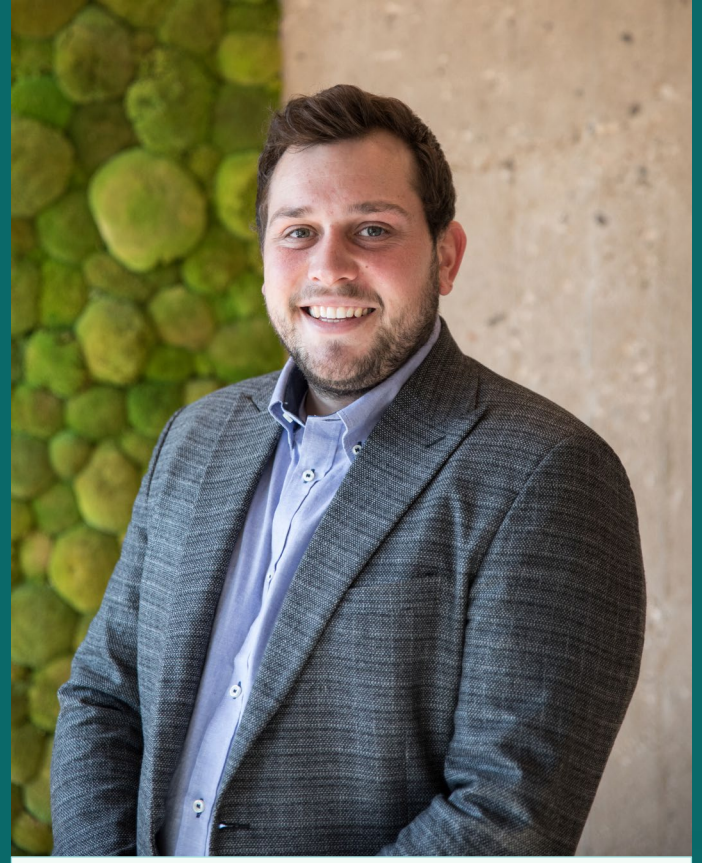
CLINIGMA®

SESSION IH10 — MARCH 25, 2026

Existing guidelines for in-trial interview study implementation

Towards a unified interpretation

Christian Holm



Christian Holm

Chief Technical Officer

MSc Computer Engineering
5+ years in clinical trial technology
Data privacy & regulatory compliance
GDPR · HIPAA · ISO 27001

Opening

Why this talk – and why me

> **“If it isn’t documented, it didn’t happen.”**
> This applies to qualitative patient data just as much as to CRFs and lab results.

Patient safety

A patient disclosed suicidal ideation during an interview. Within 30 minutes: escalated through validated systems with full audit trails. Within 4 hours: investigator confirmed appropriate action.

This worked because the systems were in place

Data integrity

The FDA received a submission based on in-trial interviews — and were unable to replicate the findings. The data didn’t hold up.

This is the outcome we need to prevent

Interview data is source data

> **"Original documents or data… irrespective of the media used. This may include… data provided/entered by trial participants…"**

ICH E6(R3) Glossary — Source Records

A	L	C	O	A	C
Attributable	**Legible**	**Contemporaneous**	**Original**	**Accurate**	**Complete**
Who conducted the interview, which patient, and when	Recording clear enough to be faithfully transcribed	Captured at the time of the interview, not reconstructed	Not a copy — the originally captured data	Recording reflects what the patient actually said	Full interview preserved, not just selected excerpts

Section 2.12.2

Systems must also be secure, validated, and reliable

Secure, validated, and reliable — audit trails, access controls, documented processes. ALCOA defines good data. System requirements define a trustworthy environment.

ICH E6(R3) Glossary (Data Integrity) · Sections 4.3.3 & 4.3.4

Sponsor accountability is explicit

You are responsible for the data regardless of who collected it – including subcontractors of your vendors

Sections 3.6.6 & 3.6.9

GCP & Data Privacy: reinforcing, not contradicting

WHERE THEY REINFORCE

- **Accuracy** — GCP: data integrity | GDPR: accuracy principle.
- **Auditability** — GCP: audit trails | GDPR: records of processing
- **Responsibility** — GCP: sponsor | GDPR: data controller

WHERE THEY CREATE TENSION

- **Preservation** — GCP push towards keeping everything for 25 years
- **Minimization** —GDPR: Anonymization of the data and minimization of collection

How they solve each other

25-year retention is a privacy risk — but GDPR explicitly accepts it when:

1. The patient gave informed consent
2. The purpose is justified

ICH-GCP provides exactly that justification: patient safety and data integrity for regulatory decision-making.

ICH-GCP makes your data credible and trustworthy for regulators

Privacy law ensures you can look the patient in the eye and say: your data was handled right

Three compliance gaps we still see

Contact details in Excel

Password-protected spreadsheets over email. Excel passwords cracked in seconds. No audit trails, no change logs. Both GCP data integrity and GDPR security violated in one email.

Consumer recording apps

Teams, Zoom, handheld recorders. Non-validated systems. No subject ID link. No control over where data is processed or who has access. GDPR cross-border transfer violation and no traceability of the data.

Deletion of recordings

Recordings deleted, only anonymized transcripts remain. Good for GDPR — but devastating for GCP. Source data destroyed. No proof the transcript is faithful. With AI, altering transcripts is trivially easy.

