MentorHealth

Live Webinar
on

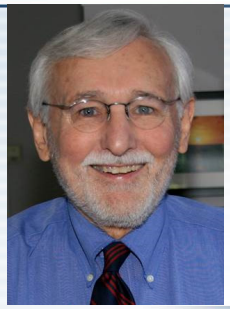
How Does Compliance with 21 CFR Part 11 Ensure Data Integrity & Subject Safety in Clinical Research

Wednesday, 19 June 2013 at 10:00 AM PST / 01:00 PM EST

By ***Charles H. Pierce****, MD, PhD, FCP, CPI*

This Webinar is Brought to you by MentorHealth

Electronic Data Processing 21 CFR Part 11



Charles H. Pierce, MD, PhD, FCP, CPI
Medical Director, Investigator
Metabolic and Atherosclerotic Research Center - Medpace
Cincinnati, Ohio

The Key is Universal Acceptance

21 CFR Part 11

Part 11 Electronic Records; Electronic Signatures

- Subpart A - General Provisions
  - 11.1 Scope
  - 11.2 Implementation
  - 11.3 Definitions
- Subpart B - Electronic Records
  - 11.10 Controls for Closed Systems
  - 11.30 Controls for Open Systems
  - 11.50 Signature manifestations
  - 11.70 Signature / Record Linking
- Subpart C Electronic Signatures

21 CFR Part 11

Part 11 Electronic Records; Electronic Signatures

- Subpart A - General Provisions
- Subpart B - Electronic Records
  - 11.10 Controls for closed systems
  - 11.30 Controls for open systems
  - 11.50 Signature manifestations
  - 11.70 Signature / record linking
- Subpart C Electronic Signatures
  - 11.100 General requirements
  - 11.200 Electronic signature components and controls
  - 11.300 Controls for identification codes / passwords

www.mentorhealth.com 5

Title 21 Code of Federal Regulations

Part 11 Discussion Points

- Scope of the Regulation
- Definition of Terms
- Computerized Systems
- Closed Systems and Their Controls
- Internal Audit Questions
- Open Systems and Their Controls
- Electronic Signatures
- Standard Operating Procedures

www.mentorhealth.com 6

The Scope of Part 11

"Regulations in this part set forth the criteria under which the agency considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be:

- Trustworthy and Reliable and
- Generally equivalent to paper records and handwritten signatures executed on paper"

Ref: **21 CFR Part 11.1(a)**

"Electronic Record" defined

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

Ref: **21 CFR Part 11.3(b)(6)**

Traditional vs. Electronic Record

It is important to know the difference between an electronic record and the paper one

- In a traditional paper (*typewriter*) record system, the information, or data content, is recorded directly onto a stable medium, such as paper. The paper record is the original form of the document and is considered trustworthy.
- **A paper printout of an e-record is NOT a traditional paper record. …**

www.mentorhealth.com 9

Traditional vs. Electronic Record

A paper printout of an electronic-record is NOT a traditional paper record. …

- With electronic records, the document is created electronically, and the content, context and structure can easily be altered by using or abusing the computing technologies required to create them .
- **When a paper print out is generated from an e-*record*, the e-*record* controls and determines the content, trustworthiness and reliability of the paper record.**

www.mentorhealth.com 10

A Computerized System

Is an electronic system that is used to create, modify, maintain, archive, retrieve or transmit information in digital form.

- Validation of the system is a prerequisite for establishing reliable and trustworthy computing bases for an organization."
- ***Validation*** **is "Confirmation by examination and provision of objective evidence that the computer system specifications conform to user needs and intended uses and that all requirements can be consistently fulfilled."**

www.mentorhealth.com 11

The Computerized System:

- **Hardware** (servers, desktops, laptops, scanners, printers, recorders etc.)
- **Software** (developed in-house or commercially developed and acquired)
- **Associated Documents** (user manuals, etc.)
- **Network Architecture** (ties the system together including whether hardwired or wireless)
- **Training** (documentation of training so all staff know… how to use the system)

www.mentorhealth.com 12

The "System" defined

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

Ref: **21 CFR Part 11.3(b)(4)**

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

Ref: **21 CFR Part 11.3(b)(9)**

www.mentorhealth.com 13

Subpart B
Closed System Controls

MentorHealth

www.mentorhealth.com 14

Closed System:

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

  Ref: **21 CFR Part 11.3(b)(4)**

- Dial-in access over public communication routes could be considered part of a closed system, but additional security measures are needed (e.g. security cards).

