

Computer Systems Validation and Data Integrity Regulatory Expectations

7th Conference on Clinical Trials in the Nordic Countries 2019

Ib Alstrup, Medicines Inspector GxP IT, Danish Medicines Agency



Ib Alstrup

Medicines Inspector, GxP IT



- Medicines Inspector GxP IT, DKMA (since 2017) inspecting CSV in GLP, GCP, GMP, GDP and GVP
- PIC/S DI Guideline
- OECD GLP DI Guideline
- EU GCP eGuidance
- EU GMP Annex 11

- Electronic Engineer (SW design and test)
- Novo Nordisk: ITQA and Supplier Auditor (14 yrs)
- Philips & Ericsson: SW Designer and Tester (12 yrs)

Presentation Topics

- Paper vs Electronic Records
- Different GxPs
- ICH GCP E6 R2
- Further Guidance
- Expectations

Paper vs Electronic Records

Paper vs Electronic Records

Batch Record (or BMI Calculation)

GxP corrections

- Who
- What
- When
- Why

② 125.000 kg according to Process Validation Report
PVR-123. Corrected by John Doe 4 Sep 2017

Blending Yield Calculation

Yield Type	Yield	Unit	Signature	Date
Theoretical (Batch Size)	② 120.000	Lb. or Kg	② Donald Duck	② 1 SEP 2017
Actual (from discharge)	125.923	Lb. or Kg	Donald Duck	2 SEP 2017
Percent (Actual / Theoretical x 100)	③ 95.3	%	Acceptable range 95-103%	

① ~~104.9% wrong calculation according to formula, corrected by Mickey Mouse 3/9-2017~~

③ 100.7% Consequence correction of ② John Doe 4 Sep 2017

Paper vs Electronic

Three representations

BatRecSys v. 1.0

Blending Yield Calculation				
Yield Type	Yield	Unit	Signature	Date
Theoretical (batch size)	125.000	Kg	[John Doe]	4 SEP 2017
Actual (from discharge)	125.923	Kg	[Donald Duck]	2 SEP 2017
Percent (A / T x 100)	100.7	%	Acceptable range 95-103%	

② 125.000 kg according to Process Validation Report PVR-123. Corrected by John Doe 4 Sep 2017

Blending Yield Calculation

Yield Type	Yield	Unit	Signature	Date
Theoretical (Batch Size)	② 120.000	Lb. or Kg	② Donald Duck	② 1 SEP 2017
Actual (from discharge)	125.923	Lb. or Kg	Donald Duck	2 SEP 2017
Percent (Actual / Theoretical x 100)	③ 95.3	%	Acceptable range 95-103%	

① 104.9% wrong calculation according to formula, corrected by Midway Mouse 3/9/2017

③ 100.7% Consequence correction of ② John Doe 4 Sep 2017

Blending Yield Calculation					
Yield Type	Yield	Unit	Signature	Date	
Theoretical (batch size)	125.000	Kg	John Doe	04-sep-17	
Actual (from discharge)	125.923	Kg	Donald Duck	02-sep-17	
Percent (A / T x 100)	100.7	%	Acceptable range 95-103%		

Paper vs Electronic

Why should we accept the electronic version?

BatRecSys v. 1.0

Blending Yield Calculation				
Yield Type	Yield	Unit	Signature	Date
Theoretical (batch size)	125.000	Kg	[John Doe]	4 SEP 2017
Actual (from discharge)	125.923	Kg	[Donald Duck]	2 SEP 2017
Percent (A / T x 100)	100.7	%	Acceptable range 95-103%	

② 125.000 kg according to Process Validation Report PVR-123. Corrected by John Doe 4 Sep 2017

Blending Yield Calculation

Yield Type	Yield	Unit	Signature	Date
Theoretical (Batch Size)	② 120.000	Lb. or Kg	② Donald Duck	② 1 SEP 2017
Actual (from discharge)	125.923	Lb. or Kg	Donald Duck	2 SEP 2017
Percent (Actual / Theoretical x 100)	③ 95.3	%	Acceptable range 95-103%	

① 104.9% wrong calculation according to formula, corrected by Midley/Morse 3/9/2017

