11 May 2026

Technology Task Force Final Report:

ICH Technology Platform Technical Capabilities and Requirements

EXECUTIVE SUMMARY

The ICH Technology Task Force (TTF) has completed its assessment of a potential secure collaboration[1] platform to support ICH harmonisation work and confirms both the value and technical feasibility of this initiative. The TTF recommends establishing a single cloud-based platform hosted in Switzerland to enable secure, temporary sharing of information (that might include commercial confidential information (CCI)) between Regulatory Authorities (RAs) and industry sponsors. This would address critical gaps in ICH's current capabilities that limit confidential collaboration on guideline implementation and development.

TTF recommends the platform operate with comprehensive security protections including encryption, role-based access controls, multi-factor authentication, and full compliance with data protection regulations, while ensuring permanent data custody remains with participating organisations. It is suggested that the ICH Management Committee lead development and oversight of the operational policies and procedures that would govern ICH use of the platform.

ICH regulatory and industry stakeholder input gathered as part of the TTF effort confirmed the platform would deliver significant value through enhanced regulatory consistency and harmonisation, proactive scientific leadership enabling evidence-based guideline development, and improved operational efficiency for global coordination. To move forward, the TTF recommends the MC undertake a legal and IT consultation with participating jurisdictions, establish governance structures, secure financing, develop and issue a Request

[1] Collaboration in this context refers to the secure, temporary sharing and joint development of documents and information among Regulatory Authorities (RAs) and industry sponsors within the ICH platform to support discussions related to development and harmonised implementation of ICH guidelines, which may include alignment of scientific understanding and approach. This collaboration encompasses all cooperative activities including document sharing, secure communications, joint document creation (e.g., information requests, Q&As, case studies), knowledge sharing, and consensus building around guideline interpretation and application.

The ICH Management Committee will determine through its formulation of governance policies the range of ICH harmonisation related activities that would be conducted on the platform and under what conditions.

for Proposal (RFP) with clear Swiss law compliance requirements, and establish an evaluation framework to monitor platform use and value. Please see Recommendations for Next Steps section for further discussion and additional details on how to move forward.

BACKGROUND AND STRATEGIC CONTEXT

ICMRA Leadership and Strategic Vision for Collaboration

In June 2021, at the height of the COVID-19 global pandemic, the International Coalition of Medicines Regulatory Authorities (ICMRA) formally stated that: "The protection of public health is core to the medicines regulatory mission, and this includes meeting patient needs by supporting the continued availability of critically important medicines. ICMRA recognizes that pharmaceutical manufacturers seek agility to maintain robust supply chains and continually update manufacturing processes to incorporate changes and improvements as equipment ages, suppliers change, innovations are developed, and knowledge is gained." The issued statement further made clear that "ICMRA is providing the global leadership and strategic vision to advance this work, which must be progressed through well-coordinated efforts undertaken by existing and highly experienced international regulatory harmonisation, cooperation, and information-sharing bodies including the ICH, PIC/S, and IPRP."

This launched a series of efforts including two ICMRA pilots aimed at enhancing global regulatory collaboration around assessment of post-approval changes, with a focus on post-approval change management protocols (PACMPs) as described in the ICH Q12 guideline, with a goal to make best use of regulators' resources, remove duplication in assessments/inspections, and facilitate faster access of important medicines to patients around the world. Another follow-on effort involved the 2022 development of a Pharmaceutical Quality Knowledge Management (PQKM) Joint Reflection Paper by ICMRA, ICH, IPRP and PIC/S accompanied by a 2023 workplan updated in 2024. In these publications ICMRA, ICH, IPRP and PIC/S identified areas of regulatory harmonisation or convergence-related work that each organisation intended to undertake to support the development of a PQKM capability outlined in the ICMRA PQKM 2022 Joint Reflection Paper. Such work is intended to strengthen international collaboration to support global development, manufacture, and supply, ultimately resulting in timely access to safe, effective, high-quality medicines, and thereby assuring public health.

ICH Leadership to Operationalize a Solution

As work progressed, needs emerged relating to the establishment and operation of a secure technology platform to operationalise the envisioned PQKM capability. To address this need, ICH agreed to establish a PQKM Technology Platform Task Force to begin exploring

what it would take to establish and govern a secure, standardised technology platform to both enable the PQKM vision and make it scalable to other collaborative regulatory use cases. In January 2024, the ICH PQKM Technology Platform Task Force was established with the remit to lead and develop an effective end-to-end strategy, approach, and technological solution to support the PQKM vision; formulate a technology governance model; identify the data and technology capabilities required to support PQKM objectives fully aligned with applicable data and system security requirements, legal and regulatory requirements, and privacy policies across participating jurisdictions; and develop a sustainable financial and procurement model.

In May 2025 the Task Force delivered a White Paper with final recommendations to the ICH Management Committee (MC) including: Adopting a phased approach that aligns investments with process maturity, mitigates risks, and begins with low-complexity solutions that deliver the greatest value to all stakeholders; having Regulators provide the initial capabilities needed to operationalize the collaborative regulatory assessment included in the original PQKM Task Force scope, utilizing existing technology and service management capabilities to accelerate deployment and minimize risks; and, subsequently or in parallel, pursuing a third-party provided secure technology solution and services; and establishing a "Technology Oversight and Governance Committee" to plan and oversee the next phases of implementation to ensure the necessary capacity and capability building to manage third-party services to support PQKM. In response, the ICH MC supported narrowing the scope to focus on a secured documentation sharing platform, instead of a collaborative assessment platform, and ensuring that any future work on establishing a secure platform benefits the harmonisation mission of ICH, with the need to clarify the use cases and the benefits for ICH, making use of learnings from other initiatives, and emphasizing the importance of starting with a limited scope.