⚠ **Impact:** Data rejection, expensive rework, compliance findings — all preventable with the right framework.

5-step framework — step 1: Planning

1 Planning → 2 Preparing → 3 Executing → 4 Analysis and Reporting → 5 Archiving

Focus today: data integrity and data privacy constraints within each step.

Research objectives

Clear justification for processing personal data. Without it, the lawful basis under GDPR falls apart.

Data privacy and DPA

Data processing agreement with your vendor. Data flow diagram: where is data stored, who accesses it, does it cross borders? Involve your data privacy department for a DPIA.

Vendor contracting & RFP

You are accountable for the data processing. The RFP must cover: validated systems, GCP compliance, privacy safeguards, staff qualifications, safety reporting, archiving.

Step 2: Preparing

1 Planning → 2 Preparing → 3 Executing → 4 Analysis and Reporting → 5 Archiving

Protocol input

Interviews described in the clinical trial protocol. Purpose, timing, sample, methodology, data management, safety reporting. Standalone studies create serious data-sharing problems.

Informed consent

ICF must cover: recording, transcription, translation, analysis, and 25-year retention. Patient must understand how contact info is shared. Critical for lawful processing under GDPR.

Pharmacovigilance agreement

Non-negotiable. Without a signed PVA, you risk a critical audit finding. Adverse events are source data — ALCOA applies.

EC/IRB submissions

All patient-facing materials must be submitted: interview manuals, notifications, system interfaces

Staff training

No staff works without documented training. Covers site, CRO, interview vendor, and sponsor

Step 3: Data collection

1 Planning → 2 Preparing → **3 Executing** → 4 Analysis and Reporting → 5 Archiving

Scheduling

- Protocol-defined interview windows (2–3 weeks after site visit)
- Contact details in validated systems — not emailed Excel sheets
- Time zone management with audit trails

Interview conduct

- Record directly into a validated system
- End-to-end encryption from the moment the call is made
- Automatic audit trails and data checks
- Approved interview manual in the patient's language
- Role-based access — limited to assigned interviewer

Safety escalation

If an adverse event is discovered, the system must capture it under ALCOA principles and ensure notification escalations within the 24-hour reporting requirement. This is why validated infrastructure matters.

Step 3: Data processing

1 Planning → 2 Preparing → **3 Executing** → 4 Analysis and Reporting → 5 Archiving

Transcription

Native-speaking transcriber works from original audio. Clear pseudonymization processes must be in place.

Four-eye review

Interviewer listens to recording while reading transcript to ensure accuracy.

Translation

If multi-country: translate to English, then four-eye review against source audio or native transcript.

Monitoring

Automated system monitors compliance. Notifications escalated when action is not taken.

Without pseudonymization: data breaches and ICH-GCP violations when transcripts are shared.
Without monitoring: high likelihood of protocol deviations.

If anything in data capture is broken here, nothing downstream can fix it.

Step 4: Analyzing & reporting

1 Planning → 2 Preparing → 3 Executing → **4 Analysis and Reporting** → 5 Archiving

The analysed data alongside the transcripts is what you submit to regulators. The key principle: ***traceability***

Traceability chain

- Source recording
- Transcript coding
- Analysis & findings
- Reports with patient quotes

If any link breaks, the only way to reproduce findings is to start over.

Where they create tension

- ⊗ Contact details in Excel — no traceability
- ⊗ No source recordings preserved
- ⊗ Transcription without reference to source audio
- ⊗ Non-validated coding tools that allow altering recordings
- ⊗ Counts in Excel without reproducible scripts
- ⊗ Report writing without four-eye review

Qualitative Analysis Plan

Like a statistical analysis plan, but for qualitative data. Defines data quality handling, analytic framework, and reproducibility approach.

If your analysis can't trace back to the recording, it won't survive regulatory scrutiny.

Step 5: Archiving - the 25-year challenge

1 Planning → 2 Preparing → 3 Executing → 4 Analysis and Reporting → **5 Archiving**

Interview eTMF

An electronic trial master file specifically for interview data. Version control, audit trails, role-based access, full system validation. Not optional.

Why split the TMF

The sponsor cannot hold patient-sensitive data with direct identifiable information — but the source recordings must be preserved. Plan archiving and labelling from day one.

Why not removable media? DVDs and USB drives don't last forever. Shipping sensitive data requires encryption handled by non-technical staff. Recommend: validated online digital systems with appropriate security controls.

Non-sensitive — sponsor TMF

- Pseudonymized transcripts & translations
- Interview report & analysis files
- Quality control documentation

Transferred securely per data transfer plan

Sensitive — interview provider

- Original source recordings
- Unredacted transcripts
- Contact details & AE reports

Stored for 25 years in validated long-term archive

Four things to take away

1

In-trial Interviews are GCP source data

Patient interviews collected in a trial are source data. Treat them with the same rigor as any other trial data.

2

ICH-GCP + data privacy do not contradict

They reinforce each other. Build your process right and a single email won't become a violation of both frameworks.

3

You are accountable for vendor compliance

Use a structured RFP. Make requirements explicit. You're accountable for your providers and their subcontractors.

4

Ensure traceability from record to report

From protocol design through 25-year retention, every stage should be defensible. Don't retrofit at the end.

"The patient voice is too important to be handled informally."

Thank you — Christian Holm, CLINIGMA®

Happy to take questions or come find me afterwards in booth B3

Get started with the RFP Template