ORACLE

A Secure Cloud Future for GCC Health Systems

Why Gulf Corporation Council health systems should transition to Oracle Cloud Infrastructure

September, 2025

Public

ORACLE

Purpose statement

This document provides an overview of Oracle Cloud Infrastructure (OCI) adoption, with a focus on the health systems in the Gulf Corporation Council (GCC) countries, including Bahrain, Kuwait, Oman, Qatar, Saudi Arabia, and the United Arab Emirates.

Disclaimer

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. Your access to and use of this confidential material is subject to the terms and conditions of your Oracle software license and service agreement, which has been executed and with which you agree to comply. This document and information contained herein may not be disclosed, copied, reproduced or distributed to anyone outside Oracle without prior written consent of Oracle. This document is not part of your license agreement nor can it be incorporated into any contractual agreement with Oracle or its subsidiaries or affiliates.

This document is for informational purposes only and is intended solely to assist you in planning for the implementation and upgrade of the product features described. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described in this document remains at the sole discretion of Oracle. Due to the nature of the product architecture, it may not be possible to safely include all features described in this document without risking significant destabilization of the code.

This document may include some forward-looking content for illustrative purposes only. Some products and features discussed are indicative of the products and features of a prospective future launch in the United States only or elsewhere. Not all products and features discussed are currently offered for sale in the United States or elsewhere. Products and features of the actual offering may differ from those discussed in this document and may vary from country to country. Any timelines contained in this document are indicative only. Timelines and product features may depend on regulatory approvals or certification for individual products or features in the applicable country or region.

Introduction

Health system leaders and government leaders across the Gulf States are confronting an urgent truth: legacy, the continued reliance on locally managed IT infrastructure, including patient record databases, is harder to justify. The risks to patient safety, data privacy, public trust, and national health strategy have never been higher, and the solution never clearer.

Oracle Cloud Infrastructure (OCI) offers GCC governments and healthcare organizations a **secure, resilient, and future-ready foundation**—not just for managing sensitive health data, but for unlocking the power of AI to transform care delivery, while limiting administrative overhead and healthcare costs.

Local health systems face a cybersecurity crisis

Recent events make it painfully clear that the risks of legacy infrastructure are no longer theoretical. In June 2025, one of the region's most prominent private providers suffered a significant ransomware attack[1] that forced system shutdowns and disrupted patient services. This incident highlighted the potential vulnerability of locally managed systems—especially those lacking modern, cloud-native security protocols, as provided with OCI.

This attack was only the most recent and well-publicized cyberattack in the region. Globally, healthcare systems are increasingly subject to aggressive cyberattacks[2] because of the highly sensitive patient data they store, their need to maintain operations 24/7/365, and their vulnerability to attack. In some cases, attackers demand a ransom to restore the system's operating capabilities; in others, sensitive health data is exfiltrated and sold on the dark web.

Healthcare data is among the most valuable—and vulnerable—assets in today's digital landscape. Yet many hospitals and ministries across the region continue to rely on local data centers, often managed at the individual facility level. These outdated systems often lack the robust perimeter defenses, unified monitoring, and rapid-response capabilities required to detect and neutralize modern cyber threats.

The **cost of inaction is clear:** financial loss, reputational damage, and national health insecurity.

Why the cloud—and why Oracle?

The recent cyberattack has become a regional wake-up call, as governments and healthcare leaders must now reassess the cybersecurity posture of their institutions. OCI directly addresses these concerns, delivering advanced, multilayered security tailored to healthcare's unique risks. With proactive threat detection, zero-trust architecture, and available private cloud options, OCI protects sensitive health data in ways legacy systems usually cannot.

The 'cloud' is the term used to describe a set of powerful, secure server computers located in professional data centers around the world. These servers are capable of storing and managing billions of data records for a range of customers while maintaining clear record separation. Each customer's data remains private and secure.

Instead of storing data on a local hospital server or individual device, cloud computing enables information to be stored, processed, and accessed over the internet. Just as people use online banking rather than visiting a bank branch to withdraw or deposit funds, or even check account balances, hospitals can use cloud platforms to store and analyze patient data more efficiently and safely—while maintaining full control over who can access that data and where it resides.

The cloud doesn't mean anywhere and everywhere—modern cloud providers like Oracle offer geopolitical region-specific data centers and strict security protections, including in the GCC countries. A secure cloud architecture provides multiple lines of defense that on-premises systems cannot match. **With OCI,** health systems gain a multi-layered security posture, full data residency control, and enterprise-grade resilience tailored to the region's unique needs.