The now-renamed ICH Technology Task Force was established with this revised scope and focus on support for development of ICH guidelines and ensuring harmonisation in their application across regions, but recognising that once established, the platform may also in the future be considered for regulatory collaborative assessment, work-sharing, and reliance activities that are conducted and governed outside of ICH.

The Challenge: ICH Mission Readiness in the 21st Century

As ICH enters the second quarter of the 21st century, traditional harmonisation approaches face unprecedented challenges as the pharmaceutical industry increasingly incorporates digital health, artificial intelligence, novel data sources, and advanced manufacturing

technologies into drug development. While ICH has developed guidelines intended to promote innovation by industry, regulators across ICH regions demonstrate inconsistent interpretation of these guidelines, creating regulatory uncertainty that discourages adoption of innovative approaches and delays patient access to new medicines. Regulators need a secure shared platform to support discussion of ICH guideline application in the context of specific industry data and to exchange views toward convergent understandings and approaches that will yield consistency, minimize regulatory uncertainty, and enable industry innovation to proceed and flourish. To ensure mission readiness, ICH requires a secure platform to support efficient and effective harmonisation work that may require confidential data sharing and collaboration amongst regulators, addressing emerging technical harmonisation challenges including harmonised implementation of guidelines and modernizing guideline development processes.

Why a Technology Platform is Essential

The current ICH SharePoint site functions as a basic file repository but lacks the capabilities needed for complex international regulatory information sharing involving confidential information. Email-based coordination is fragmented and ad hoc, with overlapping discussions across time zones that lack standardized threading or status tracking. All project planning and task management must be handled manually without automated workflows, leading to over-reliance on meetings even for simple tasks.

Most critically, the current ICH SharePoint cannot provide the robust security protections required to handle CCI, trade secrets, and regulatory documents that sponsors may authorize for sharing among RAs. It lacks granular permission controls, audit trails, and the encryption necessary for sensitive data. As ICH's work increasingly involves harmonisation of guideline implementation—which requires discussion of specific industry data and regulatory approaches, a secure collaboration platform is now essential to support ICH's mission.

TTF Remit and Methodology

In May 2025, the ICH Management Committee established the TTF to identify capabilities of such a secure document sharing platform to support ICH harmonisation work. The TTF was directed to:

- Develop use cases to identify functional requirements
- Define technical, IT, security, and legal requirements
- Gather stakeholder input on anticipated value

- Develop platform cost estimates
- Deliver a final report sufficient for MC decision on issuing an RFP

The TTF developed four complex use cases for the proposed ICH platform around guideline development (1) and harmonisation implementation (3). Working with technical and legal experts, the TTF then defined the platform characteristics including the technical, functional, IT system security, and the data security and privacy-related legal requirements needed to support these use cases. The TTF also met several times with an MC advisory subgroup to seek guidance and direction, and to raise policy issues the MC would need to address prior to or following platform establishment, recognizing that these policy issues could impact aspects of the platform design and implementation.

USE CASES: ADDRESSING CRITICAL HARMONISATION NEEDS

The TTF selected four use cases representing highly complex instances of guideline development and implementation to ensure the platform could support the full range of current and future ICH harmonisation work. Each use case addresses a specific barrier to harmonisation where secure sharing of confidential data would enable regulatory convergence.

Guideline	Current Challenge	Platform Solution	Data Type
Harmonisation Implementation Use Cases			
Q13 - Continuous Manufacturing	Varying regulatory interpretations of continuous manufacturing requirements delay industry adoption of advanced manufacturing technologies, as companies face different requirements across regions.	Enables sponsors to upload manufacturing technology proposals and lifecycle management approaches; facilitates RA discussion to achieve early convergence on regulatory and scientific principles for evaluating these documents and supporting data.	CMC data with CCI spanning multiple eCTD sections
E19 - Selective Safety Data Collection (SSDC)	Industry hesitancy to use E19 due to varying regulatory acceptance across regions and uncertainty about whether SSDC approaches will be deemed	Sponsors upload clinical study protocols incorporating SSDC; RAs discuss and converge on the approach and application of the guideline for specific protocols, providing clarity on acceptability	Clinical trial protocols with SSDC rationale containing CCI

Guideline	Current Challenge	Platform Solution	Data Type
	acceptable by all relevant authorities		
S1B(R1) - Carcinogenicity Weight of Evidence	The inability to share WoE assessments containing CCI limits the Implementation Working Group's ability to develop best practices and promote consistency in evaluating these assessments across regions	Sponsors and RAs upload WoE data and assessments (for RAs, if permitted by the jurisdiction); RAs share experiences and promote consistency in assessment approaches	Carcinogenicity assessment documents and RA analyses containing CCI
Guideline Development Use Case			
M7 - Nitrosamine Risk Assessment	Need to evaluate concordance of Enhanced Ames Tests (EAT) with in vivo studies to inform guideline recommendations on whether EAT can serve as a stand-alone assay for hazard identification	Sponsors upload EAT and TGR/ECS gene mutation study data; RAs analyse and discuss findings to drive consensus around guideline development recommendations	Gene mutation study data and RA analyses potentially containing CCI

PLATFORM VISION AND ARCHITECTURE

Core Principles

The TTF recommends a secure collaboration platform based on three foundational principles:

1. Each collaboration would operate following an outlined process with documents and data retained on a **temporary[2], not permanent** basis, during the collaboration period and then downloaded to RA systems of record or to a secure platform available to ICH for longer term storage. This approach ensures the platform serves as a temporary collaboration space rather than a permanent repository, with master records remaining in participating organisations' own systems.