www.mentorhealth.com 15

21 CFR Part 11 Subpart B

Part 11 Electronic Records; Electronic Signatures

- Subpart B - Electronic Records
  - 11.10 **Controls for Closed Systems**
  - 11.30 Controls for Open Systems
  - 11.50 Signature manifestations
  - 11.70 Signature / Record Linking

www.mentorhealth.com 16

Part 11 Subpart B - Controls

Is it possible to discern invalid or altered records

Ref: **21 CFR 11.10**

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

Ref: **21 CFR 11.10(a)**

www.mentorhealth.com 17

Part 11 Subpart B - Controls

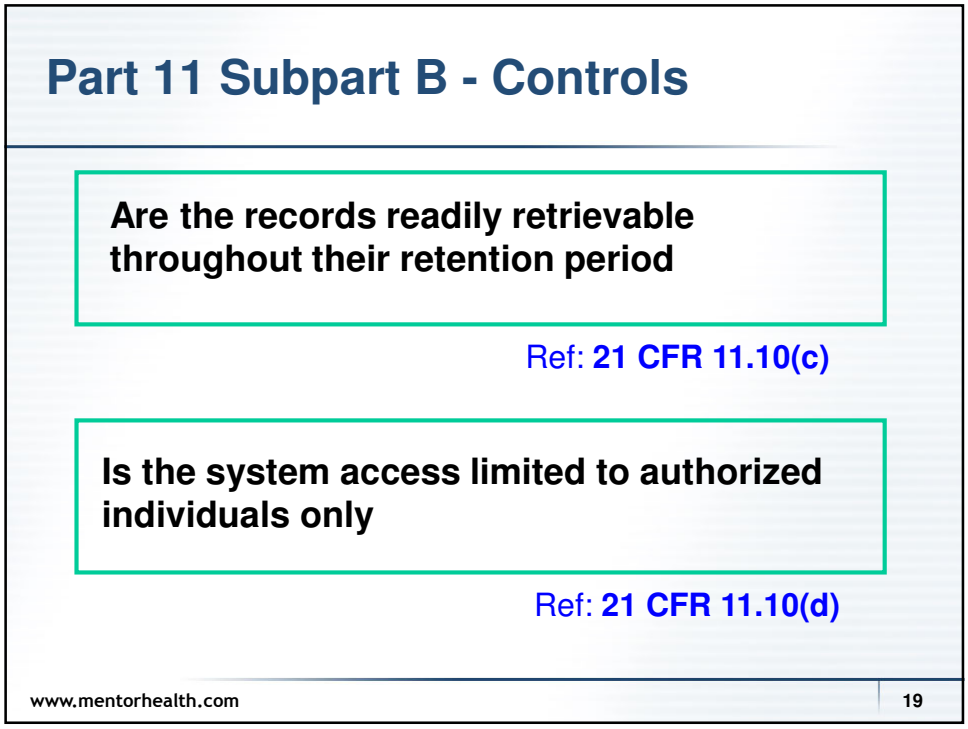
Is the system capable of producing complete and accurate copies of electronic records on paper

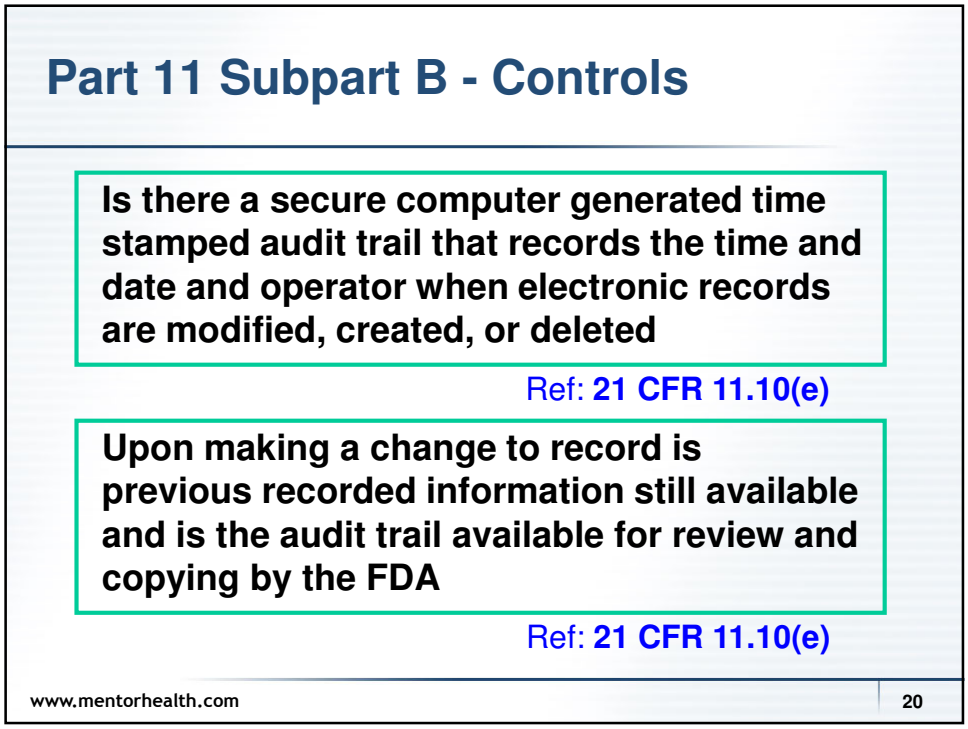
Ref: **21 CFR 11.10(b)**

Is the system capable of producing complete and accurate copies of electronic records in electronic form for inspection, review, and copying by the FDA

