



GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

COMMENTS ON DRAFT GLOBAL STRATEGY ON DIGITAL HEALTH 2028-2033

CONSULTATION FROM THE WORLD HEALTH ORGANIZATION

September 2026

The Global Data Alliance (GDA)¹ is pleased to respond to the 2026 consultation from the World Health Organization (WHO) relating to the WHO's Draft Global Strategy on Digital Health (2028-2033).

The GDA is a cross-industry coalition of companies that are committed to high standards of data responsibility and that rely on the ability to transfer data around the world to deliver healthcare services, biopharmaceutical treatments, medical technologies, and insurance / financial support to institutions, practitioners, and patients globally. GDA supports policies that build trust in the digital health systems, safeguard the responsible and secure movement of information across borders, and avoid unnecessary data localization requirements that limit access to knowledge, technologies, and services. GDA members also support trusted digital health ecosystems that enable prevention, self-care, health literacy and access to evidence-based health information. GDA member companies are active in all health-related sectors and depend on cross-border access to information and data transfers to deliver better health outcomes around the world.

We welcome the draft Strategy's recognition that international cooperation, interoperability, and secure data exchange are central to continuity of care, public health intelligence, emergency preparedness, research, and responsible innovation. Direction 2.1 appropriately calls for participation in regional and global data exchange initiatives and for WHO trust infrastructures that support rights-respecting cross-border exchange. Direction 2.3 also calls for a technical and legal blueprint that reconciles data sovereignty with participation in global health data exchange. Similarly, Direction 3.1, which addresses digital and data literacy across the health workforce and the wider population, could helpfully recognize consumer-facing digital health channels as part of the health information environment.

These are important commitments: We encourage the WHO to make them more consistent and operational across the Strategy. Cross-border data transfers and cross-border access to knowledge and health technologies are a catalyst for the ability of health systems to promote multi-region and multi-country clinical trials and research, develop specialized medical expertise, deploy secure services in the cloud, evaluate health treatments and technologies across diverse populations, and respond to safety events.

GDA therefore recommends the following revisions.

- **Make trusted cross-border data exchange an express guiding principle**

Guiding Principle 4 supports the secure flow of information across institutions, systems, and sectors, but is silent on the movement of data across transnational digital networks. The Strategy should state at the level of principle that health data and other health-related information must be able to move responsibly across borders. Doing so would connect the Strategy's vision and equity goals to the more specific commitments in Directions 2.1 and 2.3.

Recommended addition to Guiding Principle 4:

"Digital health ecosystems should enable the responsible and secure movement of health data and other information across borders, supported by interoperable legal and technical data transfer frameworks. Member States should not impose unnecessary or discriminatory data localization and transfer restrictions, which often undermine institutional, provider, and patient access to health-related information, treatments, and technologies."

This principle should cover both personal and non-personal data, with safeguards calibrated to the data and use at issue. Facilitation of cross-border data transfers improves access to quality care, patient outcomes and delivery of innovative healthcare solutions to serve unmet patient needs and enable health systems to be more efficient. For example, a domestic telehealth visit may still depend on an overseas-hosted platform that supplies encryption, authentication, analytics, storage, or other functionality. Cross-border access can therefore improve privacy, cybersecurity, reliability, and clinical functionality even when the clinician and patient are in the same country.

An express principle would also advance equity. Cross-border connectivity gives health systems, including those in remote or resource-constrained settings, access to specialized services and globally scalable technologies that may not be available locally. Such a principle could also recognize that regulations must be future proof to account for data transfer requirements for development of novel and innovative therapies/technologies. The Strategy should present trusted data movement and strong protection as mutually reinforcing objectives.²

- **Clarify that data sovereignty does not require data localization**

Direction 2.3 is right to seek a practical reconciliation of data sovereignty, individual rights, and global exchange. Because the term "data sovereignty" is used in materially different ways, however, the Strategy should define it carefully. It should not be understood as a presumption that health data must be stored or processed only within the territory where it originated.

Recommended clarification for Direction 2.3:

"For purposes of this Strategy, data sovereignty concerns the ability of Member States and individuals to establish and enforce lawful governance, rights, and accountability for health data and digital systems, even when data is transferred across borders. Data localization is neither necessary nor sufficient to secure data sovereignty: data held domestically may still be poorly governed, and data held abroad may be subject to strong and enforceable safeguards. Data sovereignty therefore does not require domestic storage or processing of data, or nationality- or origin-based ownership restrictions. Such restrictions can undermine optimal health outcomes for patients, as well as the ability to deliver health-related information, treatments, and technologies to institutions, providers and patients around the world. This is distinct from, and does not diminish, the governance rights of Indigenous Peoples and local communities over data concerning them."

