Release Considerations

This document was developed by Cerner Corporation to support our clients who conduct clinical research. It is limited to health care regulations/requirements in the United States and specific to the requirements of an FDA research regulation (21CFR Part 11). It is intended for use by health care organizations using Cerner's electronic health record (EHR) system and may not be reproduced or used by other entities without the express written consent of Cerner.

Comparison of 21 CFR Part 11 to standards/requirements for healthcare systems/processes

Note

See 21 CFR Part 11 Compliance Matrix Detailed for a printable version of this matrix.

21 CFR Part 11 ("part 11") of the United States Code of Federal Regulations outlines requirements for electronic systems/processes used by FDA-regulated entities. While the FDA has clearly stated that they will not audit electronic health record (EHR) systems/processes for compliance with part 11, and that oversight of EHRs is out of their jurisdiction (as stated in draft guidance Use of Electronic Health Record Data in Clinical Investigations), research sponsors may inquire about a site's compliance with part 11 requirements. Research sponsors may have additional requirements based on their interpretation of FDA regulatory guidance documents such as the 2007 Guidance for Industry Computerized Systems Used in Clinical Investigations (CSUCI). Guidance documents do not establish legally enforceable responsibilities but instead provide suggestions and recommendations based on the FDA's thinking at the time.

Recognizing that sites may choose different approaches for responding to sponsor inquiries, Cerner has created a matrix to crosswalk part 11 requirements to healthcare standards/requirements for healthcare systems/processes.The matrix is designed to facilitate easy documentation of the site's chosen approach:

- For sites compelled to claim compliance with part 11, the matrix is designed to support site-specific assessment.
- For sites choosing not to claim compliance with part 11, the matrix highlights the robust controls inherent in EHR systems/processes.
  In the matrix below, part 11 controls are identified in column 1; technical capabilities/controls provided by the Cerner system are identified in column 2; and validation, procedural and administrative activities performed by the site are identified in column 3.

Tip

See 21 CFR Part 11 Compliance Matrix for Millennium Summary for a Summary view of the matrix.

Legend for matrix color-coding:

ISO Quality System Management standards (Cerner's certification) or standard system capabilities
Health Information Portability and Accountability Act (HIPAA) security control standards (enforcement by the Office of Civil Rights (OCR)
Office of the National Coordinator (ONC) technology certification (Cerner) 2015 edition, and Centers for Medicaid and Medicare Services (CMS) implementation attestation (site) for Meaningful Use Stage 3
The Joint Commission (TJC) standards
Site validation activities not otherwise addressed in the above standards/requirements

	Regulation	Technical Controls (provided by the Cerner system)	Procedural and Administrative Controls (implemented by the site)
	Part B Electronic Records		

	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.	Cerner tests its software, both from a verification and validation perspective, prior to delivery to the client.	The site is expected to perform functional validation of the installed system based on their intended use and the site's individual database settings and environmental parameters. Cerner will provide Certification Guidelines to aid the client in this process, and each client should tailor and amend these Certification Guidelines according to their site-specific parameters and processes.
		Cerner's quality management system is ISO 9001:2008 certified Cerner's ISO certification demonstrates the implementation of quality controls that include processes for validation of systems to ensure accuracy, reliability, consistent intended performance and the ability to discern invalid or altered records.	
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.	Cerner Millennium has the ability to produce copies of records in human-readable form for printing and on-line viewing.	The site is expected to implement system capabilities in compliance with site policies and procedures for generating accurate and complete copies of records in both human readable and electronic form suitable for inspection, review, and copying by the agency.