③ 100.7% Consequence correction of ② John Doe 4 Sep 2017

BatRecSys Audit Trail

Date Time	Par/Unit Value	User	Reason
2017-09-01 13:21:02	TBS/Kg 120.000	Donald Duck	
2017-09-02 10:14:51	AFD/Kg 125.923	Donald Duck	
2017-09-04 09:11:02	TBS/Kg 125.000	John Doe	According to Process Validation Report PVR-123

Paper vs Electronic Records

Electronic documentation from systems without validated key functionalities, e.g. audit trail, is like GxP documentation written by a pencil



You don't know what was there before



Different GxPs

Requirements to qualification and operation of IT

In different GxPs

Design, validation and operation of IT systems described in very different depths

- GLP: 20+ pages
- GMP: 3½ pages
- GCP: 1 page
- GVP: < ½ page

With a few exemptions, no objective reason why our expectations should be different

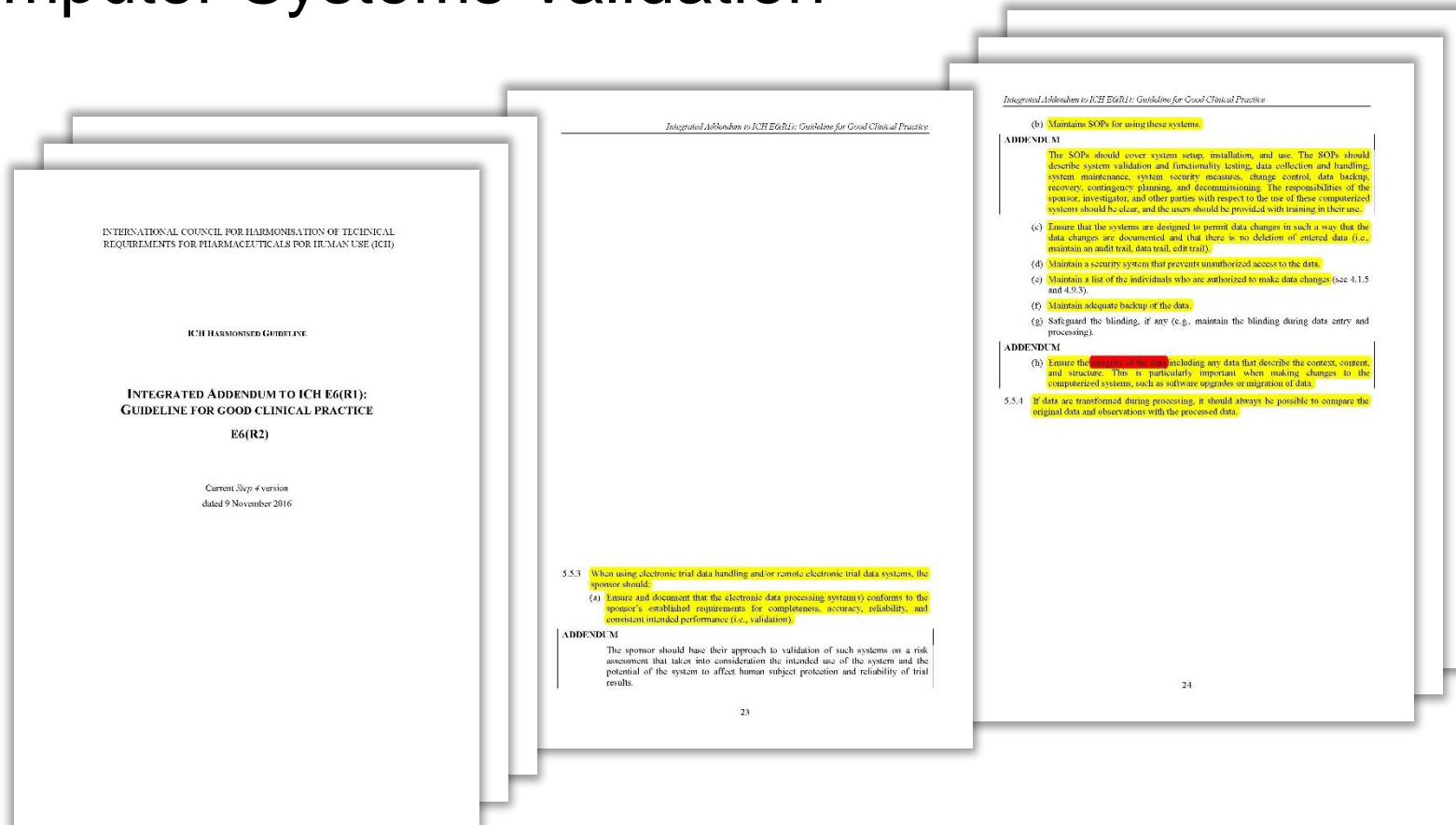
The more detailed regulatory requirements are (GLP), the less we have to interpret