Ref: **21 CFR 11.10(b)**

www.mentorhealth.com 18


Part 11 Subpart B - Controls
Are the records readily retrievable throughout their retention period
Ref: 21 CFR 11.10(c)
Is the system access limited to authorized individuals only
Ref: 21 CFR 11.10(d)
www.mentorhealth.com
19


Part 11 Subpart B - Controls
Is there a secure computer generated time stamped audit trail that records the time and date and operator when electronic records are modified, created, or deleted
Ref: 21 CFR 11.10(e)
Upon making a change to record is previous recorded information still available and is the audit trail available for review and copying by the FDA
Ref: 21 CFR 11.10(e)
www.mentorhealth.com
20

Closed System Controls

- 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

Ref: **21 CFR 11.10(e)**

Part 11 Subpart B - Controls

If the sequence of system steps or events is important, is the sequence enforced by the system

Ref: **21 CFR 11.10(f)**

Does the system ensure that only authorized individuals can use the system, electronic-ally sign records, access the operation or computer systems input or output devices, or alter a record or perform other operations

Ref: **21 CFR 11.10(g)**

Part 11 Subpart B - Controls

Does use of device (terminal e.g.) check to determine, as appropriate, the validity of the source of data input or operational instruction

Ref: **21 CFR 11.10(h)**

Is there a determination that persons who develop, maintain, or use electronic record / signature systems have the education, training and experience to perform assigned

Ref: **21 CFR 11.10(i)**

www.mentorhealth.com 23

Part 11 Subpart B - Controls

Is there the establishment of, and adherence to, written policies to hold individuals accountable and responsible for actions initiated under their electronic signatures, in order to deter record and signature falsification

Ref: **21 CFR 11.10(j)**

Does the concept of “SOP”s ring a bell?

www.mentorhealth.com 24

Part 11 Subpart B - Controls

Are there appropriate controls over system documentation (distribution of, access to, and use of documentation for system operation and maintenance

Ref: **21 CFR 11.10(k)(1)**

Are there revision and change control procedures to maintain an audit trail that documents time-sequenced development and modification of systems documantation

Ref: **21 CFR 11.10(k)(2)**

www.mentorhealth.com 25

Closed System Validation & Control

Validation of computerized systems should be maintained through physical and electronic controls such as:

- Strict control of changes to the validated system Installation of validated images on all machines
- Firewalls to limit introduction of viruses and prevent access by hackers
- Backup power to provide uninterrupted power supply (UPS)
- **...**

Ref: **21 CFR 11.10**

www.mentorhealth.com 26

Closed System Validation & Control

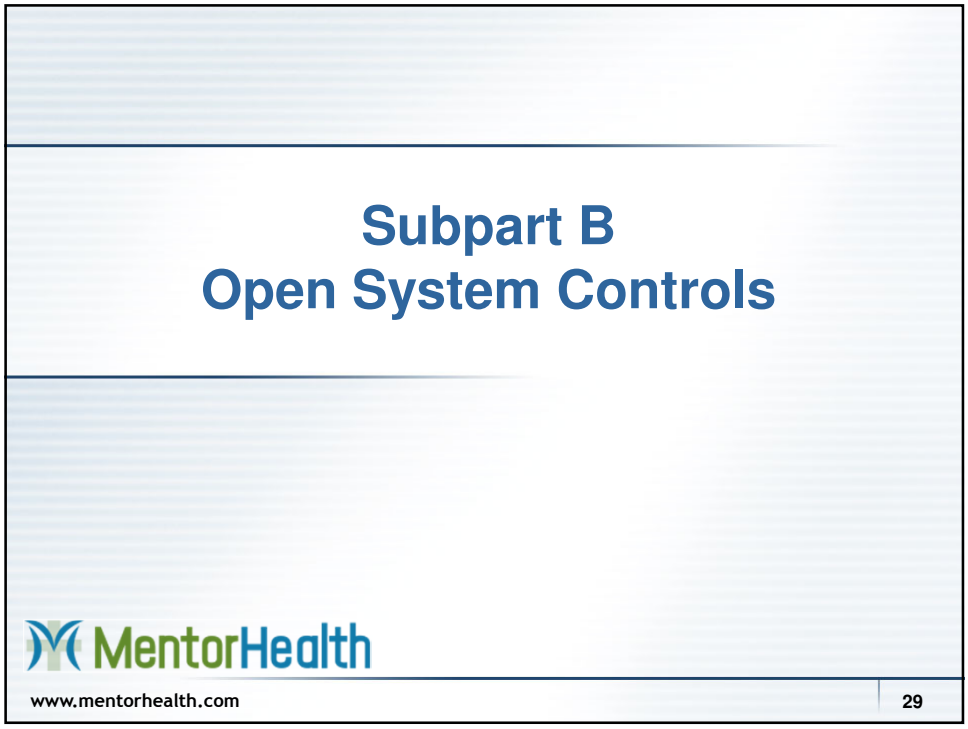
- …
- Controlled installation of all software to prevent unauthorized installations by users
- Limited physical and technical access to the critical servers upon which our electronic data resides
- Audit trails for systems managing regulated data
- Limited access to change system clocks on a workstation

