



SPA MDR CDR SCE

DH07

Blind/Unblind Workflows: Secure Separation and Governance in the CDR-SCE

MAR 2026

phuse·connect
connect share advance

The Clinical Data
Science Conference

US 2026

22-26 March
Renaissance Austin Hotel



Agenda

- Blinding/Unblinding in Clinical Trials
- Risk Vector of Unblinding and Unintended Exposure/Influence
- Architectural Elements for Secure Blinding
- Demonstrating Compliance and Inspection Readiness
- Recommendations and Implementation Options
- Wrap-up and Conclusion



Today's Journey

From Emerging Risk to Engineered Integrity.

Understanding the Shift

Why This Topic Matters Now, What Blinding Was Designed For, The Hidden Risk of Centralization, Why Blinding Needs to Evolve

Engineering Secure Platforms

Four Pillars of Secure Blinding, Architecture That Enables Secure Blinding, Embedding Governance into System Behavior

Proving Control & Leading Forward

Demonstrating Compliance and Inspection Readiness, Key Takeaways for Clinical Data Leaders

DH07 Blind/Unblind Workflows: Secure Separation and Governance in the CDR-SCE MAR 2026 Sycamore Informatics

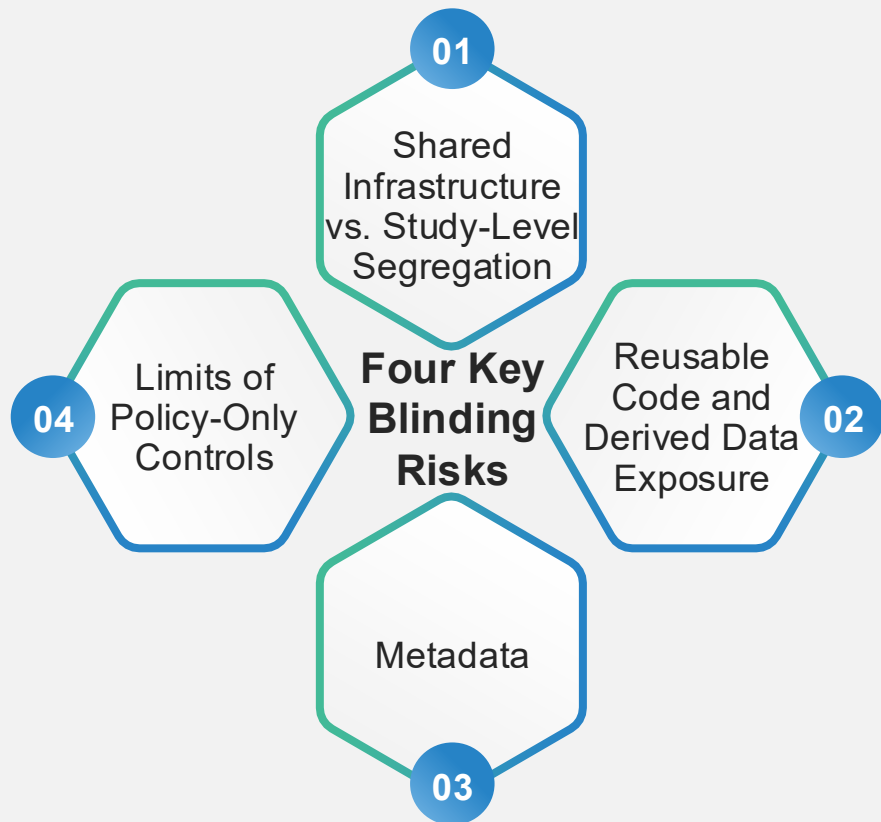


Blinding/Unblinding in Clinical Trials

- **Purpose:** ensure treatment information cannot influence data handling, analysis decisions, or interpretation before it is appropriate to do so
- Over the life of a study: Programmers, statisticians, etc. work across both blinded and unblinded info
- Interim analyses, safety reviews, final database lock, etc. all are legitimate moments where unblinded information exists and must be handled
- **Requirement:** ensure unblinded information is only accessed for approved reasons & cannot contaminate blinded workflows, outputs, or decision making