2. The platform would promote **trust-building**, providing experience using the platform and building confidence for RA uptake and harmonised implementation of guidelines. As regulators and industry gain familiarity with secure data sharing in this controlled environment, it would facilitate broader adoption of harmonised approaches.

3. The platform would provide a **neutral and secure** environment through Swiss-based hosting, ICH governance, and comprehensive data privacy and cybersecurity protections. This neutral jurisdiction would enable parties to participate with confidence in the protection of confidential information [note: ICH recommends for each jurisdiction to do their own analysis to confirm participation and determine what they can and cannot share into the ICH platform based in Switzerland].

Recommended Architecture

The TTF recommends a **single cloud-based platform** with the following characteristics:

Location: Private commercial cloud in Switzerland, subject to Swiss law. Switzerland provides a neutral jurisdiction with strong data protection laws, enabling ICH parties to participate with confidence.

[2] **Temporary or transient data/records** refer to documents and information that are retained only for the duration of an active collaboration period, protected by multiple layers of security including comprehensive encryption at rest and in transit, and are automatically deleted after the collaboration concludes rather than being permanently retained on the platform.

Data Model, System of Record: Short-term storage only; the platform is not a permanent repository. Legacy systems in each jurisdiction serve as the official system of record, with the ability for authorized users to download data during or after the collaboration period.

Workflow Model

1. Project Initiation: ICH system administrator creates secure collaboration space for the specific project or use case.
2. Data Upload: Sponsors/RAs upload documents and specify access permissions, identifying which authorized parties can view, download, or edit specific content.
3. Collaboration: Authorized parties discuss, analyse, and share documents/data and/or create information-sharing documents within the platform's secure workspace.
4. Completion: Documents/data are downloaded to systems-of-record by participating organisations; platform data is deleted after MC-determined period based on project completion, document owner requirements, and governance policies.
5. Knowledge Sharing (optional): Anonymised case studies developed through collaboration may be retained for long-term storage and use by the broader ICH community.

Types of Data Supported

The platform is specifically designed to handle multiple categories of sensitive information:

Data Category	Examples	Notes
Commercial Confidential Information (CCI)	• Manufacturing technology proposals and process data (Q13) • Clinical trial protocols with proprietary methodologies (E19) • Weight-of-evidence carcinogenicity data (S1B(R1)) • Gene mutation study data (M7) • Regulatory submission documents	Sponsor-controlled access; sponsors explicitly authorize which RAs can view their CCI
Regulatory Documents	• RA documents that are considered relevant to the discussion with other RAs. This could include on-going assessment documents--subject to RA specific jurisdictional requirements. This could include completed RA regulatory reviews (redacted or unredacted). Shared information could also include Scientific advice and analysis documents	Subject to each jurisdiction's legal requirements for sharing; documents may be uploaded by sponsors or RAs

Data Category	Examples	Notes
Information-Sharing Work Products	• Q&A documents created during platform discussions • Collaboration documents around guideline development or implementation • Anonymized case studies for knowledge sharing	Created collaboratively on the platform; may be downloaded to a secure platform available to ICH (if confidential data is included, subject to that platform's data security protections) or to RA systems of record as appropriate.

TECHNICAL CAPABILITIES AND REQUIREMENTS

Functional Requirements

The platform would need to provide the following functional capabilities:

Access & Workspace Management

- Role-based access control (RBAC) with customisable permissions
- Secure information-sharing workspaces for each project
- Sponsor-controlled access to CCI

Document Lifecycle Management

- Secure upload, navigation, and download capabilities
- Version control and document tracking
- Automatic deletion following collaboration completion

Active Collaboration

- Simultaneous editing and review capabilities
- Integrated discussion/chat functionality
- Commenting and annotation tools

Workflow & Monitoring

- Status dashboards for tracking project progress
- Timeline and deadline management
- Notification systems for user activity

Search & Analysis

- Document search capabilities
- Support for multiple file formats (e.g. eCTD, PDF/A[3], XML, CDISC and other structured data efforts such as M11 and M16)
- Application Programming Interface (API)[4] interoperability for future expansion

[3] PDF/A is an ISO-standardized version of the Portable Document Format (PDF) specialized for use in the archiving and long-term preservation of electronic documents.

[4] Application Program Interface. APIs are expected to facilitate the exchange of structured data, incorporating metadata to indicate where the data belongs within the Common Technical Document (CTD) structure (e.g., Module 4.0). This would allow for automated archiving on the health authority. The integration of APIs into regulatory processes is viewed from an "ICH technology platform perspective," especially concerning security, privacy, and jurisdictional controls for confidential information

Security Requirements

The platform would implement multi-layered security governed by NIST Cybersecurity Framework (CSF) 2.0[5] or ISO/IEC 27001: 2002[6]:

Data Protection

- Encryption at rest and in transit (ICH holds exclusive encryption keys)
- Firewalls with Intrusion Detection and Prevention Systems
- Virus scanning of all incoming documents
- Data Loss Prevention practices

Authentication and Authorisation

- Multi-factor authentication (MFA) for all users
- Role-based access control (RBAC)
- Sponsor authorisation for each CCI upload
- Terms & Conditions and Code of Conduct acceptance required

Audit & Compliance

- Comprehensive audit trails tracking all user activity
- Detailed logs of upload dates, times, and document versions
- Complete traceability for regulatory accountability
- GDPR, PIPEDA, and LGPD compliance

[5] For additional information on the NIST Cybersecurity framework, please see a link to this website: https://www.nist.gov/cyberframework
[6] ISO/IEC 27001:2002 is an international standard for information security management systems, providing a risk-based framework to protect data confidentiality, integrity and availability.