Ref: **21 CFR 11.10**

Closed System Access

Phone Access to a closed System

- Internet access over public communication routes could be considered part of a closed system, but additional security measures are needed (e.g. security cards).
- Dialup / VPN is considered point-to-point connection and is not accessible to other phone users.
- All systems should/must require user authentication and / or encryption to provide the added security for accessing the network via dialup.



What is an Open System:

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

  Ref: **21 CFR 11.3(b)(9)**

- Virtual Private Network (VPN) access to the Network may be an example of an open system because data is transmitted between parties over an insecure or public network, such as the internet (access to the internet is not controlled).

www.mentorhealth.com 30

21 CFR Part 11 Subpart B

Part 11 Electronic Records; Electronic Signatures

- Subpart B - Electronic Records
  - 11.10 Controls for Closed Systems
  - 11.30 **Controls for Open Systems**
  - 11.50 Signature manifestations
  - 11.70 Signature / Record Linking

Open System Controls

Open systems must have additional controls because records may be read, modified or compromised by others to the possible detriment of persons responsible for record content.

- Use of firewalls, anti-virus software and authentication and/or encryption are examples of methods of control for the open system.

Ref: **21 CFR 11.3**

Controls for Open Systems

- Persons who use open systems to create, modify, maintain or transmit electronic records shall employ procedures and controls designed to ensure the authenticity, integrity and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt.

Ref: **21 CFR 11.30**

Controls for Open Systems

Such procedures and controls shall include…

- those identified in 11.10, as appropriate, and additional measures such as document encryption and use of appropriate digital signature standards to ensure as necessary under the circumstances, record authenticity, integrity, and confidentiality."
- Controls can include individual encryption key (a secret code) for each user in addition to the regular user ID and password

Ref: **21 CFR 11.30**

Data Trails

In general terms, audit trails must be:

- Secure
- Operator independent
- Computer generated
- Time stamped (date and time)
- Must be retained along with e-record for duration of life cycle
- Must be available for FDA review / copying

Internal Audit Control

MentorHealth

The Audit Trail of Data

Three questions that need answers:

- **What is an audit trail**
- **Access requirements**
- **What does an Audit Assess**

What is a Data / Audit Trail?

A secure computer generated electronic record in readable form showing:

- *Who* entered or changed data
- *What* was changed (documentation of previous information that may have been deleted as well as any new information added)
- *When* change was made - date and time

Internal Audit Items

Items assessed in a QA internal audit

- Standard Operating Procedures
- Security
- Data Management process
- Audit Trails
- Electronic Signature
- Training Records
- Hardware Validation Process
- Software Validation Process

Internal Audit Questions

Standard Operating Procedures

- Do they exist?
- Are they maintained / updated on a schedule?
- Are they Followed?
- Are they communicated to all employees?
- How are they communicated to employees?
- Are they relevant to specific job titles
- Where are the training records?
- Do appropriate people know them well?

Internal Audit Questions

Unit Security

- What is the general facility access security?
- How and who has access to the system?
- Are there records of who has access privileges?
- What safeguards are in place to prevent unauthorized use of passwords / ID codes?
- What safeguards are in place to prevent access to computerized systems?
- How is data secured in case of computer viruses?
- How are records protected to enable retrieval?

www.mentorhealth.com 41

Internal Audit Questions

Data Management

- How are data / documents stored and archived?
- How is the data secured in case of disasters?
- Describe backup / disaster recovery procedures?
- Describe storage of backup records?
- Are the records stored at a secure location offsite?
- Do back-ups have recovery logs?
- Is each version of the backup archived?
- Is there version control on any electronic records?
- Is there a 'chain of custody' of the version control?

www.mentorhealth.com 42

Internal Audit Questions

Audit Trails:

- Are they complete according to current standards?
- Are they Secure?
- Are all entries date and time-stamped?
  This includes the date and time of operator entries and/or any action that creates, modifies, or deletes electronic records?
- Editable? and if so, by whom?
- Modifiable without approval in any way?