Blinding Risks in Clinical Trial Systems



Traditional Blinding Models

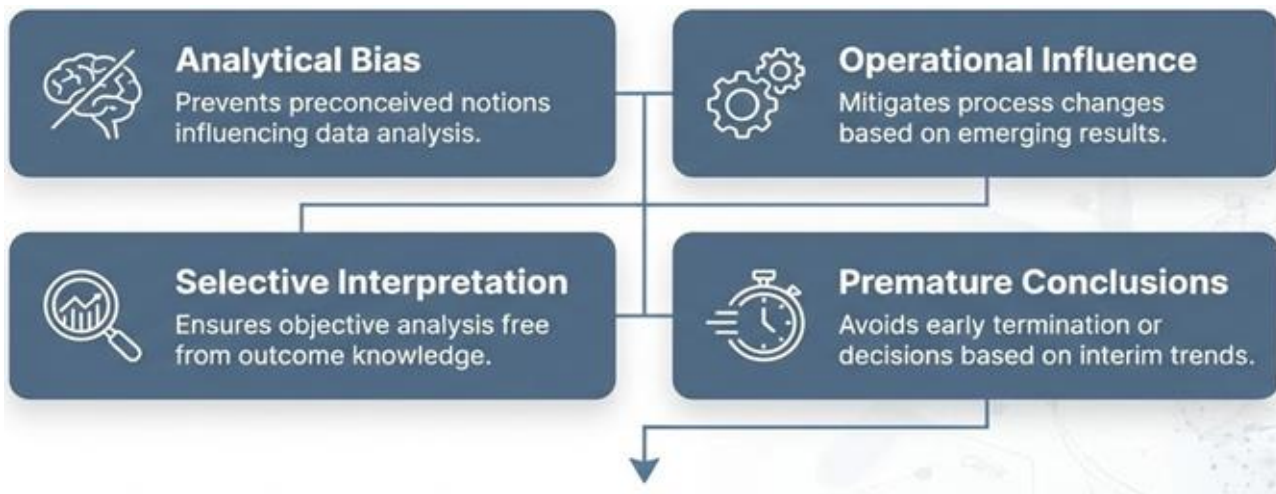


Rapid Platform Transformation



Platform modernization is outpacing traditional control models

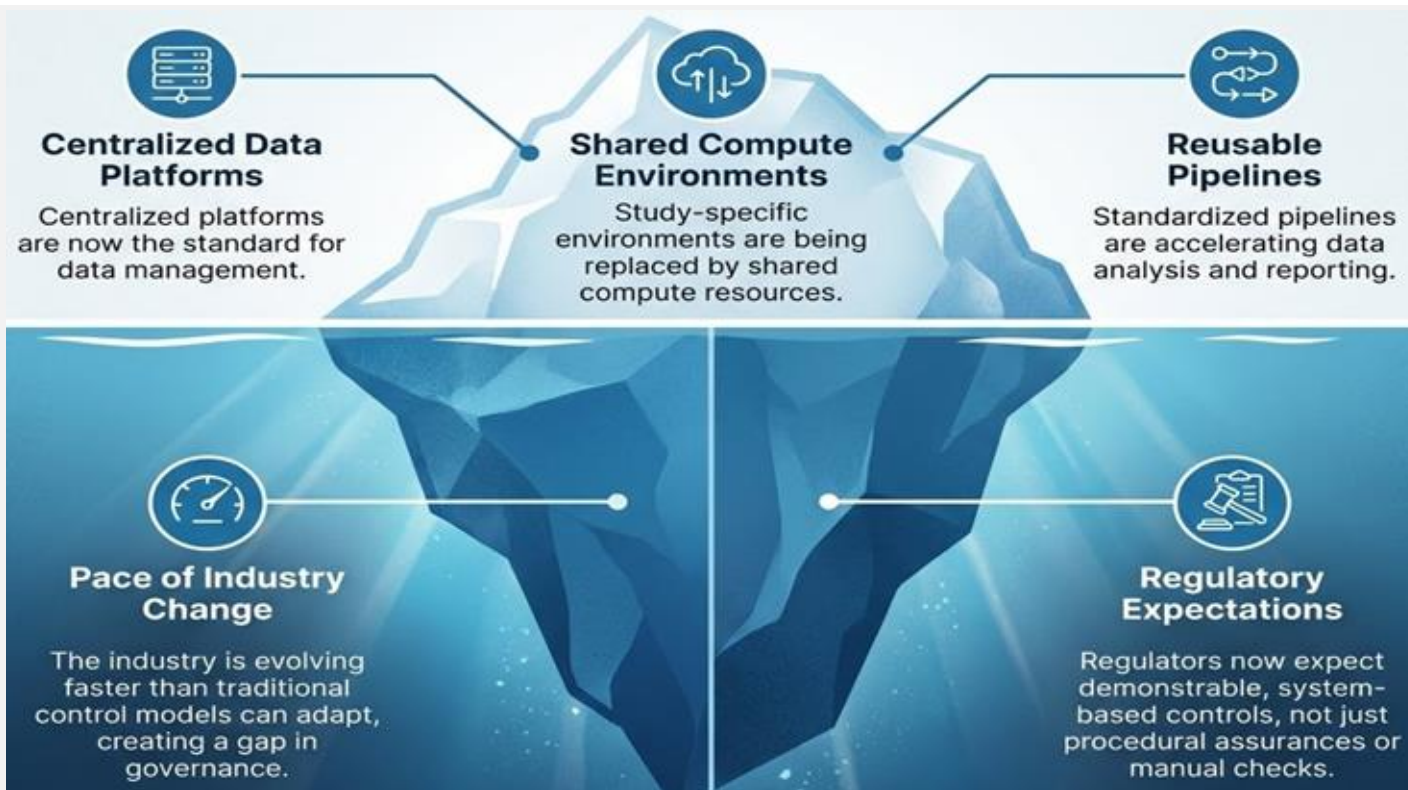
The Why of Blinding....



