AI-Supported Work Authorization

Gate Decision Record

Use this record to connect evidence to an explicit decision at any stage of the cycle (Stages 0 to 5). It is a proposed operating template, not a regulatory form. Completing reviews, tests, or training does not itself authorize the work. Select a record path in the block below: effort, formality, and documentation should be proportionate to risk, uncertainty, and consequence, consistent with ICH Q9(R1). Sections marked "full path" are omitted on the light path; record the reason for the path selected.

Use ID	Unique identifier linked to the AI Use Inventory
Decision record ID / version	
Stage	☐ 0 Inventory ☐ 1 Define risk ☐ 2 Authority/records ☐ 3 Test ☐ 4 Routine use ☐ 5 Change/correct/retire
Decision requested	Register, contain, prohibit, authorize pilot, correct and retest, authorize routine use, continue under conditions, expand, narrow, reinstate, suspend, stop, or retire
Decision date / effective date	
Next review date or trigger	
Record path	☐ Light path: complete Sections 1, 2, 6, 7, and the revision history in Section 10. Available when failure cannot affect product quality, patient safety, data integrity, or a regulated record; the system cannot create, change, approve, or release a record; and a qualified person verifies every output before use. ☐ Full path: complete Sections 1 to 10. Required for any GxP-consequential output, any write, execute, or approve authority, any Part 11 record, or any agent.
Inventory entry reference	AI Use Inventory row identifier and the inventory version this record was prepared from
Prepared by / date	Name, role, and date of the person who compiled this record; preparation is not approval

Handling note

Do not enter passwords, API keys, access tokens, full personal data, protected record content, or confidential prompts. Cite controlled repositories and evidence identifiers. Store this record under the applicable access, retention, and signature controls.

1. Bounded use and decision context

AI-supported task	Describe the specific work, not a general platform or vendor
Expected output and downstream decision	State what the output supports and who decides
Named process, product, site, and jurisdiction	State what is inside and outside scope
System, model, version, interface, and configuration	Record the qualified state and evidence reference
Source boundary	Systems, repositories, document status, inclusion rules, exclusions, and unavailable sources
Users and assigned roles	Identify operators, reviewers, approvers, administrators, and support roles
Authority Envelope	What the system may read, draft, recommend, change, execute, or approve
Prohibited actions and technical enforcement	Describe permissions, identity, approval checks, and stop controls
Authority Envelope reference	Identify the approved Authority Envelope record and version covering identity, permitted users, accessible sources, allowed and conditional operations, prohibited actions, technical enforcement, stop and recovery, and change triggers
Failure consequences	Product quality, patient safety, data integrity, compliance, privacy, security, or availability
Records and signatures	Predicate-rule basis, Part 11 determination, required evidence, retention, and electronic-signature use

2. Accountability

Role	Name / function	Responsibility for this decision	Conflict / independence note
Process owner			
Quality owner / quality unit			
System owner			
Data owner			
Evaluation owner			
IT / security / privacy			
Supplier / external party			

3. Evidence reviewed · full path

Evidence / control	Status / reviewer	Reference
☐ Current AI Use Inventory entry and ownership		
☐ Intended use, baseline process, risk assessment, and applicable requirements		
☐ Data map, source inventory, inclusion rules, and evidence identity		
☐ Approved Authority Envelope: authority design, access controls, prohibited actions, technical enforcement, and segregation of duties		
☐ Part 11 / electronic-record and signature determination where applicable		
☐ Security, privacy, and third-party dependency review		
☐ Supplier evidence and change-notification responsibilities		
☐ Representative challenge cases, scoring rubric, and protected holdout evidence		
☐ Human reviewer qualification and assessor calibration		
☐ Recovery, duplicate request, interrupted execution, and partial-success tests		
☐ Pilot results, critical failures, near misses, overrides, workload, and user feedback		
☐ Benefit and burden: time to acceptable work, correction, escalation, maintenance, and rework		
☐ Change impact, regression evidence, requalification, continuity, and retirement plan		