c	Protection of records to enable their accurate and ready retrieval throughout the records retention period.	**HIPAA Compliance (enforcement by the Office of Civil Rights)**
		Cerner Millennium enables the storage and retrieval of records and ensures record protection through technical safeguards defined in 45 CFR 164.312 which include:
		• Access control
		  • Unique user identification
		  • Emergency access procedure
		  • Automatic logoff
		  • Encryption and decryption
		• Audit controls
		• Integrity
		  • Mechanism to authenticate electronic Protected Health Information (PHI)
		• Person or entity authentication
		• Transmission security
		  • Integrity controls
		  • Encryption
			HIPAA Compliance: (Enforcement by the Office of Civil Rights)
			In compliance with HIPAA, the site is expected to ensure Administrative and Physical safeguards are implemented.
			Administrative safeguards (per 45 CFR 164.308) include:
			• Security management process
			  • Risk analysis
			  • Risk Management
			  • Sanction policy
			  • Information system activity review
			  • Assigned security responsibility
			  • Workforce security
			  • Authorization and/or supervision
			  • Workforce clearance procedure
			  • Termination procedures
			  • Information access management
			  • Access authorization
			  • Access establishment and modification
			  • Security awareness and training
			  • Security reminders
			  • Protection from malicious software
			  • Log-in monitoring
			  • Password management
			  • Security incident procedures
			  • Response and reporting
			  • Contingency plan
			  • Data backup plan
			  • Disaster recovery plan
			  • Emergency mode operation plan
			  • Testing and revision procedure
			  • Application and data criticality analysis
			  • Evaluation
			  • Business associate contracts and other arrangement
			  • Written contract or other arrangementPhysical safeguards (per CFR164.310) include:
			• Facility access controls
			  • Contingency operations
			  • Facility security plan
			  • Access control and validation procedures
			  • Maintenance records
			  • Workstation use
			  • Workstation security
			  • Device and media controls
			  • Disposal
			  • Media re-use
			  • Accountability
			  • Data backup and storage

		ONC-ACB certification: For those of Cerner's solutions that are noted as ONC-ACB Certified on the ONC Certified Product List, that EHR technology has been subject to testing of its capabilities for protecting electronic health information created or maintained by the EHR technology. Most of the certified product listings pertain to PowerChart and FirstNet. The Standards Criteria includes a requirement that *the date, time, patient identification and user identification must be recorded when electronic health information is created, modified, accessed, or deleted; and an indication of which action(s) occurred and by whom must also be recorded* (45 CFR 170.210 (e)). The Certification Criteria (45 CFR 170.315) includes requirements to demonstrate: • Access control (45 CFR 170.315 (d)(1)) • Automatic log-off (45 CFR 170.315 (d)(5)) • Audit log (45 CFR 170.315 (d)(2)) • Integrity (45 CFR 170.315 (d)(8)) • Authentication (45 CFR 170.315 (d)(1))	**Addressed by Meaningful Use Stage 3 Objectives and Measures (site attestation to CMS)** To meet Objective 1 regarding Protection of Electronic Health Information, sites must attest that they have conducted or reviewed a security risk analysis in accordance with the requirements under 45 CFR 164.308 (a)(1), and implemented security updates as necessary and corrected identified security deficiencies.
			The Joint Commission Accreditation program for healthcare organizations: Protection of records to enable their accurate and ready retrieval throughout the records retention period is addressed in Joint Commission standards for *Information Management (IM)* and *Record of Care, Treatment and Services (RC)*