**Regardless of your business
processes or platform architecture
the study integrity is non-negotiable**

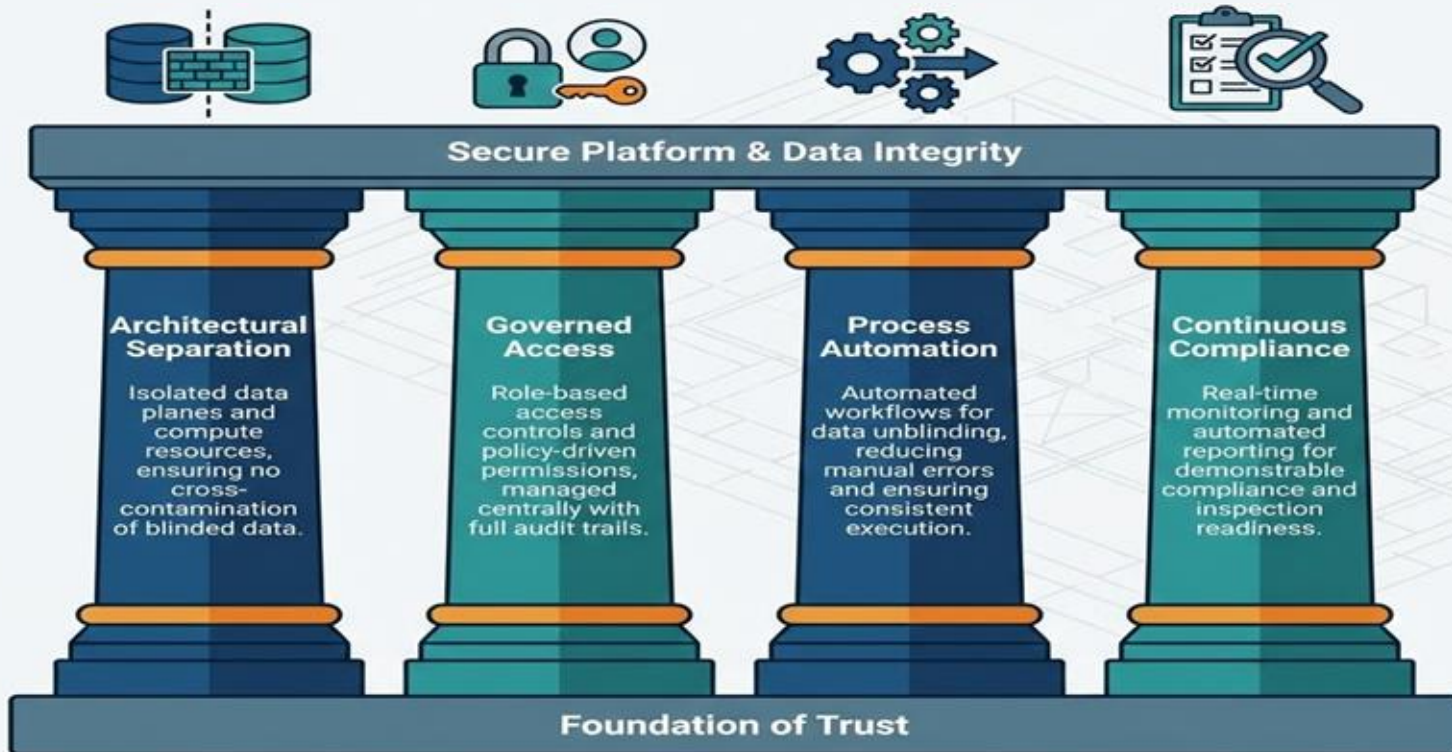
Why Blinding Needs to Evolve:

The iceberg of industry change (visible results vs underlying drivers)



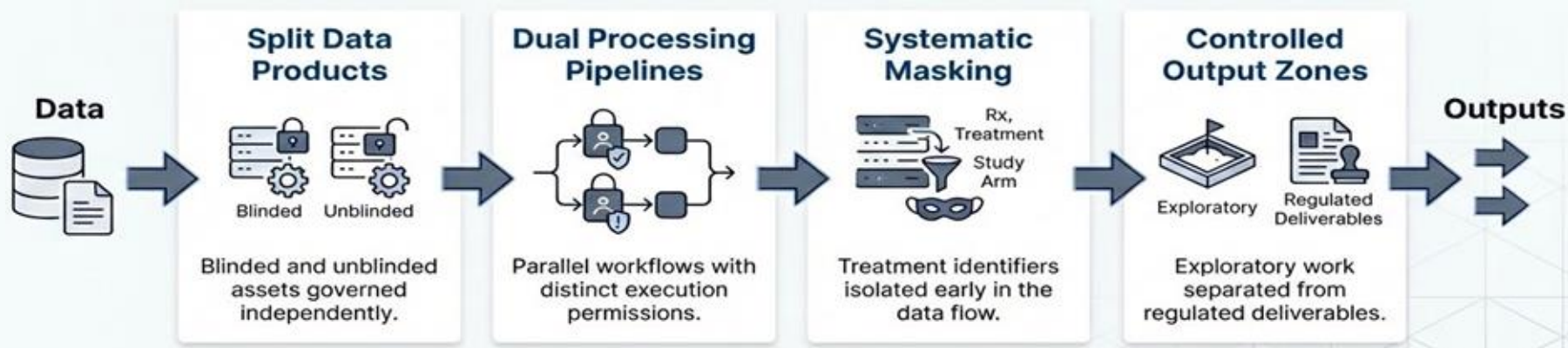
Four Pillars of Secure Blinding

Engineering trust through architectural separation, governance, and automation



Architecture Patterns that Enable Secure Blinding:

Achieving secure blinding through intentional platform architecture and not procedural controls alone



The strongest control is the one users cannot accidentally bypass

Designing for Prevention. Not Detection

Embedding Governance into System Behavior

Engineered into platform workflows for secure blinding—not managed through manual oversight.

Governance Control Loop



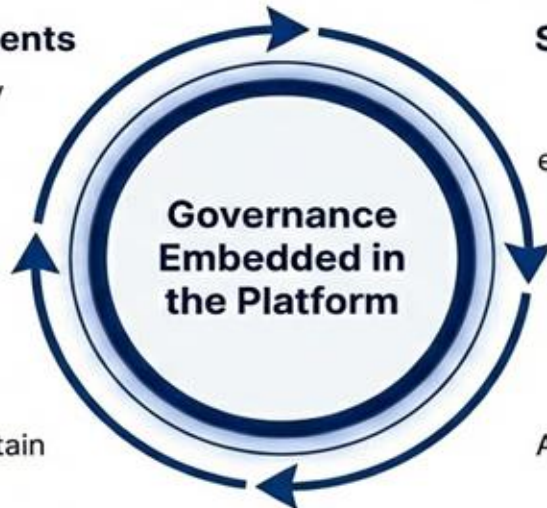
Role-Based Entitlements

Provision access at study start aligned to defined responsibilities.