Privacy by Design[7]

- Ability to impose strict limitations on personal data collection
- Privacy-by-design principles embedded throughout solution lifecycle

Infrastructure Specifications

- Cloud Service: Private commercial cloud in Switzerland
- Performance: Support for large file sizes, concurrent users across time zones
- Availability: High system availability with disaster recovery capabilities
- Standards Compliance: eCTD 4.0, M11 templates, structured data formats

[7] Privacy by design refers to a set of principles that ensure full regulatory compliance with data protection regulations such as GDPR, PIPEDA, and LGPD. It is incorporated into the design of systems and processes to uphold privacy from the outset.

Key Improvements Over Reliance on SharePoint

The proposed cloud platform would address key identified current limitations. The current SharePoint share drive, as implemented and utilised, provides basic file storage, collaboration (track changes management), and audit log functionality. Document control (sign in/out, review, approvals, version control, etc.,) and other collaborative file management functionality is not used, limiting user-experience and secured collaboration. In addition, email discussion and coordination is free-flowing and ad hoc, with several "conversations" and topics occurring simultaneously, without the use of references/identifiers or subject grouping to easily structure conversations. This is a real challenge when working internationally in different time zones on complicated regulatory multi-stream projects. There is no notification on status of work (e.g. tasks are started up, worked on or completed etc.) This becomes a real challenge when you need to scale-up work (as is the case for international regulatory collaboration) as volume of dossiers/submissions/documents increases. Work planning, progress status, assignment of work is managed manually and there is no automated business process workflows or service level performance reporting. This requires a lot of coordination and virtual meetings even for the simplest tasks. There is also no secure authentication (i.e. 2FA) and a multi-layered security setup with encryption for different submissions that may be required by sponsors, and the currently available traceability and metadata information included in the existing Purview account might not be sufficient in case of audit or judicial review. These challenges observed in the context of well-established domestic submissions management systems are even more glaring in the international settings. Thus, the proposed platform would need to address and provide the following identified required capabilities:

Proposed Cloud Platform
Advanced collaboration workspace with simultaneous editing and version management
Multi-layered security with encryption, firewalls, intrusion detection

Role-based access control with multi-factor authentication
Integrated workflow management with automated processes
Comprehensive audit capabilities with detailed activity logs
Automated workflows and service-level performance reporting
Full GDPR, PIPEDA, LGPD compliance
Strict access controls with adequate requirements on confidentiality

LEGAL CONSIDERATIONS

The legal considerations were assessed across all contemplated use cases, with confidential commercial information (CCI), trade secrets, and regulatory confidentiality protections being the clearest requirements. Most legal issues will best be addressed through a combination of governance requirements and with robust technical controls such as data tagging, encryption, access controls, audit trails, and breach detection capabilities. Additional legal considerations include public disclosure/FOI obligations, regulatory record integrity, personal data privacy, liability and indemnification, procurement requirements, competition law, and export controls/sanctions (the last included for the sake of completeness but not likely to be relevant here)—each with jurisdiction-specific implications that must be analysed.

The TTF recommends that the MC undertake jurisdictional analyses of legal requirements for the ICH association and participating Regulatory Authorities, using the representative data flow maps provided in Appendices 1 and 3 to classify triggering data and identify necessary controls to be implemented and related requirements for the 3rd party platform service provider. The methodology used for the initial analysis provided in this TTF report was limited to stakeholder interviews and AI-assisted legal review and has not been supplemented with jurisdiction- or stakeholder-specific legal review.

To inform the work related to platform services procurement, ICH should anticipate utilizing its own counsel to review the legal considerations applicable to ICH as an organisation, including vendor due diligence, contract negotiation, and provisions addressing the identified legal requirements and subcontractor arrangements. Call for Tender responses can be used to augment that analysis as well as validate what controls are readily available. Member jurisdictions will in tandem need to engage their respective counsel to analyse jurisdiction-specific legal requirements relevant to ensure their participation.

GOVERNANCE CONSIDERATIONS

ICH Management Committee would formulate policies and provide oversight of platform operations and any future plans, as needed, as the ICH gains more experience using the platform.

ICH would serve as the data controller[8] for the platform, with responsibility for ensuring data protection compliance and system security. It is anticipated that ICH would delegate these responsibilities through the contract provisions to a contracted 3rd party vendor.

Sponsors and regulatory authorities would retain ownership of their respective data[9] uploaded to the platform. ICH's role as data controller pertains to platform security and compliance, not ownership of the underlying regulatory or commercial information.

The TTF recommends that the ICH would be primarily responsible for the metadata[10] generated during platform use and other data control policies surrounding metadata such as what metadata would be captured, where it would be stored and for how long, and who can access/download the metadata.

[8] Data controller is the legal term for the entity that controls the data within the platform and is responsible for its security, processing, and compliance with data protection regulations.
[9] Data Owner refers to the entity that holds the intellectual property rights and proprietary interests in the data or documents uploaded to the platform.
[10] Metadata is platform-generated data that is created and captured during the use of the platform, which is distinct from the actual content (documents/data) uploaded by sponsors or regulatory authorities. Examples include project management data, communication logs, user activity tracking, upload dates and time, document versions, audit trail information and system use records.

- The TTF also recommends that the management committee address the following governance topics related to data on the platform: What can be downloaded, when and by whom
    - The MC needs to decide which work products can be downloaded, timing of downloads, and whether both RAs and Sponsors can download.
- Retention period
    - The MC needs to decide how long documents should remain on the platform after collaboration ends.

