IntuitionLabs

INTUITIONLABS / RESEARCH & PRACTICAL GUIDANCE

ICH E6(R3) Annex 2: DCT, Pragmatic & RWD Crosswalk

> Build practical AI for pharma and biotech with IntuitionLabs. We help life-science teams turn complex information and workflows into useful software, governed knowledge systems and AI tools.

Published by IntuitionLabs · 2026-09-19 · ich e6(r3) annex 2 · decentralized clinical trials · pragmatic clinical trials · real world data · good clinical practice · digital health technologies · clinical data governance · eclinical architecture · rwd fitness for purpose

Original article: https://intuitionlabs.ai/articles/ich-e6-r3-annex-2-implementation-crosswalk

In this article

Executive Summary

ICH E6(R3) Annex 2 is the final international Good Clinical Practice (GCP) framework for trials that incorporate decentralized elements, pragmatic elements, or real-world data (RWD). The International Council for Harmonisation (ICH) adopted the Step 4 text on **3 June 2026** (database.ich.org). The European Medicines Agency (EMA) records Committee for Medicinal Products for Human Use adoption on **25 June 2026** and EU effectiveness on **15 January 2027** (ema.europa.eu) (ema.europa.eu). In contrast, FDA's regional page still announced **draft guidance** as of 19 September 2026 (fda.gov). Global programs therefore need a common ICH control model plus a jurisdiction-specific adoption register.

Annex 2 does not approve a methodology. It requires the protocol to justify its use and address **rationale, fitness for purpose, and feasibility** (ema.europa.eu). Operational readiness therefore turns on evidence and ownership, not labels. Remote consent needs identity assurance and an accessible alternative. Distributed trial work needs proportionate investigator oversight. Direct-to-participant investigational product (IP) logistics need recipient verification, storage and return controls. DHT, electronic health record (EHR), registry, and claims flows need validated interfaces, provenance, metadata, audit trails, access control, and durable retention.

The empirical evidence explains why these controls matter. A review of **254** phase 2 to 4 protocols found decentralized data collection in **68.9%**, including telemedicine in **52.4%** (bmjopen.bmj.com) (bmjopen.bmj.com). A later review found retention or attrition difficulties in **19 of 53** decentralized studies (bmjopen.bmj.com). An EHR substudy reported **81.3% to 98.7%** categorical agreement and **95.8%** exact matches for assessed continuous-variable cases (link.springer.com) (link.springer.com). The implementation priority is thus early qualification, not retrospective repair.

The practical decision rule is a documented readiness score: completed applicable controls divided by total applicable controls. A control is not applicable only when its triggering element is absent, with rationale and approval recorded. **Any open critical control blocks readiness**, regardless of the percentage. This approach gives clinical operations, quality, data governance, and eClinical architecture a shared release decision before the EU date.

Introduction and Background

Annex 2 should be read with the **E6(R3) Principles and Annex 1**, not as a standalone DCT manual. It covers trial designs that "incorporate decentralised elements, pragmatic elements and/or real-world data" (database.ich.org). It also states that the annex should not be read as endorsement of any methodology (database.ich.org). This distinction prevents two common errors: treating "decentralized" as a compliance claim, and treating routine-care data as automatically fit for a regulatory trial.

The annex describes a **decentralized element** as an activity outside the investigator's location (database.ich.org). It defines pragmatic elements as integrating aspects of usual clinical practice (ema.europa.eu). RWD are patient-health data from sources outside clinical trials (ema.europa.eu). These categories overlap, but they trigger different controls.

The operating question is whether the proposed element can be executed with participant protection, reliable results, and reconstructable evidence across every organization and system involved. That question is narrower than whether a platform is available, and broader than whether one validation package exists. It requires clinical operations to map the journey, quality to define evidence and criticality, data governance to qualify sources and transformations, and technology owners to demonstrate secure, recoverable flows. The crosswalk below keeps those decisions tied to the methodology and the party that can actually control the risk.

For an adjacent consultancy, the useful role is translating regulatory text into accountable system and process decisions. IntuitionLabs describes its data work as "data pipelines, integration, warehousing, and business intelligence" (intuitionlabs.ai) and its implementation work as integration of enterprise systems (intuitionlabs.ai). Those capabilities can support evidence mapping and control design, but the sponsor, investigator, institutional review board or independent ethics committee (IRB/IEC), and data custodian retain their defined responsibilities.