www.mentorhealth.com 43

Internal Audit Questions

Training Records

- What is the make-up of your QA department?
- What is the organization of your IT department?
- Describe how employee qualifications are verified?
- Is training on a continuing basis?
- How are employees notified of training updates?
- Are job descriptions available for each position?
- Are there records of training and experience?
- Are job responsibilities / work load documented?
- Is company turnover documented and discussed?

www.mentorhealth.com 44

Internal Audit Questions

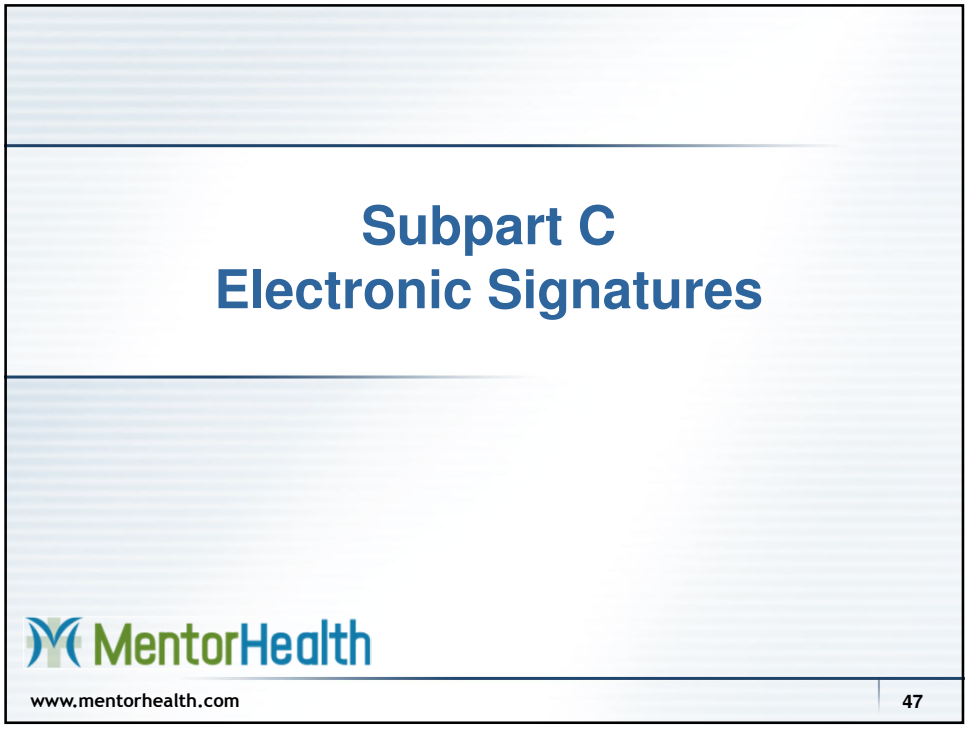
Hardware Validation Processes

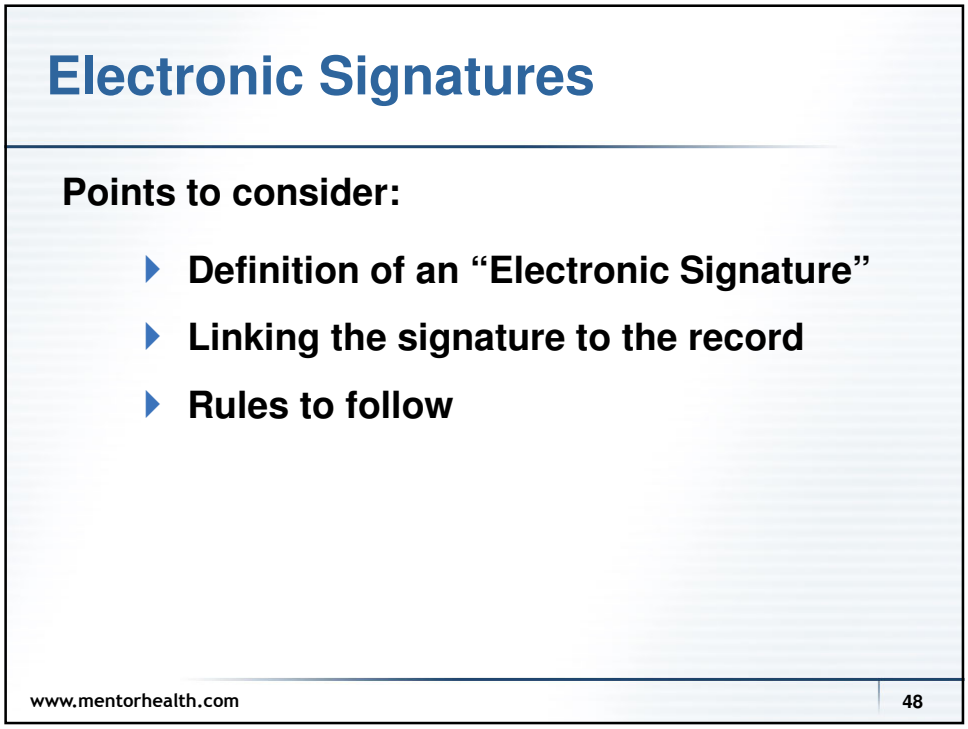
- Is there a valid documentation plan for the process?
- Are the validation procedures clear?
- Does the process identify who is responsibe?
- How are hardware validation problems resolved?
- How is hardware validation developed and tested?
- How is hardware validation process maintained?
- How is the hardware validation process changed?
- Are unit / system clocks synchronized to network server clock? and how often?