[1] Semafor. "Millions of Dubai Patient Records Hacked". August 5, 2025. https://www.semafor.com/article/06/11/2025/millions-of-dubai-patient-records-hacked
[2] Health Tech Magazine. "Healthcare Cybersecurity Threats 2025". August 5, 2025. https://healthtechmagazine.net/article/2025/01/healthcare-cybersecurity-threats-2025-perfcon

OCI is the platform trusted to power mission-critical workloads across commercial enterprises, global finance, and sensitive government agencies in the U.S. and other countries. Purpose-built for security, performance, cost efficiency, and resilience at scale, OCI provides the digital backbone required to support the most sensitive and consequential national health operations.

Key features of OCI include

- **Always-on encryption**: data is protected during transit and while stored
- **Autonomous Shield and security zones:** these enforce security best practices automatically and continuously without the need for human intervention
- **Oracle Data Safe:** provides continuous auditing of user access and sensitive data activity
- **Customer-controlled key management:** Hospitals retain control over their encryption keys using Oracle Vault, a critical capability for compliance and control
- **Dedicated cloud regions:** Oracle operates in-country data centers in Jeddah, Abu Dhabi, Oman, Dubai, and Kuwait, so that sensitive health data never leaves national borders

Together, these capabilities enable governments and providers to detect, respond to, and mitigate threats quickly and more consistently than with legacy infrastructure[3].

OCI also provides high availability, redundant backups, and disaster recovery across multiple cloud regions. This helps health systems remain operational even during cyberattacks or national emergencies, protecting both patients and infrastructure.

In contrast, on-premises systems are often single points of failure. If a ransomware attack takes down a local server, restoring operations can take days or weeks—time that patients cannot afford.

Beyond security: additional value of OCI

In addition to cybersecurity benefits of cloud adoption, OCI offers organizations a wide range of operational, financial, and clinical advantages.

Lower cost of ownership: migrating to Oracle Cloud Infrastructure has been found to limit the total cost of ownership by shifting health systems away from capital-intensive expenditures, such as hardware procurement and data center cooling. Instead, OCI enables a flexible operational expense model. Its pay-as-you-go scalability enables systems to expand during periods of high demand and contract during normal operations, enhancing cost efficiency. In addition, autonomous services in OCI alleviate the burden on IT teams, lowering personnel requirements and enabling staff to focus on innovation rather than maintenance[4].

Accelerated innovation: OCI provides advanced tools for rapid development and deployment of AI models, including graphic processing unit (GPU) clusters, automated machine learning, and FHIR-based APIs. These resources support fast training cycles and seamless integration with clinical systems. Cloud-based infrastructure also enables near real-time public health analytics and predictive care recommendations at national and regional scales. By harmonizing and standardizing data across institutions and borders, OCI could facilitate collaborative research and care coordination throughout the region.

Strategic fit: the move to OCI would directly support the digital transformation goals articulated in national initiatives, including Saudi Arabia's Vision 2030 and the UAE National Strategy for AI 2031. Customer data is stored and hosted in the same country in which the customer is located unless otherwise mutually agreed. There are some operational differences depending upon the type of data center utilized, but our information security program does not change.

[3] Oracle. "Why Migrate to the Cloud: 11 Benefits to Your Business". August 5, 2025. https://www.oracle.com/uk/cloud/why-move-to-cloud/#:~:text=4.,factor%20authentication%20and%20data%20encryption.
[4] Oracle. "CMRI uses Oracle AI to help cure children's cancer, improves efficiency by 30-50%". August 5, 2025. https://www.oracle.com/customers/cmri-case-study/

ORACLE

A safer path forward

Transitioning to OCI does not require a disruptive overhaul of local organizations' current data management processes. Instead, health ministries and hospital networks can adopt a phased, security-first strategy that offers continuity, compliance, and control throughout the process.

Oracle has extensive worldwide experience in migrating legacy systems to its OCI platform. Services and support are provided to local organizations to support a smooth transition, and local organizations retain control over their data.

As cloud adoption expands, ministries and providers can implement unified data governance policies, providing consistent access control, auditability, and regulatory alignment across departments and regions. This governance framework also sets the stage for advanced use cases, including AI-driven analytics, near real-time public health surveillance, and international research collaboration.

This structured migration not only helps mitigate cyber risk—it also creates the conditions for long-term clinical and economic transformation.

Conclusion

Cyberattacks are no longer speculative—they are happening now, across the Middle East as often as in other regions of the world. In this climate, continuing to store sensitive health data on locally managed infrastructure is no longer safe, affordable, or strategic.

OCI offers a proven, sovereign, and secure path forward. With its layered defense architecture, regional data centers, and healthcare-optimized tools, OCI enables hospitals and ministries to safeguard their most critical assets while advancing the region's bold healthcare vision.

Modern medicine demands modern infrastructure. In today's world, security is care—and OCI delivers both.

Connect with us

Call **+1.800.ORACLE1** or visit **oracle.com**. Outside North America, find your local office at: **oracle.com/contact**.

blogs.oracle.com linkedin.com/company/oracle x.com/oracle_ME