Key Changes

Finalization and regional status

The finalization timeline separates **international harmonization** from **regional effect**:

- **ICH Step 4:** Adoption occurred on 3 June 2026 (database.ich.org).
- **European Union:** CHMP adoption followed on 25 June 2026, with effectiveness on 15 January 2027 (ema.europa.eu) (ema.europa.eu).
- **United States:** FDA's Annex 2 page still announced the availability of draft guidance at the publication cutoff (fda.gov).
- **Australia:** TGA said it would use its standard consultation process before adoption (tga.gov.au).
- **Canada:** Health Canada states E6(R3) implementation on 1 April 2026, but its index does not separately confirm the later final Annex 2 (canada.ca).

The implication is simple: maintain an adoption matrix by jurisdiction, submission, site, and activity. Do not encode Step 4 as a universal legal effective date.

A methodology-by-control crosswalk

Table 1 summarizes the distinct control logic for decentralized, pragmatic, and RWD elements.

Methodology	Trigger and evidence question	Core controls	Release evidence
Decentralized	Is any consent, visit, measurement, sample, safety contact, or IP activity outside the investigator's location?	Identity assurance, remote communication, alternative access, DHT qualification, shipping chain, local-provider agreement, safety escalation, investigator visibility.	Approved workflow, identity test, device evidence, shipment simulation, escalation test, investigator dashboard and oversight record.
Pragmatic	Does the protocol incorporate usual-care people, pathways, systems, or decisions?	Protocol clarity, role boundaries, data sharing, record retention, usual-care variability, intervention fidelity, safety routing.	Care-pathway map, healthcare-professional agreement, minimum dataset, deviation logic, safety routing test.
Primary RWD collection	Are data prospectively gathered under the protocol from routine settings or technologies?	Protocol-defined collection, participant-facing information, fit-for-purpose instrument, metadata, missing-data prevention.	Data specification, validated collection method, provenance fields, reconciliation and monitoring plan.
Secondary RWD use	Were data originally collected for another purpose?	Source qualification, relevance, reliability, lawful access, provenance, transformation, linkage, completeness, validation status, refresh governance.	Custodian agreement, data dictionary, source assessment, linkage validation, transformation lineage, quality report and refresh freeze.

Primary collection means prospective gathering under the protocol (ema.europa.eu). Secondary use means data originally collected for another purpose (ema.europa.eu). The distinction affects how much control can be designed prospectively. It does not create a lower quality threshold for secondary data.

Responsibilities follow the activity

Annex 2 makes distributed execution compatible with retained accountability. The investigator must maintain appropriate and proportionate oversight (database.ich.org). Arrangements with usual-care professionals should define data sharing and record retention (database.ich.org). The sponsor must maintain service-provider oversight (database.ich.org). A contract can allocate work, but not erase these accountabilities.

Data fitness becomes a life-cycle decision

For RWD, fitness for purpose includes **provenance, traceability, and relevance** (ema.europa.eu). Assessment should consider variable formats and structures (ema.europa.eu), collection-system validation status (ema.europa.eu), and accurate person-level matching when sources are linked (ema.europa.eu). FDA likewise describes data-quality evaluation as ongoing, not one-time (fda.gov).

Implementation Considerations and Process Changes

Remote consent and identity

Remote consent is a controlled process, not merely an electronic signature. When it is used, the investigator should assure the identity of the participant or legally acceptable representative (database.ich.org). HHS guidance reinforces that responsibility remains with the investigator and cannot be delegated to the electronic system (hhs.gov) (hhs.gov).

The minimum control set should include:

- **Identity proofing:** Define acceptable evidence, exceptions, failed-proofing escalation, and re-authentication for amendments.
- **Comprehension:** Test content, language, accessibility, question handling, and confirmation of understanding.
- **Alternatives:** Offer paper or in-person consent where feasible (database.ich.org).
- **Disclosure:** Explain data uses and who will have access (database.ich.org).
- **Evidence:** Preserve version, timestamp, signer, authentication method, discussion record, copy delivery, withdrawal, and re-consent history.