Privacy and security turn primarily on how data is governed and protected, not on the physical location of a server.³ Appropriate safeguards may include encryption, access controls, data minimization, pseudonymization or anonymization where suitable, contractual controls, privacy-enhancing technologies, and enforceable accountability. Cross-border cloud services can also strengthen cybersecurity by supporting real-time threat detection, distributed resilience, timely patching, and coordinated incident response. GDA supports the draft's call for cross-border cyber threat information sharing and recommends applying the same practical approach to broader health data governance.

Likewise, GDA encourages the development of cross-border data sharing agreements between countries, which can support greater alignment on data security and privacy protection measures (applying best

practices for the collection, processing, storage, analysis, use, sharing and disposal of health data) and interoperability (harmonized standards between different regulatory systems). In this way, interoperable health data-sharing frameworks and common protocols can support responsible and ethical cross-border sharing for both general health and genomic specific data.

WHO's proposed technical and legal blueprint should help Member States establish clear and usable transfer pathways. Without prescribing one legal model, the blueprint can address interoperable mechanisms such as certifications, codes of conduct, contractual safeguards, recognized privacy frameworks such as the Global Cross-Border Privacy Rules system and ISO/IEC 27701, and other accountable transfer tools.

It should also recommend that restrictions be transparent, non-discriminatory, necessary, and proportionate to a legitimate public-interest objective. Full anonymization should not be treated as a universal prerequisite, because continuity of care, clinical research, safety monitoring, and regulatory review may require identifiable or linkable data under appropriate controls.

- **Tie cross-border exchange to concrete health outcomes**

The Strategy will be more useful to Member States if it connects cross-border exchange to specific health system functions. GDA recommends expanding the actions in Directions 2.1, 2.3, and 4.1 to address at least the following use cases:

1. **Continuity of care, telehealth, and humanitarian services.** Cross-border exchange supports remote consultations, second opinions, access to overseas laboratories and specialists, and humanitarian telemedicine networks serving underserved populations. It also supports domestic care delivered through globally operated cloud technologies.
2. **Public health intelligence and emergency response.** The cross-border consolidation and analysis of appropriately protected datasets can improve real-time tracking of health trends, epidemiological patterns, and localized disease outbreaks. This capability should be treated as part of emergency readiness, not only as an ad hoc response after a crisis begins.
3. **Research, clinical trials, and regulatory oversight.** Multi-country data supports drug discovery, representative clinical trials, research on rare and neglected diseases, collaborative regulatory review, adverse-event reporting, and post-market surveillance. It is critically important that regulated entities be able to aggregate data for proper analysis during the development of a therapy, and include all relevant data in regulatory filings with health authorities around the world. Diverse cross-border data can improve the quality and generalizability of safety and efficacy findings across populations.
4. **Medical technologies, AI, and real-world evidence.** Connected medical technologies often rely on the real-time measurement, transmission, and analysis of data. Access to data from multiple countries can strengthen post-deployment monitoring and help ensure that AI-enabled tools are trained and validated on sufficiently large and representative populations, reducing avoidable bias and performance gaps.⁴ In other words, access to diverse, representative, and responsibly shared datasets is essential for the development, validation, monitoring, and continuous improvement of healthcare AI.
5. **Self-care, prevention, and access to evidence-based health information.** Cross-border exchange supports the development, evaluation, and dissemination of evidence-based digital health resources, including tools that promote health literacy, prevention, and responsible self-care. Access to data from multiple jurisdictions can help improve the quality and reach of consumer-facing digital health interventions while supporting trust, informed decision-making, and more resilient health systems.

To reflect these functions, the Member State action in Direction 2.1 concerning regional and global initiatives should expressly include telehealth, research, regulatory cooperation, safety monitoring, and responsible

innovation. The WHO action in Direction 2.3 concerning federated governance, pseudonymization, and anonymization should expressly refer to secure cross-border transfer and should recognize a broader, risk-based range of safeguards. Direction 4.1 should call for the responsible cross-border generation and sharing of real-world evidence and for access to lawfully usable data from diverse jurisdictions when evaluating representativeness, safety, bias, and performance. Broadly speaking, the WHO should encourage frameworks that facilitate secure international collaboration and responsible cross-border use of data for evidence generation, real-world evidence (RWE) and real-world data in supporting regulatory decision-making, post-market surveillance, health technology assessment, and continuous product improvement.