ANTICIPATED VALUE

Regulatory Consistency & Harmonisation

The primary focus of the proposed technology platform is to support ICH work to advance harmonisation of scientific and technical standards including ensuring harmonisation in ICH guideline application by regulators in the implementation of guidelines across regions. The platform would enable real-time sharing of regulatory perspectives and approaches, fostering harmonised understanding and application of ICH guidelines across regions. Currently, inconsistent interpretation and implementation of guidelines such as Q13 (continuous manufacturing), E19 (selective safety data collection), and S1B(R1) (carcinogenicity weight of evidence) create regulatory uncertainty and slow the uptake of new technologies.

These specific use cases identified for TTF examination provided examples of non-public data that may be uploaded on the platform include information in the context of existing ICH guidelines where ICH Regulatory Members have different approaches (i.e. non-aligned interpretation) or where Regulatory Members have different experience in getting applications from industry. The non-public data involved in these use cases include: data to support a weight of evidence-based request for a waiver of the requirement for 2-year rat study (with the consent of the owner of the data) [S1B guideline], a study protocol involving selective safety data collection in a late-stage clinical trial [E19 guideline], and data related to utilisation of advanced manufacturing techniques [Q13 guideline].

Once established, the MC determined that the platform may also enable regulatory collaborative assessment, work-sharing, and reliance activities that are conducted and governed outside of ICH[11].

The secondary use case providing a prime example of this involves secure sharing of industry regulatory submissions, with the focus on Chemistry Manufacturing Control (CMC)/Post Approval Change (PAC) submissions, specifically those involving life cycle management applying the ICH Q12 Post Approval Change Management Protocols (PACMPs) and related questions or information generated by regulators as part of their assessment of these submissions. This secondary use case involves a compelling ICH guideline implementation issue that also makes a direct contribution to the stated ICH objective of "international regulatory convergence facilitating the aligned assessment of medicines worldwide" to ensure the availability of medicines to patients who need them.

By facilitating secure discussion of how guidelines apply to specific sponsor data and regulatory scenarios, the platform would help reduce conflicting regional interpretations that create burden and hinder the adoption of beneficial innovations.

Proactive Scientific Leadership

The platform would provide a secure forum for RAs to collaboratively analyse trends and sponsor data, enabling timely, science-based guideline development. Through structured collaboration and consensus-building, as demonstrated in the M7 nitrosamine use case[12], RAs could conduct the "pre-work" necessary to develop guidelines that keep pace with scientific advances and address real-world regulatory challenges.

Operational Efficiency

The platform would streamline global regulatory coordination through integrated workspaces with structured discussions, role-based access, and centralized task management. Currently, ad-hoc email communications create coordination delays and make cross-time-zone collaboration particularly challenging. The platform would reduce reliance on meetings for routine tasks, provide visibility into project status and progress, and enable knowledge-sharing that supports all RAs—particularly smaller authorities that face resource

[11] Minutes of the ICH MC meeting in Singapore

[12] For additional information on the M7 nitrosamine use case, please see the section above titled, "Use Cases: Addressing Critical Harmonisation Needs." The table in that section should provide additional details.

constraints in keeping pace with scientific advances. These efficiencies would benefit both regulators and industry by reducing coordination burden and accelerating harmonisation work.

RECOMMENDATIONS FOR NEXT STEPS

In summary, the TTF recommends the following next steps to advance platform development. Step 1 is foundational; Steps 2-4 should proceed in parallel to build the foundation for implementation, while steps 5-8 are sequential:

1. **Swiss Law Analysis for Jurisdictional Review:** As a foundational step, ICH will obtain a comprehensive legal analysis of Swiss data protection and privacy requirements applicable to the proposed cloud platform. This analysis will be distributed to legal counsel in each participating jurisdiction to enable them to assess compatibility with their domestic legal frameworks and identify any jurisdictional constraints that may impact their use of the platform, particularly regarding the temporary storage of CCI and regulatory documents in Switzerland.

Parallel Activities (Steps 2-4):

2. Legal and IT Consultation: Undertake structured legal and IT consultation with relevant authorities in each participating jurisdiction to ensure there are no additional local legal or security considerations that would impact their desired use of the platform (see legal considerations section for additional context of what the consult should include). Additionally, consult with the ICH Industry Members to understand and address any potential member company/ sponsor hesitancy to use the platform and ensure the design meets industry needs.

3. Workflow Validation: Validate the TTF's proposed workflow processes and procedures with a broader group of stakeholder representatives (both RA and industry) to confirm operational feasibility, identify any gaps or additional requirements, and ensure the workflows support the intended collaboration activities effectively.

4. Governance Establishment: Establish a clear governance mechanism to provide strategic oversight and coordination for platform development, implementation, evaluation, and ongoing operations. This mechanism would ensure ICH has the capacity to manage

third-party services, develop policies, and make governance decisions about platform use and evolution as well as to raise awareness of the platform and its capabilities among RAs and across industry.

Sequential Activities (Steps 5-8):

5. **Financing:** Secure funding for platform implementation and ongoing operations, including initial setup costs, subscription or licensing fees, and resources for ICH oversight and administration.

6. **RFP Development and Procurement:** Write and publish an RFP with detailed functional and technical specifications, clear Swiss law compliance requirements, security standards (NIST Cybersecurity Framework or ISO/IEC 27001:27002), and evaluation criteria. The RFP should be unambiguous about data hosting location requirements and service provider obligations, and include detailed security and compliance requirements, enabling vendor responses to validate which controls are available in commercial solutions and inform build-versus-buy decisions.

7. **Vendor Evaluation and Selection:** Evaluate vendor proposals against the established requirements and criteria, conduct due diligence on finalist vendors' capabilities and compliance, and select the platform provider that best meets ICH's needs for security, functionality, and cost-effectiveness.