The opposite is also true 😊

ICH GCP E6 R2

ICH GCP E6 R2 5.5.3

about Computer Systems Validation



ALCOA+

"Data Integrity"

ICH CGP E6 R2

1. GLOSSARY

ADDENDUM

1.9 Audit Trail

Documentation that allows reconstruction of the course of events.

Who entered or changed data?
What* was entered or changed?
When was it entered or changed?
Why was it changed?

*) New and all previous values

ICH CGP E6 R2

1.65 Validation of Computerized Systems

A process of establishing and documenting that the *specified requirements of a computerized system can be consistently fulfilled* from design until decommissioning of the system or transition to a new system. The approach to validation should be *based on a risk assessment that takes into consideration the intended use of the system* and the potential of the system to affect human subject protection and reliability of trial results.

Validation should prove that URS requirements are fulfilled

Validation based on risk assessment of URS requirements

ICH CGP E6 R2

4.9 Records and Reports

ADDENDUM

4.9.0 The investigator/institution should maintain adequate and accurate source documents and trial records that include all pertinent observations on each of the site's trial subjects. Source data should be attributable, legible, contemporaneous, original, accurate, and complete. Changes to source data should be traceable, should not obscure the original entry, and should be explained if necessary (e.g., via an audit trail).

4.9.1 The investigator should ensure the accuracy, completeness, legibility, and *timeliness* of the data reported to the sponsor in the CRFs and in all required reports.

ALCOA principles

Audit trail incl. all previous values

Who did what, when and why

Data (and audit trail) recorded in true time

ICH CGP E6 R2

5.2.1 A sponsor may transfer any or all of the sponsor's trial-related duties and functions to a CRO, *but the ultimate responsibility for the quality and integrity of the trial data always resides with the sponsor*. The CRO should implement quality assurance and quality control.

Sponsor always responsible for integrity and quality of data (and for related IT systems)

ICH CGP E6 R2

5.5.3 When using electronic trial data handling and/or remote electronic trial data systems, the sponsor should:

(a) Ensure and document that the electronic data processing system(s) conforms to the sponsor's established requirements for completeness, accuracy, reliability, and consistent intended performance (i.e., validation).

ADDENDUM

The sponsor should base their approach to validation of such systems on a risk assessment that takes into consideration the intended use of the system and the potential of the system to affect human subject protection and reliability of trial results.

Validation according to URS
Sponsor should create (or adopt) URS

Validation should be based on risk assessment of URS requirements

ICH CGP E6 R2

5.5.3 When using electronic trial data handling and/or remote electronic trial data systems, the sponsor should:

(b) Maintains SOPs for using these systems.

ADDENDUM

The SOPs should cover system setup, installation, and use. The SOPs should describe system validation and functionality testing, data collection and handling, system maintenance, system security measures, change control, data backup, recovery, contingency planning, and decommissioning. The responsibilities of the sponsor, investigator, and other parties with respect to the use of these computerized systems should be clear, and the users should be provided with training in their use.

SOPs for system validation,
data collection (date integrity)
system maintenance, security,
backup, recovery and contingency

Roles described, training provided



ICH CGP E6 R2

5.5.3 When using electronic trial data handling and/or remote electronic trial data systems, the sponsor should:

- (c) *Ensure* that the systems are designed to permit data changes in such a way that the data changes are documented and that there is *no deletion of entered data* (i.e., *maintain an audit trail*, data trail, edit trail).