Internal Audit Questions

Software Validation Processes

- What are the processes used to validate software?
- Is there a reasonable / clear validation plan?
- Is there a complete validation report generated?
- Describe the approval process of the plan & report?
- What types of test results does this report contain?
- Does the validation report evaluate how your process demonstrates that design specs are met?


Subpart C
Electronic Signatures
MentorHealth
www.mentorhealth.com
47


Electronic Signatures
Points to consider:
Definition of an "Electronic Signature"
Linking the signature to the record
Rules to follow
www.mentorhealth.com
48

Electronic Signatures

Definition of an 'electronic signature':

- "A computer data compilation of any symbol or series of symbols executed, adopted, or authorized by an individual to be the *legally binding equivalent* of the individual's handwritten signature."

Ref: **21 CFR 11.3**

"Digital Signature" defined

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

Ref: **21 CFR Part 11.3(b)(5)**

"Electronic Signature" defined

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

Ref: **21 CFR Part 11.3(b)(7)**

Internal Audit Questions

Electronic Signatures

- Do electronic records contain information associated with the signer?
- Is there a printed name of the signer?
- Is the date and time when the signature was executed stored electronically?
- Is the review and approval of data associated with the signature?
- Are signatures related to the level of responsibility?

Electronic Signature

Refers to the act of attaching a signature by electronic means, and can be done in a variety of ways and has more than one meaning.

- One meaning it has acquired is an electronic sound, symbol or process, attached to, or logically associated with, a contract or other record and executed or adopted by a person with the intent to sign the record. Electronic signatures may be digital (cryptographic).

Part 11.50 Signature manifestations

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

(1) The printed name of the signer

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

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

Ref: **21 CFR 11.50 (a)**

Electronic Signatures

Linking the electronic signature to the study record is a crucial step

- "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."

Ref: **21 CFR 11.70**

11.70 Signature/record linking

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

Ref: **21 CFR 11.70**

11.100 General Requirements

Each electronic signature shall be unique to one individual and shall not be reused by, or assigned to, anyone else

Ref: **21 CFR 11.100(a)**

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

Ref: **21 CFR 11.100(b)**

11.100 General requirements

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

(1) The certification shall be submitted in paper…

(2) Upon request prove it is the legally binding =

Ref: **21 CFR 11.100(c)**

11.200 Electronic signature controls

Electronic signatures that are not based on biometrics shall:

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

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

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

Ref: **21 CFR 11.200 (a)**

www.mentorhealth.com 59

11.300 Controls for ID codes and passwords

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

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

(b) Ensuring the ID code and password issuances are periodically checked, recalled, or revised.

Ref: **21 CFR 11.300(a,b)**

www.mentorhealth.com 60

11.300 Controls for ID codes and passwords

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

Ref: **21 CFR 11.300(b)**

11.300 Controls of ID codes and passwords

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

Ref: **21 CFR 11.300(c)**

11.300 Controls of ID codes and passwords

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

Ref: **21 CFR 11.300(d)**

11.300 Controls of ID codes and passwords

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

Ref: **21 CFR 11.300(e)**

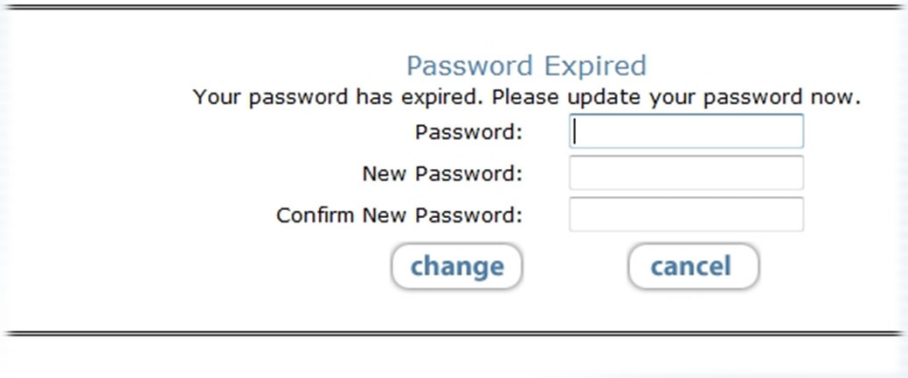
Electronic Signature Control

- **Unique to one individual**
  No reuse by someone else; no reassignment
- **At least two distinct components**
  Example: Unique User ID and Password
- **Used only by their genuine owners - Periodically checked, recalled or revised**
  Example: Password aging and forced change
- **Subject to loss management procedures**
  Deauthorize if potentially compromised
- **Subject to transaction safeguards**
  Report unauthorized use attempts immediately

