, or other written documents. See Preamble Comments # 86 - 87 for a full discussion.
RG.5.1	Verify documentation as described in RG.5.

Guidance #	Assessment Guidance
	"The agency also disagrees with the assertion that personnel qualifications of system developers are irrelevant...Validation does not lessen the need for personnel to have the education, training, and experience to do their jobs properly. Indeed, it is highly unlikely that poorly qualified developers would be capable of producing a system that could be validated." (Preamble Comment #87.) *"...it is...vital that vendor personnel are likewise qualified to do their work."* (Preamble Comment #87.)
RG.5.2	Verify documentation as described in RG.5.
RG.5.3	Verify documentation as described in RG.5. *"The agency does not intend that to require that the check of personnel qualifications be performed automatically by a computer system itself (although such automation is desirable)."* (Preamble Comment #86.)
RG.6	Verify that Corporate INFOSEC policies are applied. Is there a written procedure that describes user responsibilities for use of computerized systems? Does it include: • Not sharing passwords, periodically changing passwords, not using easy-to-guess passwords? • Not installing unapproved software, running virus protection software? • User acceptance/approval in writing that acknowledges their understanding that violation of policy is the same as record falsification (i.e. forgery) and is subject to disciplinary action and possible personal criminal liability, etc.? *"There may be a general perception that electronic records and electronic signatures...are less significant and formal than traditional paper records and handwritten signatures."* (Preamble Comment #88.) *"Employees need to understand the gravity and consequences of signature or record falsification."* (Preamble Comment #88.) *"The agency considers the compromise of electronic signatures to be a very serious matter, one that should precipitate an appropriate investigation into any causative weaknesses in an organization's security controls."* (Preamble Comment #89.) *"...the presence of strong accountability and responsibility policies is necessary to ensure that employees understand the importance of maintaining the integrity of electronic records and signatures."* (Preamble Comment #88.) --*"...where one individual signs his or her name on behalf of someone else, the signature applied should be that of the delegatee, with some notation of the fact, and not the name of the delegator."* (Preamble Comment #91.) See Preamble Comments #88 - #91 for a full discussion.
RG.7	See Preamble Comments #92 and #93 for a full discussion.
RG.7.1	Note that the agency considers both the "positive" and "negative" aspects of this requirement. I.e. do the right people have the right systems documents and are the wrong people prohibited from seeing sensitive system documents? "Sensitive" document may include system hardware / software manuals, start up and disaster recovery procedures, investigation procedures and other such documents. Consider the following when assessing compliance: *"...it is important for employees to have correct and updated versions of standard operating and maintenance procedures"* [and manuals]. (Preamble Comment #92.) *"FDA does not agree that control over system documentation should only extend to security related software or to application or configurable software. Failure to control such documentation...could permit and foster records falsification by making the enabling instructions for these acts readily available to any individual."* (Preamble Comment #92.)
RG.7.1.1	Check the distribution lists, both formal and ad-hoc.
RG.7.1.2	Are sensitive document locked up?
RG.7.1.3	Do end-users typically use system administrator / DBA documents?
RG.7.2	This clause applies only to systems documentation that can be changed by individuals within CCPI. This clause means that requirements, design, test, and qualification specifications must be under some form of