d	Limiting system access to authorized individuals.	**HIPAA Compliance (enforced by the Office of Civil Rights)** Cerner Millennium provides the technical safeguards (per 45 CFR 164.312) to limit system access to authorized individuals. Relevant capabilities include: • Ability to create, maintain and apply the roles, access permissions and capabilities of each user that accesses the system, such that users have access only to those system features and functions to which they have been granted access • Ability to limit the number of log-in attempts and record unauthorized access log-in attempts • Ability to enforce password or other access keys to be changed at established intervals • Ability to automatically log off users after a period of inactivity	**HIPAA Compliance (enforced by the Office of Civil Rights)** In compliance with HIPAA, the site is expected to implement Administrative and Physical safeguards per 45 CFR 164.308 and 45 CFR 164.310 to ensure system access is limited to authorized users. Administrative safeguards include: • Implementation of security management policies and procedures to include risk analysis, risk management, sanction policy and information system activity review • Designation of a security official responsible for the development and implementation of policies and procedures • Implementation of workforce security policies and procedures that address authorization, workforce clearance and termination procedures • Implementation of information access management policies and procedures for granting and modifying user access to the system • Implementation of a workforce security awareness and training policies and procedures that address security reminders, protection from malicious software, log-in monitoring and password management • Implementation of security incident policies and procedures for responding to and reporting suspected or known security incidents Physical safeguards include: • Implementation of facility access policies and procedures to address contingency operations, facility security, access control and validation procedures and facility maintenance records • Implementation of policies and procedures for workstation use and workstation security • Implementation of device and media policies and procedures to address disposal, re-use, accountability and data back-up and storage
		ONC-ACB certification: For those of Cerner's solutions that are noted as ONC-ACB Certified on the ONC Certified Product List, that EHR technology has been subject to testing of its capabilities for protecting electronic health information created or maintained by the EHR technology. Most of the certified product listings pertain to PowerChart and FirstNet. The Standards Criteria includes a requirement that *the date, time, patient identification and user identification must be recorded when electronic health information is created, modified, accessed, or deleted; and an indication of which action(s) occurred and by whom must also be recorded* (45 CFR 170.210 (e)). The Certification Criteria specific to Access Control [45 CFR 170.315 (d)(1)] requires the assignment of a unique name and/or number for identifying and tracking user identity and establishment of controls that permit only authorized users to access electronic health information.	**Addressed by Meaningful Use Stage 3 Objectives and Measures (site attestation to CMS):** Meaningful use includes an Objective to *protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical, administrative, and physical safeguards*. To meet Objective 1 regarding Protection of Electronic Health Information, sites must attest that they have conducted or reviewed a security risk analysis in accordance with the requirements under 45 CFR 164.308 (a)(1) and implemented security updates as necessary and corrected identified security deficiencies.
			The Joint Commission Accreditation program for healthcare organizations: Limiting system access to authorized individuals is addressed in Joint Commission standards for *Information Management (IM)* and *Record of Care, Treatment and Services (RC)*

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.	**HIPAA Compliance (enforced by the Office of Civil Rights)** Cerner Millennium provides the technical safeguard audit controls (per CFR 164.312) to produce secure, computer-generated time-stamped audit trails to independently record the date, time and author of any data creation, change or deletion. New audit trail information does not overwrite previous information. Audit log information is retained with the record and accessible to authorized users.	**HIPAA Compliance (enforced by the Office of Civil Rights)** In compliance with HIPAA, the site is expected to ensure audit control capabilities are implemented, records are maintained and access is granted to authorized users in accordance with system access policies and procedures.
		ONC-ACB certification: For those of Cerner's solutions that are noted as ONC-ACB Certified on the ONC Certified Product List, that EHR technology has been subject to testing of its capabilities for protecting electronic health information created or maintained by the EHR technology. Most of the certified product listings pertain to PowerChart and FirstNet. The Standards Criteria includes a requirement that *the date, time, patient identification and user identification must be recorded when electronic health information is created, modified, accessed, or deleted; and an indication of which action(s) occurred and by whom must also be recorded* (45 CFR 170.210 (e)). The Certification Criteria specific to Audit Log [45 CFR 170.315 (d)(2)] requires the recording of actions related to electronic health information in accordance with the standard specified in 45 CFR 170.210 (e) and enabling the user to generate an audit log for a specific time period and to sort entries in the audit log according to any of the elements specified in the standard at 170.210 (e).	**Addressed by Meaningful Use Stage 3 Objectives and Measures (site attestation to CMS):** Meaningful use includes an Objective to *protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical, administrative, and physical safeguards*. To meet Objective 1 regarding Protection of Electronic Health Information, sites must attest that they have conducted or reviewed a security risk analysis in accordance with the requirements under 45 CFR 164.308 (a)(1) and implemented security updates as necessary and corrected identified security deficiencies.
f	Use of operational system checks to enforce permitted sequencing of steps and events, as appropriate.	Cerner Millennium provides operational system check capabilities to enforce permitted sequencing of steps and events, as appropriate.	Sites configure and validate appropriate operational system checks during implementation. (addressed under system validation checks above)
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.	**HIPAA Compliance (enforced by the Office of Civil Rights)** Cerner Millennium provides the technical safeguards (per 45 CFR 164.312) to limit system access to authorized individuals. Capabilities relevant to authority checks include the ability to create, maintain and apply the roles, access permissions and capabilities of each user that accesses the system, such that users have access only to those system features and functions to which they have been granted access	**HIPAA Compliance (enforced by the Office of Civil Rights)** In compliance with HIPAA, the site is expected to ensure access control capabilities (including authority checks) are implemented, records are maintained and access is granted to authorized users in accordance with system access policies and procedures.