Comprehension cannot be assumed from completion. A meta-analysis of **117 studies, 155 datasets, and 22,118 participants** found particularly low understanding for placebo and randomization concepts (journals.plos.org) (journals.plos.org). A 2025 decentralized-trial review found eConsent in **41 of 49** studies assessed for methods (bmjopen.bmj.com).

Investigator oversight beyond the site

The oversight design should give the investigator timely visibility into clinical status, safety signals, completion, deviations, and escalations. For participant safety, Annex 2 expects review of health-status information across available sources (database.ich.org). The sponsor needs processes that make decentralized or pragmatic safety information accessible to the investigator promptly (ema.europa.eu).

- **Activity inventory:** List who performs each activity, where, under whose instruction, and in which source system.
- **Competency:** Define qualification and training evidence for mobile staff, local professionals, laboratories, couriers, and support desks.
- **Visibility:** Give the investigator role-appropriate, timely access to critical data and unresolved alerts.
- **Escalation:** Set safety, technical, privacy, and IP thresholds, with acknowledgement and closure times.
- **Evidence of review:** Record meaningful investigator assessment, not only passive system access.

MHRA's EHR position is consistent: the investigator should be able to demonstrate medical oversight (assets.publishing.service.gov.uk).

Investigational product and safety logistics

Direct-to-participant IP introduces custody and environmental controls. The process must address **receipt, storage, handling, administration, return, and disposition** (database.ich.org). It should confirm receipt by the intended participant or authorized designee (database.ich.org). The investigator retains responsibility for safe and appropriate use even when the sponsor arranges shipment (database.ich.org).

A release simulation should test:

- **Prescription and authorization:** Correct participant, dose, schedule, destination, and jurisdiction.
- **Packaging and transport:** Temperature, light, tamper evidence, chain of custody, and excursion handling.
- **Receipt and storage:** Identity verification, acknowledgement, participant instructions, and restricted access.
- **Administration:** Training, adherence, error reporting, and rescue pathway.
- **Reconciliation:** Shipment, dispense, use, return, destruction, and exception records.
- **Safety:** Prompt routing from participant, DHT, local clinician, laboratory, and support provider to the investigator.

Privacy and cybersecurity

Remote collection expressly requires cybersecurity and privacy controls (ema.europa.eu). European data protection by default limits processing to necessary data (commission.europa.eu), and high-risk processing should have a data protection impact assessment before processing begins (commission.europa.eu). NIST Cybersecurity Framework 2.0 provides six outcome functions and adds **Govern** (nist.gov) (nist.gov).

The trial security profile should cover:

- **Govern:** Named risk owner, asset inventory, provider duties, threat review, and exception approval.
- **Protect:** Least privilege, multifactor authentication, encryption at rest and in transit, device configuration, and secrets management.
- **Detect:** Security logging, anomalous-access monitoring, integrity checks, and alert routing.
- **Respond:** Containment, trial impact assessment, participant communication decision, and evidence preservation.
- **Recover:** Tested backup, data reconciliation, safe resumption, and post-event control review.
- **Minimize:** Collect only protocol-required information. EMA states “required by the protocol and not more” (ema.europa.eu).

Responsible-Party Governance

Table 2 is a practical RACI-style ownership map. **A** means accountable, **R** responsible for execution, **C** consulted, and **I** informed. Local law and the protocol may require a different assignment, but accountability should never be blank.

Control	IRB/IEC	Investigator	Sponsor	Provider or data custodian
Methodology suitability and participant protections	A/R for ethical review	R for submission and local feasibility	A/R for design evidence	C
Remote consent, identity, and alternatives	C	A/R	R for platform and process design	R for configured service
Distributed activity and safety oversight	I	A/R	A/R for governance and information flow	R within contracted scope
DHT selection, verification, validation, and support	I	C/R for clinical use	A/R	R for technology evidence and operations
RWD access, provenance, transformation, and linkage	I	C	A/R	R for source, extraction, metadata, and records
IP shipment and accountability	I	A/R for safe use	A/R for arranged logistics	R for assigned custody steps
Privacy, security, retention, and continuity	C	R for site controls	A/R for trial-wide design	R for platform and custodian controls

IRB/IEC review should receive enough information to evaluate the methodology (database.ich.org). Its attention includes privacy, confidentiality, and data security (database.ich.org). The sponsor should establish clear communication lines and maintain oversight of providers and their essential records (database.ich.org) (ema.europa.eu).