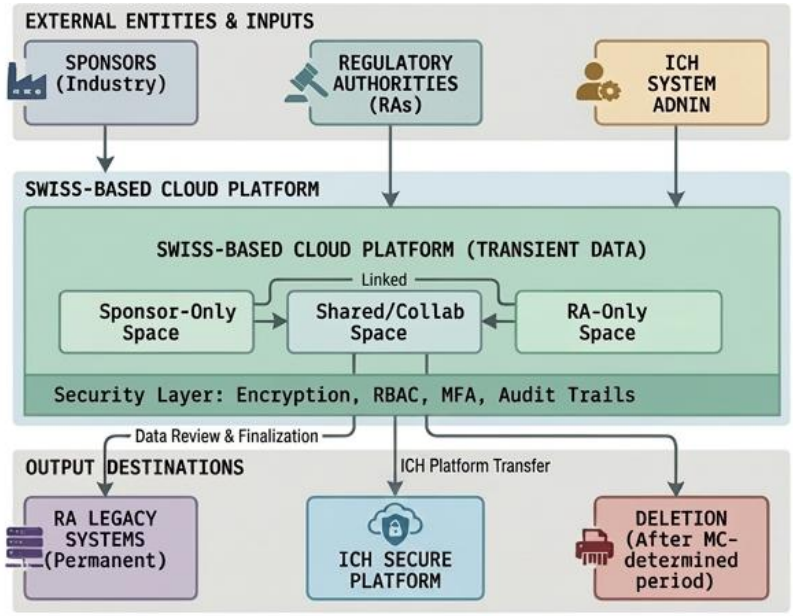
8. **Evaluation Framework Development:** Develop metrics and a monitoring framework before platform launch to assess value delivery, track usage patterns, gather user feedback, and define the future evolution of the platform. This framework should include key performance indicators related to harmonisation outcomes, user satisfaction, operational efficiency, and potential expansion to support additional use cases or guideline development activities.

CONCLUSION

The TTF assessment confirms that a secure collaboration platform is both valuable and technically feasible for supporting confidential collaboration between RAs and industry. This platform will future-proof ICH operations, ensure consistent application of guidelines

across regions, and enable ICH to fulfil its mission in an increasingly complex regulatory environment. The recommended single cloud-based approach in Switzerland provides the optimal balance of security, neutrality, and functionality to support ICH harmonisation work while building trust and confidence among regulatory and industry stakeholders.

Appendix 1: Data Flow Diagram (DFD): The following data flow diagram (left) and detailed data flows with labels (right) illustrates the movement of information between external entities (sponsors, regulatory authorities, and ICH system administrators), the Swiss-based cloud platform, and more permanent storage systems, mapping the primary data flows that support the platform's transient collaboration model



DETAILED DATA FLOWS WITH LABELS

1. SPONSOR → PLATFORM
   - ├─ CCI Documents (Q13: Manufacturing technology proposals)
   - ├─ Clinical Trial Protocols (E19: SSDC rationale)
   - ├─ Carcinogenicity Data (S1B(R1): WoE documents)
   - ├─ Gene Mutation Studies (M7: EAT/TGR/ECS data)
   - ├─ Completed RA Reviews previously received by the Sponsor
   - └─ Collaborative Documents (created on the Platform)

2. RA → PLATFORM
   - ├─ Assessment Documents (RA jurisdiction dependent)
   - ├─ Analysis of Sponsor Data (RA jurisdiction dependent)
   - ├─ Guidances (non-confidential)
   - └─ Collaborative Documents (created on the Platform)

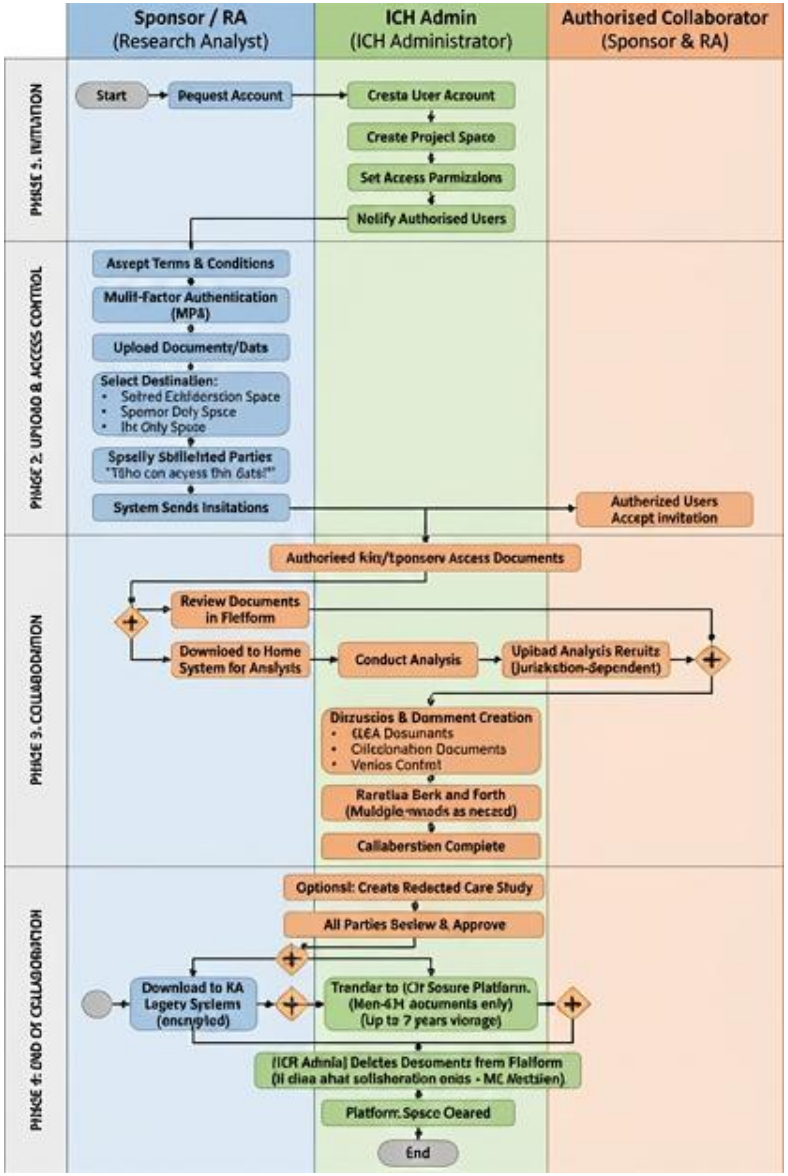
3. PLATFORM → RA LEGACY SYSTEMS
   - ├─ Encrypted Downloads (authorized documents)
   - ├─ CCI (with sponsor authorization)
   - ├─ Collaboration Documents
   - └─ Analysis Results