- **Translate the commitments into guidance, capacity building, and metrics**

The Strategy's implementation framework should make cross-border readiness measurable. The two indicators proposed in the draft, drawn from GPW14 Output 3.3.1, count the number of countries with a digital health strategy or roadmap and the number of countries that have improved their health information system capacity scores under the SCORE for Health Data technical package. Neither measures whether a country is able to exchange health data across borders. WHO's supplemental monitoring framework should also assess whether Member States can participate safely and effectively in regional and global health data exchange.

Relevant maturity indicators could assess whether a country:

- Permits and/or maintains interoperable legal mechanisms for cross-border transfers of health-related data;
- Participates in regional or global exchange networks, trust frameworks, or regulatory collaborations;
- Implements and tests conformance with internationally recognized interoperability, privacy, and security standards;
- Can exchange relevant data rapidly and securely during public health and cybersecurity emergencies; and
- Has identified and addressed localization or transfer restrictions that unnecessarily obstruct care, research, regulatory oversight, or access to digital health services.

These indicators should evaluate capability, safeguards, and health outcomes rather than the volume of personal data transferred. WHO should develop them with Member States, standards bodies, providers, researchers, patients, civil society, and the private sector, and should incorporate at least one cross-border readiness measure into the supplemental monitoring framework in time for the 2030 mid-term review.

Direction 3.2 already calls on Member States to establish inclusive multistakeholder collaboration platforms and to participate in regional and global cooperation platforms. Building on that commitment, the Strategy should encourage Member States to establish multistakeholder processes that engage responsible private-sector actors, alongside patient groups, civil society, providers, standards bodies, and technical experts, in the design, implementation, and evaluation of digital health ecosystems.⁵ Technical assistance should help lower-resource health systems adopt interoperable governance and security tools without recreating infrastructure that is safely available through cross-border services.

Cross-border data and digital connectivity support Sustainable Development Goal 3 by improving diagnosis and treatment, pandemic response, humanitarian assistance, and medical research. They also advance equity, resilience, and sustainable development. WHO can help countries pair high, enforceable protections with practical access to data and technology across borders.

Conclusion

GDA encourages WHO to preserve the draft's strong references to cross-border continuity of care, international interoperability, and global health data exchange, while making those commitments more explicit throughout the Strategy. A clear principle favoring responsible and secure cross-border data movement, a

distinction between sovereignty and localization, concrete health use cases, and workable metrics would give Member States a stronger roadmap for trusted digital health.

GDA appreciates WHO's consideration of these comments and welcomes the opportunity to support further work on interoperable, rights-respecting, and globally connected digital health ecosystems.

¹ The GDA is a cross-industry coalition of companies that are committed to high standards of data responsibility and that rely on the ability to access and transfer information across borders to innovate and create jobs. GDA member companies are active in the accounting, agriculture, automotive, aerospace and aviation, biopharmaceutical, consumer goods, energy, film and television, finance, healthcare, hospitality, insurance, manufacturing, medical device, natural resources, publishing, semiconductor, software, supply chain, telecommunications, and transportation sectors. For more information, see <https://www.globaldataalliance.org>

² By contrast, localization mandates can fragment services, raise infrastructure and compliance costs, and reduce access to best-in-class tools. Modeling by the European Centre for International Political Economy estimated that economy-wide data localization requirements would reduce GDP by 1.1 percent in the European Union and the Republic of Korea and by 0.8 percent in Brazil and India, with EU domestic investment falling by 3.9 percent. ECIPE, *The Costs of Data Localisation: Friendly Fire on Economic Recovery* (2014), <https://ecipe.org/publications/dataloc/>.

³ This governance-based approach is reflected in the OECD Recommendation of the Council on Health Data Governance, OECD/LEGAL/0433 (adopted 13 December 2016), which frames the protection of personal health data around governance, safeguards, and accountability rather than storage location. See <https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0433>.

⁴ Narrow geographic sourcing of training data is well documented. A review of US deep-learning diagnostic studies published between 2015 and 2019 found that 71 percent of the studies for which cohort geography could be determined drew on patient data from California, Massachusetts, or New York alone, with most other states unrepresented. Amit Kaushal, Russ Altman & Curt Langlotz, *Geographic Distribution of US Cohorts Used to Train Deep Learning Algorithms*, 324 JAMA 1212 (2020), doi:10.1001/jama.2020.12067, <https://jamanetwork.com/journals/jama/article-abstract/2770833>.

⁵ Relatedly, under Direction 3.1, the Strategy could draw a stronger link between digital literacy and trust, safe adoption and the effective use of digital health tools. If regulators, individuals and health stakeholders lack the skills to understand data use, privacy protections, and online safety, economies may face challenges in building trust in the digital health ecosystem. The WHO could helpfully encourage member states to invest in practical literacy programs for these stakeholders as part of digital health readiness.