For externally controlled RWD, contracts need actual data access and use rights (ema.europa.eu). Sponsor accountability persists through extraction, linkage, and transformation (ema.europa.eu). The custodian should supply dictionaries, refresh history, quality procedures, linkage method, audit evidence, and retention commitments, not only a dataset.

Each owner should produce evidence appropriate to the responsibility:

- **IRB/IEC:** Written review procedures, methodology-specific submission requirements, qualification review, privacy and security considerations, and documented decisions. HHS calls for initial and continuing review procedures and staff-qualification review (hhs.gov) (hhs.gov).
- **Investigator:** Identity assurance, consent discussion, delegation, clinical review, safety acknowledgement, IP accountability, and documented oversight. HHS says electronic consent authority cannot be delegated to the system and the signer must be the intended participant or representative (hhs.gov) (hhs.gov). MHRA expects demonstrable medical oversight (assets.publishing.service.gov.uk).

- **Sponsor:** Protocol rationale, quality-risk decisions, provider qualification, system validation, data-flow specification, access governance, monitoring, and issue closure. FDA identifies documented data collection, handling, security, and management procedures, along with validation evidence and continuity plans (fda.gov) (fda.gov) (fda.gov).
- **Technology provider:** Requirements traceability, configuration, validation support, audit logging, access control, release evidence, availability, recovery, export, and essential-record retention. FDA recommends secure transfer to a durable repository, controlled DHT access, and safeguards for data at rest and in transit (fda.gov) (fda.gov) (fda.gov).
- **Data custodian:** Source definitions, collection context, dictionary, coverage, refreshes, quality checks, lineage, linkage, access, retention, and change notification. FDA expects origin information for each registry element, periodic quality assessment, interoperability testing, and version control (fda.gov) (fda.gov) (fda.gov) (fda.gov).
- **Security and privacy owners:** Data minimization, purpose, identity, authorization, transmission, audit, response, recovery, retention, and impact assessment. HHS calls for identity verification and transmission security (hhs.gov) (hhs.gov). NIST organizes governance and operational outcomes but does not prescribe how they must be achieved (nist.gov).

System-Control Architecture

An Annex 2 architecture should make the path from participant or routine-care event to analysis reproducible. EMA expects a detailed electronic-data transmission diagram (ema.europa.eu); FDA similarly recommends a flow from creation to final storage (fda.gov).

Table 3 converts common data flows into testable controls.

Flow	Principal risk	Required architecture evidence	Operational test
DHT to gateway to cloud to clinical repository	Wrong participant, clock drift, firmware change, loss, duplication, insecure transfer	Device identity, participant binding, firmware and algorithm version, timestamps, transmission status, encryption, durable raw and derived data	Simulate offline use, duplicate upload, clock change, replacement device, alert and recovery
EHR to extract-transform-load pipeline to EDC or lakehouse	Unstable source meaning, undocumented mapping, refresh drift, incomplete capture	Source dictionary, extraction specification, terminology mapping, interface validation, lineage, refresh version, reconciliation	Reperform a sample from source to analysis and reconcile missing or transformed fields
Registry or claims to linkage service to analysis dataset	Wrong-person linkage, lag, missing outcomes, changing coverage	Eligibility and relevance assessment, linkage variables, match thresholds, quality report, provenance, cutoff and version	Validate matched and unmatched samples, assess false match risk, rerun quality rules after refresh
eConsent to identity service to trial master file	Impersonation, wrong form version, incomplete discussion evidence	Identity method, role binding, form version, signature timestamp, discussion and copy-delivery evidence, amendment history	Test failed identity, interrupted session, corrected signature, withdrawal, re-consent and export

Flow	Principal risk	Required architecture evidence	Operational test
Remote provider or laboratory to safety workflow	Delayed or fragmented safety information	Source-to-investigator routing, urgency classification, acknowledgement, reconciliation, downtime path	Inject representative safety scenarios and measure receipt, assessment, escalation and closure

The architecture baseline includes:

- **Validated interfaces:** EMA expects system interfaces to be clearly defined and validated (ema.europa.eu).
- **Traceable transformations:** Preserve lineage through derivations and transformations (ema.europa.eu).
- **Device metadata:** Automated measurements should carry metadata about the device (ema.europa.eu).
- **Auditability:** Audit trails should be secure, computer-generated, and timestamped (ema.europa.eu).
- **Controlled change:** Maintain formal change control, impact assessment, validation evidence, and release approval (ema.europa.eu).
- **Segregated access:** Base access on duties, and generally use two-factor authentication where selected by risk assessment (ema.europa.eu) (ema.europa.eu).
- **Continuity:** Document migration, retention, backup, recovery, and contingency arrangements (fda.gov).
- **Standards:** Use a model that transports data with metadata, reference data, administration, and audit information. CDISC Operational Data Model 2.0 supports these elements (cdisc.org).

For a DHT, qualification is use-specific. FDA frames selection around fitness for purpose, expects verification and validation regardless of device classification, and calls for access control and cybersecurity safeguards (fda.gov) (fda.gov) (fda.gov). Storage capacity and transmission frequency should minimize missing data (fda.gov).

For EHR, claims, or registry data, a common data model may improve interoperability, but it does not prove semantic equivalence or completeness (fda.gov). Registry reliability includes accuracy, completeness, and traceability (fda.gov). Access controls and audit trails should demonstrate provenance (fda.gov).

Data Analysis and Evidence

The evidence base shows broad use but uneven operational maturity. In **254** protocols from 2019 and 2020, **68.9%** reported decentralized data collection. Telemedicine appeared in **52.4%**, patient-reported outcomes in **41.7%**, and devices or biomarker kits in **15.8%** (bmjopen.bmj.com) (bmjopen.bmj.com). Decentralized consent rose from **4.2%** to **20.9%** across the study period (bmjopen.bmj.com).

Implementation is not frictionless. A review of **53** completed decentralized studies found eConsent in **41 of 49** assessed studies, retention or attrition difficulty in **19 of 53**, and home-monitoring data problems in three studies (bmjopen.bmj.com) (bmjopen.bmj.com) (bmjopen.bmj.com). A separate review of **45** randomized

decentralized trials classified **62%** as fully remote and found external vendors in **44%** (pmc.ncbi.nlm.nih.gov) (pmc.ncbi.nlm.nih.gov). These data support formal provider oversight, continuity testing, and participant support.

Pragmatic scale can be much larger. ADAPTABLE approached about **450,000** people, randomized **15,076**, and followed them for a median **26.2 months** (nejm.org) (nejm.org). A 2025 review of **22** pragmatic use cases found randomization in **21**, RWD in half, and participant counts from **450 to 39,600** (ascpt.onlinelibrary.wiley.com) (ascpt.onlinelibrary.wiley.com).

The **VESALIUS-CV** EHR substudy provides a concrete data-quality example: **75 participants at nine sites**, **81.3% to 98.7%** agreement for categorical baseline variables, and **95.8%** exact matches for assessed continuous-variable cases (link.springer.com) (link.springer.com) (link.springer.com). High agreement is encouraging, but the range illustrates why source-specific qualification and reconciliation remain necessary.

Taken together, the studies do not establish a universal performance advantage for any methodology. They show that remote execution is already common, that large pragmatic enrollment is feasible, and that data concordance can be high in a qualified setting. They also show why readiness cannot be inferred from adoption. Consent completion does not establish understanding, an external vendor does not establish sponsor oversight, and a common data model does not establish that a required outcome is present or clinically equivalent.

The evidence therefore supports three planning choices. First, qualify the source and technology before final protocol dependency makes replacement costly. Second, define missingness, latency, reconciliation, and participant-support indicators before first enrollment. Third, preserve enough metadata to stratify performance by site, device version, provider, source refresh, and participant pathway. These measures let the team distinguish random variation from a controllable process issue and decide whether a corrective action, protocol amendment, or alternative collection route is needed.

Readiness Assessment Before EU Effectiveness

The gap assessment should begin with an **element inventory**, not a document inventory. For each participant journey, identify the location, performer, technology, source record, transfer, decision, and accountable owner. This prevents a protocol that mentions “remote visits” from obscuring separate consent, laboratory, DHT, shipment, safety, and support workflows. Decentralization is a continuum rather than an all-or-nothing design (frontiersin.org).