Guidance #	Assessment Guidance
	configuration control during the time-sequenced development process. Note also that this implies (i.e. requires) that the systems actually used a time-sequenced development process (a.k.a. a systems development methodology). *"Where the documentation is in paper form, an audit trail of revisions need not be in electronic form. Where systems documentation is in electronic form, however, the agency intends to require the audit trail also be in electronic form..."* (Preamble Comment #93.)
	11.50: SIGNATURE MANIFESTATIONS
RG.9	Consider the following when assessing compliance: • Identify every display screen and report generated by the computerized system where an electronic signature is represented; each occurrence must be separately assessed for compliance. • The most important ones of these are the signature input screens. • *"FDA advises that the purpose of this section is not to protect against inaccurate entries, but to provide unambiguous documentation of the signer, when the signature was executed, and the signature's meaning."* (Preamble Comment #99.) • *"The agency intends that this section apply to all signed electronic records regardless of whether other regulations require them to be signed....Because signing information is important regardless of the type of signature used, the agency has revised 11.50 to cover all types of signings."* (Preamble Comment #100.) See Preamble Comments #98 - 106 for a full discussion.
RG.9.1	It is unacceptable to display other information, such as employee ID or user ID, as a substitute for the printed name of the signed. Verify that real names (first and last) are displayed. See Preamble Comment #102. *"Recording the meaning of the signature does not infer that the signer's credentials or other lengthy explanations be part of that meaning. The statement must merely show what is meant by the act of signing..."* (Preamble Comment #105.)
RG.9.2	*"...the signer's local time is the one to be recorded."* (Preamble Comment #101.) Guidance for this requirement is the same as for RG.4.3 and RG.4.4 above.
RG.9.3	*"The statement must merely show what is meant by the act of signing (e.g., review, approval, responsibility, authorship)"*. (Preamble Comment #105.)
	All items identified in 11.50 (a)(1), 11.50 (a)(2), and 11.50 (a)(3) (RG.9 - RG.9.3 above) shall be:
RG.9.4	• Subject to the same controls as for electronic records. [11.50 (b)]
RG.9.5	• Included as part of any human readable form of the electronic record (such as electronic display and/or printout or report). [11.50 (b)]
	11.70: SIGNATURE/RECORD LINKING
RG.10	What is the linking mechanism? It will almost certainly be some form of journal or audit trail applied at the database level. *"...because it is relatively easy to copy an electronic signature to another electronic record and thus compromise or falsify that record, a technology based link is necessary....The agency does not believe that procedural or administrative controls alone are sufficient."* (Preamble Comment #107.) *"The agency acknowledges that, despite elaborate system controls, certain determined individuals may find a way to defeat antifalsification measures...the agency's intent is to require measures that prevent electronic records falsification by ordinary means."* (Preamble Comment #108.) *"...in the traditional paper record, the signature remains bound to its corresponding record regardless of where the record may go."* (Preamble Comment #108.) The regulation does not require that electronic records be kept on inalterable media. It is required that all changes to an electronic record do not obscure the original entries. (See Preamble Comment #111.)

Guidance #	Assessment Guidance
	"...this section does not prohibit copies of handwritten signatures recorded electronically from being made for legitimate reasons that do not relate to record falsification." (Preamble Comment #111.) *"...FDA does not believe that cryptographic and digital signature methods would be the only ways of linking an electronic signature to an electronic document."* (Preamble Comment #112.) See Preamble Comments #107 - 113 for a full discussion.
	SUB-PART C: **ELECTRONIC SIGNATURES**
	GENERAL GUIDANCE FOR ELECTRONIC RECORDS
	11.100: GENERAL REQUIREMENTS FOR ELECTRONIC SIGNATURES
RG.11	
RG.11.1	Consider the following when assessing compliance: • Is there a policy or procedure explicitly stating that each assigned electronic signature is unique to one person? • Is there a policy or procedure that explicitly states that electronic signatures shall not be reused by or reassigned to anyone else? • -It is permissible for one person to have multiple e-sigs, so long as it is clearly established to whom each e-sig belongs. For example, one e-sig may indicate "review" while a separate esig may indicate "approval". *"Part 11 does not prohibit the establishment of a common group identification code/password for read only access. However, such commonly shared codes and passwords would not be regarded, and must not be used, as electronic signatures."* (Preamble Comment #114.) *"...electronic signatures are those of individual human beings and not organizations...FDA does not regard a corporate seal as an individual's signature. Humans may represent and obligate organizations by signing records..."* (Preamble Comment #116.) See Preamble Comments #114 - 116 for a full discussion.
RG.11.2	Consider this requirement met if: a) an employee has a currently valid Employee Number or other identification that allows access to the facility. b) a contract or temporary employee has been cleared by Security and/or Human Resources to enter the workplace. c) there is a policy or procedure ensuring that it is not possible for one person to falsely gain the electronic signature of another person. For example, if one person completes a request form using another person's name and there is no subsequent verification that the requester is the same as the electronic signature holder, then the former has gained the electronic signature of latter (even if both pass tests a) and b) above). *"...organizations [must] substantiate a person's identity to prevent impersonations...the agency disagrees with the assertion that this requirement is unnecessary."* (Preamble Comment #118.) *"The agency does not believe that the size of an organization, or global dispersion of its employees, is reason to abandon this vital control...Further, the agency does not accept the implication that multinational firms would not verify the identity of their employees as part of other routine procedures, such as when individuals are first hired."* (Preamble Comment #118.) See Preamble Comments #117 - 118 for a full discussion.
RG.11.3	A certification will be filed on behalf of CCPI by Corporate Regulatory Affairs.
RG.11.4	A certification will be filed on behalf of CCPI by Corporate Regulatory Affairs.
RG.11.5	A certification will be filed on behalf of CCPI by Corporate Regulatory Affairs.
	11.200: ELECTRONIC SIGNATURE COMPONENTS AND CONTROLS