Periodic Access Certification

Ongoing reviews to maintain least-privilege posture.



Structured Unblinding Workflows

Approval-driven access expansion with full traceability.



Lifecycle-Triggered Permissions

Automated access changes tied to study milestones.



Control Mapping to Key Guidance

Control Area	What the Platform “Must Do”	People &/or Process Controls
Identity, access, segregation	Enforce least privilege roles tied to study state and task. Segregate blinded and unblinded execution contexts, not just datasets.	Define roles and responsibilities. Perform periodic access reviews and remove excess entitlements.
Unblinding entitlements	Require approval for unblinding. Grant time boxed entitlements with constrained scope.	Document unblinding criteria and procedures. Review deviations and escalation thresholds.
Audit trail and metadata review	Generate secure time stamped audit trail events for access changes, workflow approvals, executions, promotions, and releases. Provide interpretable review views and exportable inspection bundles.	Establish an audit trail review SOP with periodic review and escalation. Define what constitutes high risk events and review cadence.
Workflow governance for unblinding	Route unblinding requests through a governed workflow. Capture approvals, scope, rationale, and gate condition. Enforce immutable linkage between approval and execution, including who ran what and what data was used.	Maintain documented unblinding procedures and approval responsibilities. Manage deviations and ensure Quality oversight. Periodically review workflow effectiveness.



Control Mapping to Key Guidance, Continued

Control Area	What the Platform “Must Do”	People &/or Process Controls
Reproducible reporting builds	Record code versions and dependency versions across data, programs, and outputs. Enforce deterministic builds and publish an evidence bundle per run.	Define release management and change control. Manage configuration and versioning with documented approvals.
Controlled output zones and release governance	Enforce export controls and read only review portals. Record release events by zone and audience. Block uncontrolled copying from regulated zones.	Define review and approval workflow for releases and exports. Perform periodic checks of release logs and access.



Demonstrating Compliance and Inspection Readiness



Implementation Paths

Option 01

Vendor Platform With Native Separation and Evidence Bundles

Fastest route to full inspection readiness; look for architectural separation, workflow governance, interpretable audit trails, and push button reporting with evidence packages

Option 02

Build the Capability Internally as Product Functionality

Define clear ownership, roadmap governance, and ongoing funding. Avoid using ad hoc scripts, informal access reviews, etc. because it creates hidden dependencies and accumulate audit debt quickly

Option 03

Operate Manually With Defined Guardrails and a Minimum Evidence Standard

Relies on procedural separation and human review, can be viable for small portfolios or for transitional periods, but it does not scale and it carries predictable schedule and inspection risk



Key Takeaways for Clinical Data Leaders

Demonstrating Compliance and Inspection Readiness



Blinding Must Be Engineered...

Traceability from raw data to blinded and unblinded outputs.



Centralization Requires...

Immutable records of who accessed what and when.



Governance Is Strongest...

Clear linkage between unblinding actions and authorized decisions.



Inspection Readiness...

Proof that controls were tested before production use.

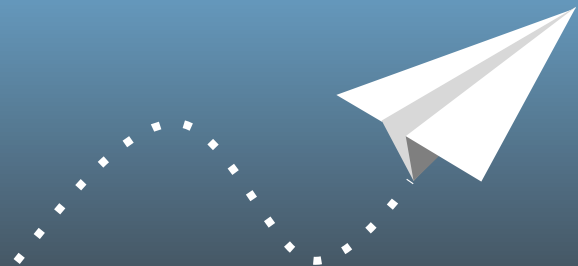


Secure Platforms...

Version-controlled updates demonstrating sustained platform control.



Thank You



<https://www.sycamoreinformatics.com>



Kala Shivali

Kala.Shivali@SycamoreInformatics.com

Sachin Walawalkar

sachin.walawalkar@csllbehring.com