Eight work packages create a usable evidence set:

- **Design justification:** Link each decentralized, pragmatic, or RWD element to a trial objective, participant need, operational constraint, and critical-to-quality factor. Record rejected alternatives and residual risks. NICE summarizes data fitness through quality and relevance (nice.org.uk). Swissmedic also expects identification of sources and applied data standards (swissmedic.ch).
- **Ethics package:** Give the IRB/IEC diagrams, participant materials, identity method, privacy analysis, data-access explanation, burden assessment, alternative pathway, and provider roles. HHS expects written procedures for initial and continuing review and review of staff qualifications (hhs.gov) (hhs.gov).

- **Participant pathway:** Walk through recruitment, proofing, consent, training, access support, visits, sampling, safety contacts, returns, withdrawal, and closeout. Technology access should not itself become an exclusion criterion (frontiersin.org). A 2026 program analysis covered **7,469 participants in 765 decentralized trials**, showing the scale at which pathway consistency can matter (jamanetwork.com). In that program, **29.6%** of first-quarter 2025 participants lived more than 120 miles from an academic site (jamanetwork.com).
- **Data-source qualification:** Define concepts, population, capture process, coding, latency, history, coverage, completeness, accuracy, plausibility, validation, refresh, and change notification. FDA recommends evaluating completeness, accuracy, and plausibility, including verification against original sources (fda.gov). CDISC identifies traceability as fundamental to data quality (cdisc.org).
- **Technology assurance:** Tie intended use to requirements, verification, validation, usability, configuration, version, cybersecurity, technical support, data export, and decommissioning. A 2026 review included **48** sensor-based DHT studies, of which **38** collected physiological data and **12** described sensor-based outcomes (nature.com) (nature.com) (nature.com).
- **Provider assurance:** Inventory subcontractors, fourth parties, locations, access, records, continuity, security, service levels, audit rights, transition assistance, and exit data. MHRA says backup and recovery should be validated and periodically tested (assets.publishing.service.gov.uk). It also expects archive arrangements that permit recovery and readability (assets.publishing.service.gov.uk).
- **Privacy and security:** Document lawful basis, purpose, minimization, role-based access, identity, encryption, logging, transfer, retention, deletion, incident workflow, and impact assessment. HHS requires controls that allow only authorized people to access electronic protected health information and mechanisms that record system activity (hhs.gov) (hhs.gov). Swissmedic expects appropriate consent and de-identification controls for RWD (swissmedic.ch).
- **Operational qualification:** Execute integrated scenarios with expected results, evidence capture, defects, retest, accountable approval, and a monitored production baseline. FDA identifies risk assessment, validation plans, execution, and reports as validation documentation (fda.gov). MHRA expects validation and procedures for change and system failure (assets.publishing.service.gov.uk).

A numerical score supports governance only when the denominator is controlled. **Readiness calculation (Hypothetical Example):** suppose **64** controls are identified, **8** have approved not-applicable rationales, and **49** of the remaining **56** are complete. Readiness is **49 / 56 = 87.5%**. The score does not authorize launch if one of the seven open controls is critical. Conversely, teams should not inflate the denominator with generic controls unrelated to the actual design. Quality should approve applicability, evidence criteria, criticality, and closure.

The final review should produce four signed outputs: an applicability matrix, a control-owner map, an evidence index, and a residual-risk decision. These records make the readiness conclusion reproducible and allow future protocol amendments, provider changes, and source refreshes to trigger targeted reassessment instead of a wholesale restart.

Implications and Future Directions

Readiness should be measured at the **control level**, not by declaring a trial decentralized, pragmatic, or RWD-enabled. Use this calculation:

Readiness percentage = completed applicable controls / total applicable controls x 100

- **Complete:** Evidence exists, is approved by the accountable owner, and passed its defined test.
- **Incomplete:** Evidence is missing, draft, unapproved, untested, or has an open material exception.
- **Not applicable:** The triggering element is absent, and the rationale is documented and approved.
- **Critical gate:** Any open critical control blocks operational readiness even if the calculated percentage is high.

Suggested critical gates are valid consent and identity, timely safety flow, investigator oversight, IP chain of custody, critical-data provenance, validated critical interfaces, privacy authorization, security safeguards, and recoverability. This calculation is an internal decision method, not an external benchmark.