www.mentorhealth.com 65

Electronic Signature Controls

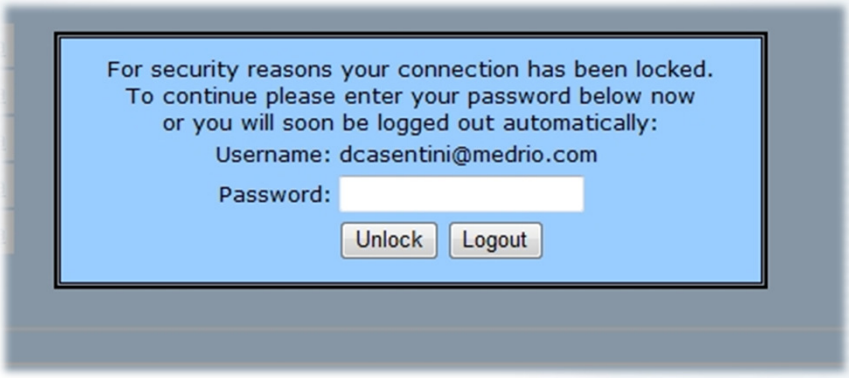
A screen like this is typical for password control



www.mentorhealth.com 66

Electronic Signature Controls

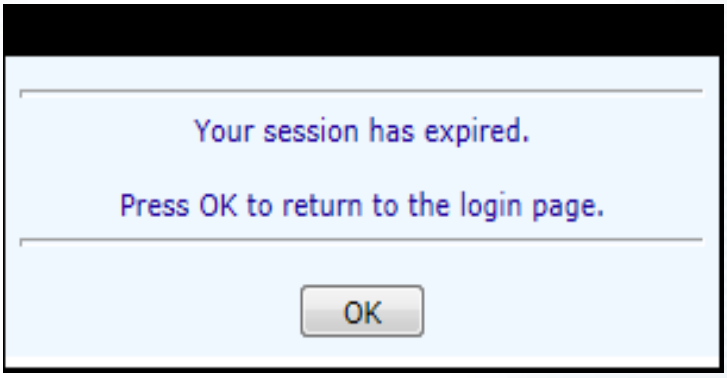
A screen like this is typical if there is a "time-out" or potential security breach



www.mentorhealth.com 67

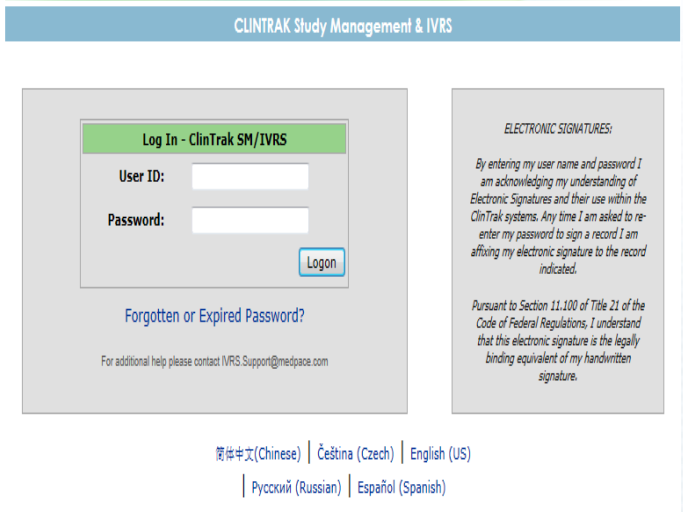
Electronic Signature Controls

A screen like this is typical if there is a "time-out" or potential security breach



www.mentorhealth.com 68

Part 11 requirements



www.mentorhealth.com 69

Part 11 requirements

The Key requirements of Part 11

- Validation
- Security
- Audit trails
- Record retention and protection

www.mentorhealth.com 70

Why Regulate?