4. PLATFORM → SECURE PLATFORM AVAILABLE TO ICH
   - ├─ Redacted Case Studies (anonymized)
   - ├─ Non-confidential Collaboration Documents
   - └─ Guidances

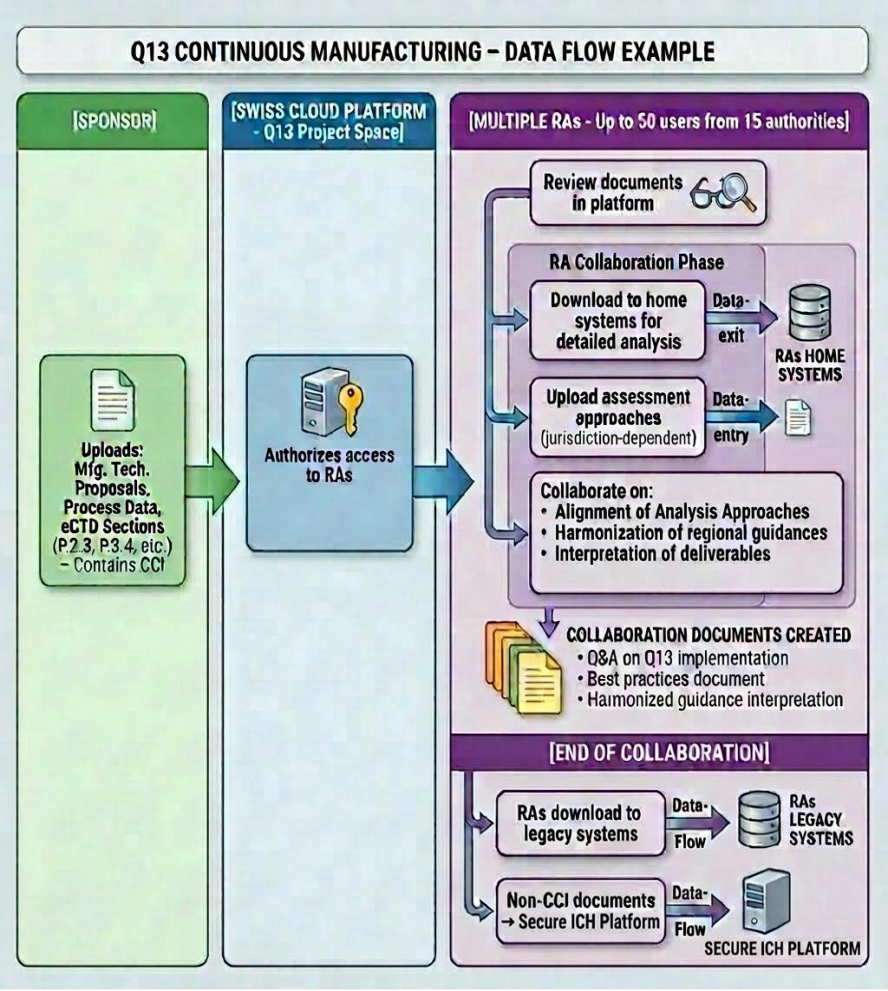
5. ICH ADMIN → PLATFORM
   - ├─ Account Creation
   - ├─ Project Space Setup
   - ├─ Access Control Management
   - └─ Document Deletion (post-collaboration)