A practical pre-15 January 2027 program can proceed in five increments:

1. **Inventory:** Map every remote activity, usual-care dependency, RWD source, technology, provider, jurisdiction, and data transfer.
2. **Classify:** Mark each Annex 2 control as applicable, not applicable with rationale, or unresolved.
3. **Assign:** Name one accountable owner and execution owners for every applicable control.
4. **Test:** Run end-to-end scenarios for consent, DHT loss, missing transmission, EHR refresh, safety escalation, IP excursion, provider downtime, and recovery.
5. **Release and monitor:** Approve only when critical gates close, then track measurable indicators. UK guidance describes key risk indicators as early warnings of emerging issues (gov.uk).

The direction of travel is toward reusable, governed data infrastructure. NIH's Data COUNTS initiative, for example, describes a federated zero-trust architecture and preservation of EHR provenance and lineage (nih.gov) (nih.gov). Reuse can reduce repeated integration work, but every protocol still needs its own fitness-for-purpose justification.

Readiness also sits inside broader trial governance. WHO describes development of international trial-registration norms in **2006** (who.int), while CISA describes its cross-sector goals as a baseline set of cybersecurity practices (cisa.gov). Neither replaces Annex 2, but each can anchor an adjoining control family.

Conclusion

ICH E6(R3) Annex 2 is a control framework for modern trial elements, not a general endorsement of decentralization, pragmatic design, DHTs, EHR extraction, or secondary RWD. Its practical demand is that the chosen method be justified, feasible, fit for purpose, and governed through retained sponsor and investigator accountability.

For EU/global planning, **3 June 2026** is the ICH Step 4 date, **25 June 2026** is the CHMP adoption date, and **15 January 2027** is the EU effective date. FDA's regional Annex 2 status remained draft at the 19 September 2026 cutoff. These milestones belong in separate fields, not one global status flag.

The implementation crosswalk yields a clear sequence: identify the methodological trigger, map the responsible parties, qualify the data and technology, test the complete operational flow, and retain evidence of review. Remote consent requires identity and comprehension controls. Distributed activity requires real investigator visibility. DHT and EHR flows require metadata, validation, lineage, controlled change, and recovery. Secondary RWD requires source access, relevance, reliability, linkage assurance, and continuing quality assessment. Direct IP shipment requires end-to-end custody and reconciliation.

The recommended release decision is a transparent score of completed applicable controls divided by total applicable controls, combined with non-negotiable critical gates. That structure turns Annex 2 from a broad compliance narrative into a traceable operational decision for clinical operations, quality, data governance, and eClinical architecture.

Source links

Links cited in this article, in order of first appearance. Full addresses are provided for readers using extracted text.

1. https://database.ich.org/sites/default/files/ICH_E6%28R3%29_Annex%202_Guideline_Step%204_2026_0603_0.pdf
2. https://www.ema.europa.eu/en/ich-e6-good-clinical-practice-scientific-guideline
3. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/e6r3-good-clinical-practice-annex-2
4. https://www.ema.europa.eu/en/documents/scientific-guideline/ich-e6r3-guideline-good-clinical-practice-annex-2-step-5_en.pdf
5. https://intuitionlabs.ai/articles/decentralized-clinical-trials-guide
6. https://bmjopen.bmj.com/content/12/8/e063236
7. https://intuitionlabs.ai/articles/patient-retention-clinical-trials
8. https://bmjopen.bmj.com/content/15/11/e106823
9. https://link.springer.com/article/10.1186/s13063-026-09683-7
10. https://intuitionlabs.ai/
11. https://www.tga.gov.au/resources/publication/corporate-reports/ich-guideline-good-clinical-practice
12. https://www.canada.ca/en/health-canada/services/drugs-health-products/drug-products/applications-submissions/guidance-documents/international-council-harmonisation/guidelines.html
13. https://intuitionlabs.ai/articles/clinical-trial-vendor-management
14. https://www.fda.gov/media/152503/download
15. https://www.hhs.gov/ohrp/regulations-and-policy/guidance/use-electronic-informed-consent-questions-and-answers/index.html
16. https://journals.plos.org/plosone/article?id=10.1371%2Fjournal.pone.0295784
17. https://assets.publishing.service.gov.uk/media/5a80948940f0b62305b8bfa7/Electronic_Health_Records_MHRA_Position_Statement.pdf
18. https://commission.europa.eu/law/law-topic/data-protection/information-business-and-organisations/obligations_en
19. https://www.nist.gov/news-events/news/2024/02/nist-releases-version-20-landmark-cybersecurity-framework