		ONC-ACB certification: For those of Cerner's solutions that are noted as ONC-ACB certified on the ONC Certified Product List, that EHR technology has been subject to testing of its capabilities for protecting electronic health information created or maintained by the EHR technology. Most of the certified product listings pertain to PowerChart and FirstNet. The Standards Criteria includes a requirement that *the date, time, patient identification and user identification must be recorded when electronic health information is created, modified, accessed, or deleted; and an indication of which action(s) occurred and by whom must also be recorded* (45 CFR 170.210 (e)). The Certification Criteria specific to Access Control (45 CFR 170.315 (d)(1))requires the assignment of a unique name and/or number for identifying and tracking user identity and establishment of controls that permit only authorized users to access electronic health information.	**Addressed by Meaningful Use Stage 3 Objectives and Measures (site attestation to CMS):** Meaningful use includes an Objective to *protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical, administrative, and physical safeguards*. To meet Objective 1 regarding Protection of Electronic Health Information, sites must attest that they have conducted or reviewed a security risk analysis in accordance with the requirements under 45 CFR 164.308 (a)(1) and implemented security updates as necessary and corrected identified security deficiencies.
h	Use of device (e.g., terminal) checks to determine, as appropriate, the validity of the source of data input or operational instruction, as appropriate.	**HIPAA Compliance (enforced by the Office of Civil Rights)** Cerner Millennium provides the technical safeguards (per 45 CFR 164.312) to limit system access to authorized individuals. Capabilities relevant to authority checks include the ability to create, maintain and apply the roles, access permissions and capabilities of each user that accesses the system, such that users have access only to those system features and functions to which they have been granted access	**HIPAA Compliance (enforced by the Office of Civil Rights)** In compliance with HIPAA, the site is expected to ensure access control capabilities (including authority checks) are implemented, records are maintained and access is granted to authorized users in accordance with system access policies and procedures.

		ONC-ACB certification: For those of Cerner's solutions that are noted as ONC-ACB certified on the ONC Certified Product List, that EHR technology has been subject to testing of its capabilities for protecting electronic health information created or maintained by the EHR technology. Most of the certified product listings pertain to PowerChart and FirstNet. The Standards Criteria includes a requirement that *the date, time, patient identification and user identification must be recorded when electronic health information is created, modified, accessed, or deleted; and an indication of which action(s) occurred and by whom must also be recorded* (45 CFR 170.210 (e)). The Certification Criteria specific to Access Control [45 CFR 170.315 (d)(1)] requires the assignment of a unique name and/or number for identifying and tracking user identity and establishment of controls that permit only authorized users to access electronic health information.	**Addressed by Meaningful Use Stage 3 Objectives and Measures (site attestation to CMS):** Meaningful use includes an Objective to *protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical, administrative, and physical safeguards*. To meet Objective 1 regarding Protection of Electronic Health Information, sites must attest that they have conducted or reviewed a security risk analysis in accordance with the requirements under 45 CFR 164.308 (a)(1) and implemented security updates as necessary and corrected identified security deficiencies.
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.	**Cerner is ISO 9001:2008 Quality Management System certified** Section 6.2.2 of ISO 9001:2008 requirements validates that persons who develop and maintain Cerner Millennium have the education, training and experience to perform their assigned tasks. ISO 9001:2008 Section 6.2.2 specifies requirements for “Competence, Training and Awareness”:* Organization must identify the training needed for each job or task, and review the gap between the people who perform the job to the requirements.* Provide the required training to the people if there is a gap. • To review and evaluate the people after training provided to ensure the effectiveness of training. • People must be aware and understand the importance of how their activities can contribute to the achievement of quality objectives. • Training records, evaluation records must be maintained according to ISO 9001 requirements.	Sites must implement policies and procedures to ensure persons who maintain or use the EHR have the education, training and experience to perform their assigned tasks.