Guidance #	Assessment Guidance
RG.12	See Preamble Comments #122 - 127 for a full discussion.
RG.12.1	Verify that Corporate INFOSEC policies are applied. Every electronic signature execution requires, at minimum, the contemporaneous execution of the identification code and password, except in the limited scenario in RG.12.2 below. The initial log on to the system also requires execution of the identification code and password. *"The agency believes that using a password alone...would clearly increase the likelihood that one individual, by chance or deduction, could enter a password that belonged to someone else and thereby...impersonate that individual."* (Preamble Comment #124.) The combination of these 2 components must be unique. Any possible combinations of this two-factor authentication method are permissible. (See Preamble Comment #125.) *"The agency cautions against using passwords that are common words easily associated with their originators..."* (Preamble Comment #130.) *"The agency advises that 'each signing' means each time an individual executes a signature...For example, in the case of a laboratory employee who performs a number of analytical tests...it is permissible for one signature to indicate the performance of a group of tests (21 CFR 211.194(a)(7))."* (Preamble Comment #126.)
RG.12.2	*"...an individual performs an initial system access or 'log on', which is effectively the first signing, by executing all components of the electronic signature...then performs subsequent signings by executing at least one component of the electronic signature, under controlled conditions..."* (Preamble Comment #124.) Recommend that the "password" component generally be the single signature component in these cases, since it is known only to the signer. *"...it is vital to have stringent controls in place to prevent...impersonation. Such controls include:* *(1) Requiring an individual to remain in close proximity to the workstation throughout the signing session; (2) use of automatic inactivity disconnect measures that would 'de-log' the first individual if no entries or actions were taken within a fixed short timeframe; and (3) requiring that the single component needed for subsequent signing be known to, and usable only by, the authorized individual."* (Prerambl Comment #124)
RG.12.3	*"The agency's concern here is the possibility that, if a person leaves the workstation, someone else could access the workstation and impersonate the legitimate signer by entering an identification code or password."* (Preamble Comment #124)
RG.12.4	Corporate INFOSEC Policies shall be applied. *"The agency does not believe that system administrators would routinely need to know an individual's password because they would have sufficient privileges to assist those users who forget their passwords."* (Preamble Comment # 123.) When resetting the account in some systems, this results in resetting the password to a "default" condition (for example, the same as the identification code or to some standard result such as "password"). This is acceptable when: • the system forces the user to change the password immediately upon log on using the "default" password • the time between resetting the password and the first user logon is required to be very short, so as to minimize the opportunity for records/signature falsification
RG.12.5	Consider the following when assessing compliance: In a system where the electronic signature is executed using an identification code and password, and where the identification codes are known or readily determined, it is unacceptable for anyone, including the system administrator, to know the password of any other person. Recommend that "back-door" system tools that can be used by a system administrator to falsify electronic records and/or electronic signatures be strictly controlled, through any combination of manual procedures, separation of duties, technology-based controls (such as check-in/check-out such software), or countermeasures (such as a system-level audit trail). Where adequate controls of this nature are in-place for system-level tools, consider the intent of the Regulation to be satisfied relative to back-door system tools. *"The agency advises that the intent of the collaboration provision is to require that the components of a nonbiometric electronic signature cannot be used by one individual without the prior knowledge of a second individual. One type of situation the agency seeks to prevent is the use of a component such as a card or token*