6. PLATFORM → DELETION
   - └─ All transient documents (X time after collaboration ends)

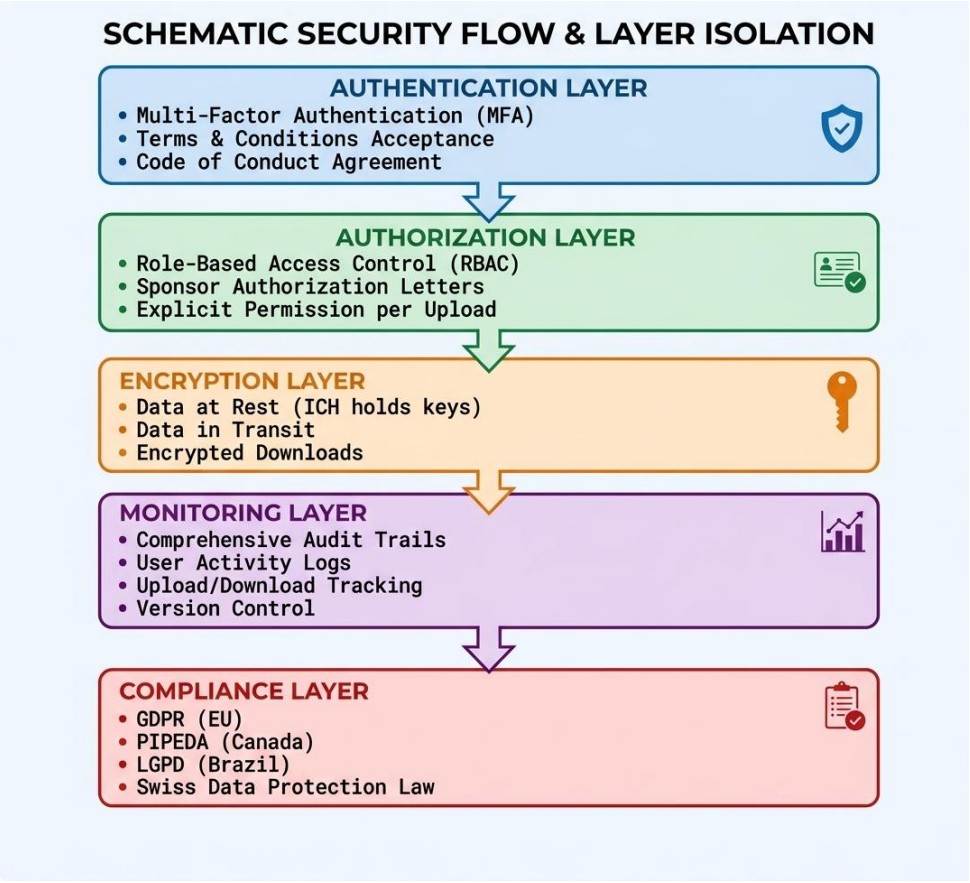
Appendix 2: Workflow Diagram: The following workflow diagram illustrates the end-to-end process for platform collaboration across four distinct phases: initiation (account creation and project setup), upload and access control (document sharing with explicit authorisation), collaboration (review, analysis, and document creation), and end of collaboration (downloads, case study creation, and systematic deletion). This visual representation demonstrates how sponsors and regulatory authorities interact with the platform from initial access through final data disposition, highlighting key decision points, security controls, and the transient nature of platform storage.



Appendix 2A: Use Case-Specific Data Flow Example (Q13): The following diagram provides a detailed example of how data flows through the platform for the Q13 continuous manufacturing harmonisation use case, illustrating the specific types of documents uploaded by sponsors, the multi-authority collaboration process involving up to 50 users from 15 regulatory authorities, and the creation of harmonised guidance documents. This example demonstrates how the platform's generic data flow architecture supports complex, real-world regulatory harmonisation scenarios involving highly sensitive CCI.



Appendix 2B: Security & Access Control Layer: The following diagram illustrates the five-layered security architecture that protects all data on the platform, from initial user authentication through encryption, authorisation, monitoring, and compliance controls that ensure CCI and regulatory documents remain secure throughout the collaboration lifecycle.



Appendix 3: ICH Platform—Data Element Inventory

The ICH Technology Platform will process, store, and transfer multiple types of highly sensitive data including CCI, trade secrets, regulatory assessment documents, and platform operational metadata. To ensure comprehensive data governance, privacy compliance, and security planning, the TTF undertook a data element analysis, whereby each data element is analysed against twenty-two standardized criteria including classification, legal basis, retention policy, encryption requirements, access controls, and risk rating to support informed decision-making and robust platform implementation. Below is a representative example of a sponsor-uploaded data element for the Q13 use case. If the Management committee finds this analysis useful, the TTF could continue this analysis across other data elements including sponsor-uploaded data, regulatory authority-uploaded data, and platform-generated metadata.

Manufacturing Technology Proposals (Q13)

Field	Value
Data Element (field name)	Manufacturing*Process*Data_Q13
Example Value Type	Document (PDF), structured data (XML/eCTD)
Classification	Commercial Confidential Information (CCI) / Trade Secret
Source System	Sponsor proprietary systems
Purpose(s) of Processing	ICH Q13 guideline harmonisation; RA collaboration on continuous manufacturing assessment approaches
Legal Basis	Consent (explicit sponsor authorisation); Legitimate interest (regulatory harmonisation)
Consent Details	Sponsor Authorisation Letter per upload; timestamp recorded in audit log; scope limited to identified RAs
Retention Policy / Retention End Date	Transient only; deleted X days after collaboration ends (MC to determine); Master record remains with sponsor
Storage Location	Swiss-based private commercial cloud (Switzerland jurisdiction)
Encryption at Rest	Y - ICH holds exclusive encryption keys; method per ISO/IEC 27001
Encryption in Transit	Y - TLS/SSL encryption for all uploads/downloads
Pseudonymisation/Anonymisation	N - Original CCI maintained; Optional anonymisation for case studies only
Access Control	Role Based Access Controls (RBAC) - Sponsor-specified RAs only; Multi-Factor Authentication (MFA) required; explicit invitation acceptance
Logging / Audit Enabled	Y - Comprehensive audit trails: upload date/time, access logs, download tracking, version control
Third Parties / Onward Transfers	Authorized RAs only (per sponsor consent); No third-party vendors access CCI
Transfer Mechanism	Swiss law compliance; Sharing subject to policies

	laid out by MC governance body
Data Privacy Impact Assessment Required	Y - Risk due to CCI/trade secrets
Legal Hold	N - Not applicable for transient collaboration platform
Data Subject Rights Impact	N/A - No personal data; Corporate data subject to IP protection
Risk Rating	Trade secrets and CCI require protection
Notes / Mitigations	Multi-layered security (encryption, RBAC, MFA, audit trails); Sponsor controls access; Data flagged as CCI in platform; Firewalls, intrusion detection, virus scanning
Owner / Responsible Team	ICH MC (data controller); Sponsor (data owner/IP holder)