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.	**HIPAA Compliance (enforced by the Office of Civil Rights)** Cerner Millennium provides the technical safeguards (per 45 CFR 164.312) to limit system access to authorized individuals. Relevant capabilities include: • Ability to create, maintain and apply the roles, access permissions and capabilities of each user that accesses the system, such that users have access only to those system features and functions to which they have been granted access • Ability to limit the number of log-in attempts and record unauthorized access log-in attempts • Ability to enforce password or other access keys to be changed at established intervals • Ability to automatically log off users after a period of inactivity	**HIPAA Compliance (enforced by the Office of Civil Rights)** In compliance with HIPAA, the site is expected to implement Administrative and Physical safeguards per 45 CFR 164.308 and 45 CFR 164.310 to ensure system access is limited to authorized users. Administrative safeguards include: • Implementation of security management policies and procedures to include risk analysis, risk management, sanction policy and information system activity review • Designation of a security official responsible for the development and implementation of policies and procedures • Implementation of workforce security policies and procedures that address authorization, workforce clearance and termination procedures • Implementation of information access management policies and procedures for granting and modifying user access to the system • Implementation of a workforce security awareness and training policies and procedures that address security reminders, protection from malicious software, log-in monitoring and password management • Implementation of security incident policies and procedures for responding to and reporting suspected or known security incidents Physical safeguards include: • Implementation of facility access policies and procedures to address contingency operations, facility security, access control and validation procedures and facility maintenance records • Implementation of policies and procedures for workstation use and workstation security • Implementation of device and media policies and procedures to address disposal, re-use, accountability and data back-up and storage
		ONC-ACB certification: For those of Cerner's solutions that are noted as ONC-ACB certified on the ONC Certified Product List, that EHR technology has been subject to testing of its capabilities for protecting electronic health information created or maintained by the EHR technology. Most of the certified product listings pertain to PowerChart and FirstNet. The Standards Criteria includes a requirement that *the date, time, patient identification and user identification must be recorded when electronic health information is created, modified, accessed, or deleted; and an indication of which action(s) occurred and by whom must also be recorded* (45 CFR 170.210 (e)). The Certification Criteria specific to Access Control [45 CFR 170.315 (d)(1)] requires the assignment of a unique name and/or number for identifying and tracking user identity and establishment of controls that permit only authorized users to access electronic health information.	**Addressed by Meaningful Use Stage 3 Objectives and Measures (site attestation to CMS):** Meaningful use includes an Objective to *protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical, administrative, and physical safeguards*. To meet Objective 1 regarding Protection of Electronic Health Information, sites must attest that they have conducted or reviewed a security risk analysis in accordance with the requirements under 45 CFR 164.308 (a)(1) and implemented security updates as necessary and corrected identified security deficiencies.
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.	**Cerner is ISO 9001:2008 Quality Management System certified** Section 4.2.3 of ISO 9001:2008 validates Cerner's implementation of adequate controls over the distribution of, access to and use of documentation for operation and maintenance to ensure:* controlled documents obtain approval before release and distribution to other.* any new revision of documents have been reviewed and approved before release and distribution to other. • the revision of document is properly identified. • relevant version of documents are available to retrieve at point of use. • documents remain legible. • all external documents determined by organization follow the same control processes. • any old version of documents are obsolete to prevent the unintended use	Sites must implement policies and procedures to ensure 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.	**Cerner is ISO 9001:2008 Quality Management System certified** Sections 4.2.3 of ISO 9001:2008 validates Cerner's implementation of revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documentation to ensure:* controlled documents obtain approval before release and distribution to other.* any new revision of documents have been reviewed and approved before release and distribution to other. • the revision of document is properly identified. • relevant version of documents are available to retrieve at point of use. • documents remain legible. • all external documents determined by organization follow the same control processes. • any old version of documents are obsolete to prevent the unintended use	Sites must ensure implementation of revision and change control procedures to maintain an audit trail that documents time-sequenced modification of systems documentation.
	11.30 Controls for open systems.	From a system development perspective, software code for Cerner Millennium is not based on open source code. It is developed in a closed environment that is secure, controlled and limited to Cerner-authorized/trained developers working within the framework of Cerner's ISO 9001 certified quality management system.	Sites must determine if their implementation and use of the EHR system within the scope of research is open or closed. Consideration of the system from the perspective of an EHR environment in which system access is controlled by persons responsible for the content of electronic records in the system might support this determination. Closed System or Open System