4. Security, privacy, and data-integrity disposition · full path

Authentication and identity	Identify the user/system identity and whether a handle, URL, shared credential, or weak bearer identifier creates exposure
Access and least privilege	Show that technical permissions match the Authority Envelope; instructions alone are insufficient
Data classification and privacy	State personal, confidential, GxP, or cross-border data; identify minimization and approved storage
Third-party and script dependencies	List suppliers, integrations, embedded services, external scripts, and change/incident responsibilities
Decision provenance and audit evidence	Inputs, versions, retrievals, output, changes, human reasons, approvals, and resulting state
Retention and uncontrolled copies	Keep enough evidence to explain the decision without indiscriminate logging
Incident, stop, and recovery controls	Detection, containment, reconciliation, compensating action, notification, and suspension authority
Security / privacy disposition	☐ Acceptable ☐ Acceptable with actions ☐ Not acceptable ☐ Not applicable; cite reviewer and evidence

5. Evaluation findings and uncertainty · full path

Evaluation design	Conditions compared, sample, case classes, versions, reviewer instructions, blinding, and holdout protection
Predefined thresholds and critical failures	Cite the approved scoring sheet and decision rules
Scoring sheet identity	Scoring sheet ID, version, and file hash or controlled location
Evaluation collection frozen	Date frozen and the name and role of the person who froze it, confirming that no results had been read at that point. The same freeze date must also be recorded in the evaluation scoring sheet (in the GxP Frame AI Workflow Evaluation Scoring Sheet v1.2, this is the Gate summary block, cell B11); the two entries must match, and any discrepancy must be resolved and explained before the decision is made.
Critical-failure mapping confirmed	Name, role, and date of the person who confirmed the critical-failure mapping against the approved rubric definitions, independent of the evaluation owner
Deviations from the frozen design	Each deviation, the reason, who approved it, and when
Results	Completed cases, date scored for each case (in the GxP Frame scoring sheet v1.2, Case scoring column AG), the condition being authorized (Gate summary B15), the holdout 95% upper bound (Gate summary B23), average score, critical failures, disagreements, withdrawals, and time to acceptable output
Important failure modes	Consequential omissions, unsupported conclusions, rejected correct work, unnecessary escalation, and recovery failures
Reviewer performance and workload	Competence, evidence access, review time, queue, escalation patterns, and practical authority
Benefit and cost	Compare the complete job with the baseline, including control and maintenance burden
Limitations and unresolved uncertainty	State what was not tested, small-sample uncertainty, unavailable evidence, or supplier constraints
Corrective actions required before decision	Owner, due date, evidence needed, and whether use remains restricted

6. Gate decision

Select one decision. The written scope and conditions govern; the checkbox alone is not authorization.

☐ Register / assign ownership	☐ Contain or prohibit	☐ Authorize bounded pilot	☐ Correct and retest	☐ Continue under conditions	
☐ Authorize routine use	☐ Authorize expansion	☐ Narrow or restrict	☐ Suspend / stop	☐ Reinstate	☐ Retire

Decision rationale	Explain how the evidence supports the decision and identify contrary evidence
Authorized scope	Task, sources, system/version, users, site/product, authority, operating hours, and output destination
Conditions and open actions	Owner, due date, evidence required, and consequence of non-completion
Accepted residual risk	Remaining risk after controls, why it is acceptable for the authorized scope, compensating controls, the owner accepting it, and the date and trigger for re-review
Monitoring	Consequential performance, drift indicators, incidents, near misses, overrides, workload, and user feedback
Stop or restriction criteria	State the finding, threshold, incident, or unavailable control that triggers action
Change and re-review triggers	Model/version, retrieval, interface, procedure, product/site, staff, permission, supplier, or regulation
Records, retention, and investigation access	Regulated-record determination, linked evidence and provenance records, retention location and period, and how records are retrieved for investigation or inspection
Effective period / expiry	State when the decision must be reconsidered even if no trigger occurs

7. Accountable approvals

Use the organization's approved approval and electronic-signature system where required. This Word template is not itself configured or validated as a Part 11 system. By approving, the accountable process and quality owners confirm that the technical permissions and operating controls match the referenced Authority Envelope. Any expansion beyond the recorded boundary requires a new decision before use.

