GLOBAL DATA ALLIANCE
TRUST ACROSS BORDERS

November 11, 2026

GLOBAL DATA ALLIANCE COMMENTS ON ABU DHABI DEPARTMENT OF HEALTH CIRCULAR NO. 191/2026

The Global Data Alliance (GDA) thanks the Department of Health – Abu Dhabi (DoH) for the opportunity to comment on Circular No. 191/2026, concerning multi-cloud strategies and on-site physical backups.[1]

Background

The GDA is a cross-industry coalition of companies that are headquartered across multiple regions and that are committed to high standards of data privacy, security, and responsible data use. Its members rely on trusted cross-border data flows to innovate and compete. In healthcare, such flows enable clinical care, claims administration, medical device monitoring, cybersecurity, clinical trials, pharmacovigilance, and medical research.[2] Secure cloud environments play an important role in healthcare, supporting these uses and other data-enabled health services.

Discussion

The Circular provides: "All healthcare providers, payers, and service providers shall plan, implement, and sustain multi-cloud and on-premise strategies, including on-site physical backup(s)."

The Circular's reach is very broad. It appears to cover medical device manufacturers whose connected devices, robotic platforms, medical software, or remote monitoring services process Abu Dhabi patient data. It also appears to affect biopharmaceutical companies and their research, clinical trial, pharmacovigilance, and patient support service providers that manage health information through global platforms. Hospitals, laboratories, clinics, insurers, third-party administrators, and claims processors are also impacted. The Circular may also affect a wide array of cloud service providers, including both IaaS and SaaS providers.

GDA supports the goal of keeping critical healthcare data and services available, confidential, accurate, and recoverable during cyber incidents and other disruptions. Multi-cloud architectures can be helpful in some cases. However, they should remain optional, rather than a broad mandate for every single regulated entity to procure and design services to operate across multiple cloud architectures and to store data onsite within Abu Dhabi.

Prescribing multiple clouds and on-site physical storage for every covered organization can increase complexity and cybersecurity exposure without improving resilience. Fragmented local backups create additional sites to secure, patch, monitor, and test, while increasing the attack surface and exposure to cybersecurity risks. Synchronizing systems across on-site and cloud environments can introduce data configuration errors, as well as new data protection and integrity risks. Conversely, secure geographically separated backups, immutable or offline copies, tested restoration procedures, and appropriate recovery objectives can provide strong resilience without mandatory on-site infrastructure.

These concerns are particularly acute in regulated biopharmaceutical, medical device, healthcare provision, and insurance sectors. For example, in the context of medical devices, hosting architecture for connected devices and software as a medical device (SAMD) can form part of a validated design and the manufacturer's lifecycle cyber controls.[3] Migration to a second cloud or on-premise hardware may require renewed validation, risk assessment, or regulatory submissions, potentially across multiple jurisdictions. These processes cannot feasibly be completed by the Circular's January 1, 2027 effective date and are likely to disrupt functionality and patient access.

Instead of the approach outlined in the Circular, GDA urges DoH to consider building on its existing Policy on Risk Management and Business Continuity for the Health Sector, which calls for risk-based continuity planning and identification of critical functions.[4] Resilience requirements should ultimately be measured by their ability to protect patient safety and maintain continuity of care. A risk- and outcomes-based framework would require healthcare organizations to demonstrate robust availability, recovery, and disaster-recovery capabilities, while allowing flexibility in the technical architecture used to achieve those outcomes. Demonstrated resilience – rather than a prescribed number of cloud providers or backup locations – would better support patient safety, cybersecurity, and continued investment in Abu Dhabi healthcare, while preserving the healthcare sector's ability to adopt secure, innovative technologies.

Recommendations

GDA respectfully recommends that DoH preserve its resilience objective while adopting a risk-based, outcome-oriented, technology-neutral implementation. Specifically, DoH should:

(a) remove the "on-premise" data residency mandates, the local physical infrastructure mandate, and the mandate to host data across multiple cloud architectures;

(b) permit documented equivalence through business continuity assessments, recovery time and recovery point objectives, encryption, isolated backups, and demonstrated restoration testing, without the mandates described in (a) above;

(c) apply requirements proportionately to the clinical and operational criticality of each system, with enhanced resilience requirements for systems directly supporting patient care, medical-device functionality, or other critical health services, and appropriate safeguards for systems presenting lower patient or operational risk, consistent with the critical-function classification in DoH's existing business continuity policy;

(d) exclude validated, regulatorily compliant infrastructure (e.g., for medical devices or drug production, and/or for data processing associated with healthcare provision or insurance) and avoid requirements that unnecessarily restrict lawful cross-border data processing; and

(e) immediately announce an extended consultation period so that DoH can receive more meaningful public input. If DoH maintains some elements of its proposal, it should extend the implementation period by roughly 24 months – i.e., December 31, 2028, given the significant burdens that the proposals would create for these regulated sectors.

GDA welcomes further discussion and has enclosed relevant background materials on cross-border data flows in Biopharmaceutical Research & Development and Medical Technologies.

Sincerely,
Joseph P. Whitlock
Executive Director, Global Data Alliance
jwhitlock@bsa.org

References

[1] DoH Circular No. 191/2026 (Sept. 25, 2026; effective Jan. 1, 2027), https://www.doh.gov.ae/en/resources/Circulars.

[2] GDA, Cross-Border Data Transfers & Remote Health Services (2020), https://globaldataalliance.org/wp-content/uploads/2020/09/09152020cbdtremotehealth.pdf; Cross-Border Data Transfers & Biopharmaceutical R&D (2021), https://globaldataalliance.org/wp-content/uploads/2021/09/09092021cbdtbiopharma.pdf; Data Transfers Under the EU Proposal on the European Health Data Space (2022), https://globaldataalliance.org/wp-content/uploads/2022/08/07282022gdaeuhealthdataspace.pdf.

[3] IMDRF, Principles and Practices for Medical Device Cybersecurity (2020), §§ 4.2, 5.1–5.2, https://www.imdrf.org/node/461; IMDRF, Principles and Practices for Software Bill of Materials for Medical Device Cybersecurity (2023), § 2, https://www.imdrf.org/sites/default/files/2023-04/Principles%20and%20Practices%20for%20Software%20Bill%20of%20Materials%20for%20Medical%20Device%20Cybersecurity%20%28N73%29.pdf; U.S. FDA, Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submissions (Feb. 2026), https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-medical-devices-quality-management-system-considerations-and-content-premarket.

[4] DoH, Policy on Risk Management and Business Continuity for the Health Sector (2026), DoH/POL/CEPAR/PRMBCHS/V1/2026, §§ 3.1.2.2, 3.2.2, https://www.doh.gov.ae/-/media/3F8709C089064DDEA2529A6AEA70462A.ashx.