		The interpretation of requirements for electronic signatures is variable across use cases and jurisdictions. Cerner Millennium provides robust controls to ensure authenticity, integrity and confidentiality of data and also supports the secure interchange of health information with technical capabilities including access control, audit logs, authentication and encryption/decryption. **ONC-ACB certification:** For those of Cerner's solutions that are noted as ONC-ACB certified on the ONC Certified Product List, that EHR technology has been subject to testing of its capabilities for protecting electronic health information created or maintained by the EHR technology. Most of the certified product listings pertain to PowerChart and FirstNet. The Standards Criteria includes requirements under 45 CFR 170.210 specific to access control, audit logs, integrity: • Record actions related to electronic health information • Verification that electronic health information has not been altered in transit • Encryption and decryption of electronic health information The Certification Criteria (45 CFR 170.315) includes requirements to demonstrate: • Access control (45 CFR 170.315 (d)(1)) • Automatic log-off (45 CFR 170.315 (d)(5)) • Audit log (45 CFR 170.315 (d)(2)) • Integrity (45 CFR 170.315 (d)(8)) • Authentication (45 CFR 170.315 (d)(1))	The interpretation of requirements for electronic signatures is variable across use cases and jurisdictions. CMS requirements for Meaningful Use include procedures and controls to ensure authenticity, integrity and confidentiality of data. **Supported by Meaningful Use Stage 3 Objectives and Measures (site attestation to CMS):** Meaningful use includes an Objective to *protect electronic health information created or maintained by the certified EHR technology through the implementation of appropriate technical, administrative, and physical safeguards*. To meet Objective 1 regarding Protection of Electronic Health Information, sites must attest that they have conducted or reviewed a security risk analysis in accordance with the requirements under 45 CFR 164.308 (a)(1) and implemented security updates as necessary and corrected identified security deficiencies.
	Procedures and controls to ensure authenticity, integrity, and as appropriate, confidentiality. Include additional measures beyond 11.10 requirements such as document encryption and use of digital signature standards.		
	11.50 Signature manifestations		
a	Signed electronic records contain the following information associated with the signing: (1) Name (2) Date and time (3) Meaning (author, review, approval)		

b	Readable forms of electronic records are to include the information as defined in item 11.50.a concerning signers.		
	11.70 Signature linking		
a	Electronic and handwritten signatures executed to electronic records shall; be linked to ensure they cannot be excised, copied, or otherwise transferred.		
	Part C Electronic Signatures		
	11.100 General requirements.		
a	Electronic signatures shall be unique and not reused or reassigned.		
b	Individual verified before assigned electronic signature authority.		
c	Certify in writing to the agency that the electronic signatures are intended to be the legally binding equivalent of handwritten signatures.		
	11.200 Electronic signature components and controls.		
a	Electronic signatures not based on biometric links:		
	(1) Employ two distinct identification components.		
	(i) First electronic signature executes all components of the electronic signature, subsequent signings use at least one component.		
	(ii) When electronic signature not executed during continuous period, all components of the electronic signature shall be used.		
	(2) Used only by their genuine owner.		
	(3) Collaboration of two or more individuals required to prevent use by other than the genuine owner.		

- Cerner is ISO 9001:2008 Quality System Management certified. For for information on ISO 9000 certification see, ISO 9000 Quality Management.
- Cerner EHR systems have been certified for Meaningful Use by the Certification Commission for Health Information Technology (CCHIT®). For more information on Meaningful Use CCHIT Certification, see CCHIT ONC Certification.
- For more information on Meaningful Use Core Measure for the Objective to *Protect Electronic Health Information*, see CMS- Protect Electronic Health Information .

Release Considerations

This document was developed by Cerner Corporation to support our clients who conduct clinical research. It is limited to health care regulations/requirements in the United States and specific to the requirements of an FDA research regulation (21CFR Part 11). It is intended for use by health care organizations using Cerner's electronic health record (EHR) system and may not be reproduced or used by other entities without the express written consent of Cerner.

Note

Reference to the FDA's statement that the FDA does not intend to assess the compliance of EHRs with Part 11 can be found on page 8 of the eSource guidance, Guidance for Industry: Electronic Source Data in Clinical Investigations.

Note

A recorded presentation, 21CFR Part 11: A new matrix document for Cerner clients Illumination, that discusses these matrix documents can be found on Cerner.com.

This page includes links to external resources. These resources are provided for reference purposes and should be used with caution. Contact your Cerner support team for more information about third-party content.