Qualification should ensure no real deletion of data (only marked as such)
Captured by audit trail

ICH CGP E6 R2

5.5.3 When using electronic trial data handling and/or remote electronic trial data systems, the sponsor should:

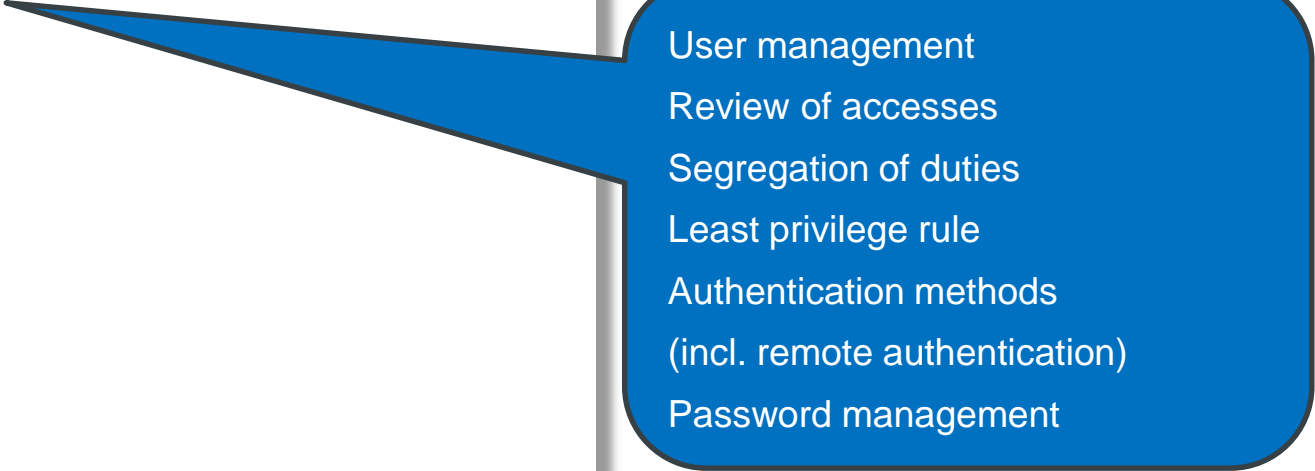
(d) Maintain a *security system that prevents unauthorized access to the data.*

Physical access control
Logical access control
Authentication method
Firewall management
Platform management
Security patching
Security incidents
Penetration testing
Virus protection
Intrusion detection
Use of USB devices
etc

ICH CGP E6 R2

5.5.3 When using electronic trial data handling and/or remote electronic trial data systems, the sponsor should:

(e) *Maintain a list of the individuals who are authorized to make data changes (see 4.1.5 and 4.9.3).*



- User management
- Review of accesses
- Segregation of duties
- Least privilege rule
- Authentication methods
(incl. remote authentication)
- Password management

ICH CGP E6 R2

5.5.3 When using electronic trial data handling and/or remote electronic trial data systems, the sponsor should:

(f) *Maintain adequate backup of the data.*

Data centre

- replication
- physical separation

Backup

- type (incremental or complete)
- frequency (hour, day, week, month)
- retention (day, week, month, forever)
- logical separation (not same server)
- physical separation (media)

Restore test

Disaster recovery

Archival



ICH CGP E6 R2

5.5.3 When using electronic trial data handling and/or remote electronic trial data systems, the sponsor should:

(g) *Safeguard the blinding, if any (e.g., maintain the blinding during data entry and processing).*

Specification and qualification of functionality designed to safeguard blinding, e.g.

- data entry
- audit trail
- edit checks

ICH CGP E6 R2

5.5.3 When using electronic trial data handling and/or remote electronic trial data systems, the sponsor should:

ADDENDUM

(h) *Ensure the integrity of the data including any data that describe the context, content, and structure. This is particularly important when making changes to the computerized systems, such as software upgrades or migration of data.*

Qualification and safe operation
(all of the above)

Changes should be qualified
(incl upgrade of operating system)

Data migrations should be qualified
(incl audit trail)

Further Guidance

Further Guidance

EMA GCP Q&A

- No. 8: Pitfalls regarding contractual arrangements with vendors of electronic systems
- No. 9: Level of qualification to be performed by sponsor when using electronic systems qualified by a provider / Documentation required to be available during inspection

www.ema.europa.eu/human-regulatory/research-development/compliance/good-clinical-practice/qa-good-clinical-practice-gcp

EMA GCP Reflection Paper

www.ema.europa.eu/en/documents/scientific-guideline/reflection-paper-good-clinical-practice-compliance-relation-trial-master-files-paper/electronic-management-audit-inspection-clinical-trials_en.pdf