Computerized systems must provide the same degree of confidence as a paper system

- Computer systems and electronic records store vital corporate data and support crucial business operations
- Sponsor company and FDA rely on data
- Concerns for data quality:
  - Data integrity
  - Management control
  - System reliability
  - Auditability

www.mentorhealth.com 71

Suggested Controls

To ensure authenticity, integrity, & confidentiality

- Physical and logical security
- Consistent application of security procedures across the organization
- Unique ID and password for each user
- Implementation of standard desktop configurations (titles linked to a standard)
- IT control of all installation of hardware and software
- Robust virus detection system
- Active monitoring of the system

www.mentorhealth.com 72

Suggested Controls

To ensure authenticity, integrity, & confidentiality

- Analysis of security violations including diagnosis and corrective actions to prevent recurrences
- Change control
- Document control
- Backup and archival procedures
- Provide the environment to support individual accountability expectations.
- Includes training, communicating new or revised policies and procedures

Standard Operating Proceedures

MentorHealth

Standard Operating Procedures

Areas of greatest importance to have SOPs in:

- Control of Hardware and software
- The monitoring processes
- Rules for data transfer
- Personnel / employee training in handling EDC
- Proper handling or the legally binding electronic signatures and their limitations

Suggested SOPs

- Validation Procedures
- Change Control
- Document Control for System Validation
- Monitoring Violation Attempts
- Computer Virus Protection
- Access to the Computer Room
- Computer Date and Time Setting

Suggested SOPs

- Computer File Backup, Storage and Retention
- Backup Media Verification
- Domain Account Security Policy
- Granting Permission to Sponsor regarding access to Study Data
- Archiving Sponsor Study Data
- Disaster Recovery

Suggested SOPs for IT Types

- Set up of a Study Specific Database for Data Collection/Handling
- Code Management for a Study Specific Database
- Electronic Project File Storage / Backup
- EDC System Maintenance

Role of Unit Staff

It is essential that staff orientation and reinforcement include the following:

- Know and follow the company security policies, practices, and SOPs.
- Do not reveal or share your password with any other individual
- Do not open e-mails from unknown sources
- If you have a laptop, you must maintain personal control when traveling

www.mentorhealth.com 79

Role of Unit Staff

It is essential that staff orientation and reinforcement also include the following:

- Know that policies and controls that are in place to prevent installation of unauthorized software
- Understand the significance of systems and applications that allow entry, modification, reporting and analysis of regulated data
- Know and comply with SOPs and company policies at all times

www.mentorhealth.com 80

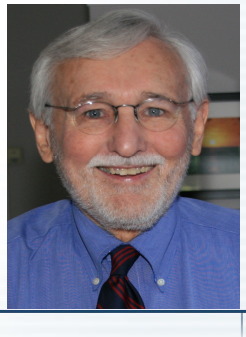
In the end ...

... a physician doing clinical research is still a physician with all that entails.

- She / he will take great care in all aspects of the care of those with whom she / he is responsible.
- This care includes accurate record keeping and clear documentation of ones thought process and actions before, during, and after a study is conducted including clear knowledge of the electronic systems used.

This Webinar is Brought to you by MentorHealth

Now you Know
Thanks For Listening



URL: http://Dr.Pierce1.net
Email: Charles@Pierce1.net
Emil charles.pierce@MARC-CTC.com

References

Suggested reading:

- 21 CFR Part 11, "Electronic Records; Electronic Signatures; Final Rules." Federal Register 62(54), 13429, March 1997
- Guidance for Industry: Part 11, Electronic Records; Electronic Signatures: Scope and Application, FDA, August 2003 fda.gov/regulatoryinfromation/guidance
- Guidance for Industry: Computerized Systems Used in Clinical Investigations; DHHS, FDA, OC; May 2007, fda.gov/regulatoryinformation/guidances/
- Consolidated Guidance: E6 Good Clinical Practice

www.mentorhealth.com 83

MentorHealth

QUESTIONS

If there are any further questions which we were not able to get to today please feel free to contact me through Global Compliance Panel.

www.mentorhealth.com 84

MentorHealth

Upcoming Webinars of Charles H. Pierce

- The GCP-ICH Obligations of Sponsors, Monitors, and Investigators - Barriers and Solutions
  Tuesday, July 9, 2013 10:00 AM PDT | 01:00 PM EDT
- How Accurate Adverse Event Reporting is the Key to Subject Safety of Approved Drugs?
  Tuesday, July 23, 2013 10:00 AM PDT | 01:00 PM EDT

www.mentorhealth.com 85

MentorHealth

Past Webinars of Charles H. Pierce

- How to Prevent or Handle Protocol Deviations and Violations to be GCP and Regulatory Compliant
- Using Independent Data Safety Monitoring in Clinical Research – How and Why
- 21 CFR Part 11 Compliance - Ensuring Data Integrity and Safety in Clinical Research
- The GCP-ICH Obligations of Sponsors, Monitors, and Investigators - Barriers and Solutions
- How Accurate Adverse Event Reporting is the Key to Subject Safety of Approved Drugs?

For further details please click on the link below:
http://www.mentorhealth.com/control/webinarsearch?topic_name=&category_id=-1&speaker_id=20122&webinar_month=ALL&x=61&y=12

www.mentorhealth.com 86

MentorHealth

Contact Us:

- Customer Support at :
  1-800-385-1607
- Questions/comments/suggestions:
  webinars@mentorhealth.com
- Partners & Resellers:
  partner@mentorhealth.com

www.mentorhealth.com 87