20. https://www.ema.europa.eu/bg/media/57985
21. https://www.hhs.gov/ohrp/regulations-and-policy/guidance/institutional-issues/institutional-review-board-written-procedures/index.html
22. https://www.fda.gov/media/166215/download
23. https://www.fda.gov/media/155022/download
24. https://www.fda.gov/media/154449/download
25. https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html
26. https://www.nist.gov/publications/nist-cybersecurity-framework-csf-20
27. https://www.cdisc.org/standards/data-exchange/odm-xml/odm-v2-0
28. https://pmc.ncbi.nlm.nih.gov/articles/PMC9306873/
29. https://www.nejm.org/doi/full/10.1056/NEJMoa2102137
30. https://ascpt.onlinelibrary.wiley.com/doi/10.1002/cpt.70033
31. https://www.frontiersin.org/journals/public-health/articles/10.3389/fpubh.2022.1081150/full
32. https://www.nice.org.uk/corporate/ecd9/chapter/assessing-data-suitability
33. https://www.swissmedic.ch/dam/swissmedic/en/dokumente/zulassung/zl/positionspapier-verwendung-real-wordl-evidence.pdf.download.pdf/Positionspapier%2520RWE_EN.pdf
34. https://jamanetwork.com/journals/jamanetworkopen/fullarticle/2849940
35. https://intuitionlabs.ai/articles/cdisc-sdtm-adam-guide
36. https://www.cdisc.org/standards/foundational/cdash/primer
37. https://www.nature.com/articles/s41746-026-02512-w
38. https://assets.publishing.service.gov.uk/media/5aa2b9ede5274a3e391e37f3/MHRA_GxP_data_integrity_guide_March_edited_Final.pdf
39. https://www.gov.uk/guidance/clinical-trials-for-medicines-guidance-on-quality-and-risk-proportionality
40. https://www.nih.gov/data-counts
41. https://www.who.int/tools/clinical-trials-registry-platform/reporting-on-findings
42. https://www.cisa.gov/cybersecurity-performance-goals

THE PUBLISHER

About IntuitionLabs

IntuitionLabs is an AI consulting, custom software development and data engineering firm serving pharmaceutical, biotechnology, medical-device and other life-science organizations. We work with clinical, regulatory, medical-affairs, commercial, quality and IT teams to connect technology decisions with the work people need to accomplish.

AI consulting and adoption

Our AI enablement services cover readiness assessments, use-case selection, governance and policies, team workshops, adoption measurement and ongoing advisory support. We help organizations structure the information layer behind AI: source material, context, permissions and maintained knowledge that make generated answers useful and reviewable. Private LLM inference and hosted AI options support teams evaluating how to operate AI with appropriate control over their data and infrastructure.

Software, data and life-science workflows

IntuitionLabs develops custom software for pharma and biotech, integrates enterprise systems, and builds data engineering and business intelligence solutions. Areas of focus include AI agents, regulatory research, medical writing, medical affairs, CMC information, competitive intelligence and clinical-document workflows. Our eTMF intelligence work includes cross-system reconciliation and inspection-readiness support.

Enterprise platforms and regulated delivery

We provide Veeva services, application support, managed services, integrations and custom applications, alongside enterprise content work involving platforms such as Egnyte. For regulated workflows, our services include GxP enablement, computer-system validation and software development addressing 21 CFR Part 11 requirements. The applicable controls, validation responsibilities and acceptance criteria are defined for each engagement.

Work with IntuitionLabs

Explore AI enablement, pharma and biotech software development, data engineering and BI, and Veeva services. Contact IntuitionLabs to discuss your workflow, information sources and implementation needs.

IntuitionLabs publishes educational research to help life-science teams make informed technology decisions. Coverage of a product or organization does not imply a client relationship, endorsement or partnership.

Website: https://intuitionlabs.ai