Role	Name / title	Decision / signature reference	Date
Process owner			
Quality owner / quality unit			
System owner (as applicable)			
Data owner / privacy / security (as applicable)			

8. Authority Envelope · full path

Define permission separately from technical capability. The boundary below must be specific enough to configure, test, monitor, and inspect. A prompt instruction is not an authority control while the technical permission remains available.

Envelope element	Authorized boundary	Evidence that enforces or verifies it
Identity and version	System/service identity, model and configuration version, environment, integration versions, and accountable system owner	Approved configuration baseline; change-control record
Permitted users and roles	Who may initiate, review, approve, administer, or support the workflow; segregation-of-duties limits	Role matrix; account/role configuration; training or qualification record
Accessible sources	Named systems, repositories, data classes, sites/products, document statuses, and exclusions	Access review; source inventory; retrieval or integration configuration
Allowed operations	Read, retrieve, transform, draft, classify, recommend, create, update, notify, or execute only if approved	Least-privilege configuration; workflow design; action logs
Conditional actions	Actions allowed only after a named approval, a state check, a validated confidence threshold where one exists, or a staffed-period restriction	Approval-state binding; operational checks; tested scenarios
Prohibited actions	Actions the workflow must never perform, including any approval, release, disposition, record change, notification, or external action outside scope	Denied permissions; negative test evidence; monitoring alert
Technical enforcement	Service identity, authentication, access controls, action checks, rate/volume limits, and separation from the initiating user's privileges	Configuration evidence; security review; test results
Stop, recovery, and escalation	Who can suspend use; automatic stop conditions; recovery/reconciliation method; contact path outside normal operating hours	Recovery test; incident procedure; on-call or staffing arrangement
Change and review triggers	Events requiring reassessment: model, prompt/configuration, source, interface, user role, product/site, volume, or permission change	Change-control linkage; review date; monitoring plan

Approval statement: the accountable process and quality owners confirm that the technical permissions and operating controls match this Authority Envelope. Any expansion beyond the recorded boundary requires a new decision before use.

9. Attachments and superseded records · full path

Attachments / evidence index	List controlled identifiers and locations; do not embed protected source records here
Superseded decision records	List the decision record IDs and versions this record replaces, and where they are retained

10. Revision history

Version	Date	Change / reason	Approved by
1.1	19Sep2026	Aligned to Governing AI in Pharmaceutical Operations v2.2: added accepted residual risk, records/retention and Authority Envelope entries; added 'continue under conditions' decision option.	Brian Drapeau 19Sep2026
1.2	19Sep2026	Added Section 8 Authority Envelope with approval statement; revision history now required on both record paths; attachments index marked full path; corrected document title metadata.	Brian Drapeau 19Sep2026
1.3	19Sep2026	Added evaluation integrity attestation to Section 5: scoring sheet identity and version, holdout freeze date and signer, independent confirmation of the critical-failure mapping against the rubric, and deviations from the frozen design.	Brian Drapeau 19Sep2026
1.4	19Sep2026	Section 5: freeze date cross-linked to the evaluation scoring sheet (Gate summary B11) with a requirement that the two match; per-case date scored (Case scoring column AG) added to the results fields.	Brian Drapeau 19Sep2026
1.5	19Sep2026	Corrected linked-template version references to the AI Workflow Evaluation Scoring Sheet v1.1 and Governing AI in Pharmaceutical Operations v2.2.	Brian Drapeau 19Sep2026
1.6	19Sep2026	Removed document editing restriction so the record can be completed; organizations apply their own protection at local issue. Section 5 references updated to AI Workflow Evaluation Scoring Sheet v1.2 and its condition (B15) and holdout bound (B23). File properties corrected; punctuation normalized.	Brian Drapeau 19Sep2026

Template basis: Brian Drapeau, Governing AI in Pharmaceutical Operations, version 2.2 (September 19, 2026), AI-Supported Work Authorization Cycle, Appendix A (Gate Decision Record) and Appendix B (Authority Envelope). Security prompts reflect the supplied September 18, 2026 review of gxpframe.com and lifesciencesai.academy; users must perform a current, use-specific assessment.