EU GCP eGuidance (coming)

Expectations (excerpt)

Access Control

Expectations

- Systems should **restrict logical access to authorised individuals**
- **Physical access to data media should be restricted** for normal users
- System **accounts should be uniquely named** (not just a name)
- **Normal users should have no admin access to systems** (incl. PCs) hosting critical data
- Access roles should be **assigned according to the least-privilege rule**
- Systems should be able to generate a **list of users**, to be used for review of users
- Systems should be able to generate a **list of login attempts**, to be used for review
- All users should have **individual accounts**, shared accounts should be prohibited
- Access based on **segregation of duties**, admin users should not conduct normal work
- **User reviews** should be made at suitable intervals to ensure only approved accesses

Inactivity Logout Expectations

- Appropriate [inactivity logout time is defined](#), rather shorter than longer, risk based
- [Re-authentication](#), required after inactivity logout
- [Deactivation or change of inactivity logout settings](#), not possible for normal users

Time Settings

Expectations

- System **clock and time zone non-editable** for normal users (segregation of duties)
- System **clock synchronized** with connected systems or standards

Audit Trails

Expectations

- Record who (incl. role), what, when and why for manual entries, changes and deletions
- Contain new and all previous values must be available
- Recorded in true time, not at end of process; change after critical info is aggravating factor
- Audit trail non-deactivatable, at least for normal users, deactivation should create entry
- Audit trail non-editable, for normal users and preferably for privileged users
- Possible to print and obtain electronic copy, e.g. for regulatory use
- Readable and understandable for normal users, auditors and inspectors
- Reviewable, accommodating an efficient audit trail review
- A procedure for audit trail reviews should exist, incl. what to review, when and by whom
- Audit trails should be reviewed according to the procedure and appropriate actions taken
- Audit trails should be included in backup, restore and archival procedures

Audit Trails

Not required but...

- **Searchable**, e.g. user, parameter, value, date and time interval, reason
- **Sortable**, e.g. to block out alarms, events and other non-audit trail information
- **Exportable** (e.g. to Excel), in lack of proper built-in search or sort functionality

Platform Management and Security Patching Expectations

- Operating systems are updated timely according to vendor recommendations
- Operating systems are security patched timely according to vendor recommendations
- Un-patched or unsupported systems are isolated from the internet and remaining network

Cyber Attacks



WannaCry (May 2017)

- Preyed on un-supported and un-patched systems
- Spread with user interaction
- Encrypted data and left them unavailable to users
- Recovering from attack is expensive and uncertain
- Microsoft had released security patch only 8 weeks before attacks exploded
- So, patching must be very timely..!

Cyber Attacks

- In June 2019, a large GxP regulated company, informed the DKMA that a facility had *“detected a form of ransomware that has caused disruption to some of our IT systems. Neither data integrity [!!] nor client confidentiality has been impacted by the incident”* and *“we do not have access to information in many of our systems, so we cannot provide live updates on sample progress or details on testing of samples [REDACTED]”*
- In August 2019, a large clinical research facility informed the DKMA that *“the database and backup [!!] belonging to a specific GCP study had been hacked and all original data had disappeared”* and had been *“replaced with bitcoin codes”* [Sic.]

Management of Firewalls

Expectations

- Firewalls should carefully designed only allowing traffic on necessary ports to be opened
- Firewall rules should be documented and approved and should be available for reviews
- Firewall settings should be periodically reviewed against their specifications

Backup, Restore and Disaster Recovery Expectations

- Backups should include **all data and meta data** (audit trail), may also include the system
- Backups should be **made frequently** based on risk, e.g. hourly, daily, weekly and monthly
- **Retention of backups should be based on risk**, e.g. a day, a week, a month, forever
- Backups should **not be stored on the same server** as original data (logical separation)
- Backups should **not be stored on the same location** as original data (physical separation)
- **Restore tests should be made** when making changes to the system or backup process
- **Restore tests should verify complete restore** of system data and audit trail
- **A disaster recovery plan should be in place** for systems hosting critical data, especially where data is stored on only one data center without replication to another

Thanks for your attention

For questions:

Ib Alstrup, Medicines Inspector GxP IT, Danish Medicines Agency
ibal@dkma.dk, www.linkedin.com/in/ib-alstrup-baa2542