Guidance #	Assessment Guidance
	that a person may leave unattended." (Preamble comment #127.) *"...the agency would consider as falsification the act of substituting the signature of a supervisor for that of a subordinate. The electronic signature of the subordinate must remain inviolate...Although supervisors may overrule the actions of their staff, the electronic signatures of the subordinates must remain a permanent part of the record, and the supervisor's own electronic signature must appear separately."* (Preamble Comment #127.)
RG.13	**Electronic Signatures Based On Biometrics**
RG.13.1	• Electronic records based upon biometrics shall be designed to ensure that they cannot be used by anyone other than their genuine owners. [11.200 (b)] Consider the following when assessing compliance: --The key word is "designed". The agency believes that a properly designed and implemented biometric-based electronic signature system makes it highly unlikely that any electronic signature could be falsified. *"The agency notes that the rule does not require the use of biometric-based electronic signatures."* (Preamble Comment #128.)
	11.300: CONTROLS FOR IDENTIFICATION CODES/PASSWORDS
RG.14	See Preamble Comments # 129 - 138 for a full discussion.
RG.14.1	Verify that Corporate INFOSEC policies are applied.
RG.14.2	Verify that Corporate INFOSEC policies are applied. Consider the following when assessing compliance: • --Does any part of the computerized system contain functionality that requires users to periodically revise their passwords, such as password aging? • Is there a manual procedure that requires users or system administrators to manually expire or revise their passwords? If so, is there an auditing procedure to ensure that the procedure is followed? • *"FDA disagrees that this system control is unnecessary or impractical in large organizations..."* (Preamble Comment # 131.) • Password expiration is not the only reason or method for recalling, revising, or checking issuances. • --*"If, for example, identification codes and passwords have been copied or compromised, they should be changed."* (Preamble Comment #131.)
RG.14.3	Verify that Corporate INFOSEC policies for ID badges are applied.
RG.14.3.1	Verify that Corporate INFOSEC policies for ID badges are applied.
RG.14.3.2	Verify that Corporate INFOSEC policies for ID badges are applied. *"FDA uses the term 'rigorous' because device disappearance may be the result of inadequate controls over the issuance and management of the original cards or devices, thus necessitating more stringent measures to prevent problem recurrence."* (Preamble Comment #132.)
RG.14.4	Does the system have transaction-level safeguards?
RG.14.4.1	Consider the following when assessing compliance: • --Is there a procedure or system function that revokes sign-on privileges when an incorrect combination of identification code and password is repeatedly entered? • Has testing been conducted to ensure that "inactive" user accounts cannot be activated by unauthorized persons? • Are there procedures and appropriate training to assure that users understand that passwords are not to be shared and the serious consequences of such actions? • *"The agency considers attempts at unauthorized use of identification codes and passwords to be extremely serious..."* (Preamble Comment #133.) • *"The agency's security concerns extend to system as well as record access."* (Preamble Comment #135.)
RG.14.4.2	Consider the following when assessing compliance:

Guidance #	Assessment Guidance
	• Does the computerized system contain any functionality to detect and report possible unauthorized use of the system? • "The agency advises that a simple typing error may not indicate an unauthorized use attempt, although a pattern of such errors, especially in short succession... could signal a security problem that should not be ignored". (Preamble Comment #134.)
RG.14.4.3	Consider the following when assessing compliance: • Is there a procedure or system function that specifies the conditions under which a security alert should be communicated to management? • Does the computerized system generate an email or a security log file to be reviewed by the system security group when attempts at unauthorized use are made? • Is there a procedure that describes the security group's responsibility and required activities when notified of possible security breaches? • Is there a procedure that requires the security group to periodically monitor all computerized systems covered under Part 11 and determine if any security breaches have occurred? *"In FDA's view, the significance of such attempts requires the immediate and urgent attention of appropriate security personnel in the same manner that individuals would respond to a fire alarm." (Preamble Comment #133.)* *"The agency believes that the same technology that accepts or rejects an identification code and password can be used to relay to security personnel an appropriate message regarding attempted misuse." (Preamble Comment # 133.)* *"If this section were removed, falsifications would be more probable to the extent that some establishments would not alert security personnel." (Preamble Comment #135.)* *"The agency agrees that not every misuse attempt would have to be reported simultaneously to an organization's management if the security unit...responded appropriately. FDA notes, however, that some apparent security breaches could be serious enough to warrant management's immediate and urgent attention." (Preamble Comment #137.)*
RG.14.5	• Consider the following when assessing compliance: --Is there a procedure that requires both initial and periodic testing of these devices to assure that no unauthorized modifications have been made, and that the device continues to function as-designed despite wear and tear? *"Testing for system access alone could fail to discern significant unauthorized device alterations. If , for example, a device has been modified to change the identifying information, system access may still be allowed, which would enable someone to assume the identity of another person."(Preamble Comment #138.)* *"Because validation of electronic signature systems would not cover unauthorized device modifications, or subsequent wear and tear, validation would not obviate the need for periodic testing." (Preamble Comment #138.)*

OBSERVATIONS AND RECOMMENDATIONS:

OBS/ REC #	Require-ment #	Observation / Recommendation