ORACLE

Advisory: Oracle Cloud Infrastructure and the United Arab Emirates Health Data Law

Description of Oracle Cloud Infrastructure in the Context of the United Arab Emirates (UAE) Federal Law No. 2 of 2019 on the use of Information and Communication Technology (ICT) in Health Fields

February 2022, Version 2.0

Public

Disclaimer

This document in any form, software or printed matter, contains proprietary information that is the exclusive property of Oracle. This document is not part of your 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 assessing your use of Oracle Cloud Infrastructure in the context of the requirements applicable to you pursuant to Federal Law No. 2 of 2019 Concerning the Use of Information and Communication Technology (ICT) in Health Fields (Health Data Law). This may also help you to assess Oracle as an outsourced service provider. You remain responsible for making your own independent assessment of the information in this document as the information in this document is not intended and may not be used as legal advice about the content, interpretation or application of laws, regulations, and regulatory guidelines. You should seek independent legal advice regarding the applicability and requirements of laws and regulations discussed in this document.

This document does not make any commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, and timing of any features or functionality described in this document remains at the sole discretion of Oracle.

The Health Data Law referenced in this document is subject to periodic changes or revisions by the applicable regulatory authority. The current version of the guidelines is available at mohap.gov.ae/app_content/legislations/php-law-en-77/mobile/index.html. Because this document is based on information available at the time of its drafting, it is subject to change at the sole discretion of Oracle Corporation, and may not always reflect changes in the regulations.

Revision History

The following revisions have been made to this document since its initial publication.

DATE	REVISION
February 2022	Revised to limit document scope to Oracle Cloud Infrastructure
July 2021	Initial publication

Table of Contents

Introduction

The Federal Law No. 2 of 2019 Concerning the Use of Information and Communication Technology (ICT) in Health Fields (Health Data Law) in the United Arab Emirates (UAE) went into effect on November 1, 2020. The Health Data Law regulates the use of information and communication technology (ITC) in the healthcare sector. Article 2 provides the scope and application of this law: "This Law shall apply to all Information and Communication Technology (ICT) methods and usages in the health fields in the State, including Free Zones."

One stated objective in Article 3 of the Health Data Law is to enable the Ministry of Health and Prevention ("Ministry") to "collect, analyze, and keep health information at the state [UAE] level." In accordance with Article 5 on page 3, the Ministry establishes a central system in coordination with federal or local government health authorities in the state to keep, exchange, and collect health information data in the UAE.

Document Purpose

Key aspects of the Health Data Law need to be considered when a regulated entity evaluates the use of Oracle Cloud Infrastructure (OCI) to support healthcare workloads. This document provides information to help you determine the suitability of using OCI in the context of the Health Data Law requirements. The document also describes several Oracle Cloud services and practices that can help you address your regulatory obligations. The information contained in this document doesn't constitute legal advice. Customers are advised to seek their own legal counsel to develop and implement their compliance program and to assess the features and functionality provided by Oracle regarding to their specific legal and regulatory requirements.

About Oracle Cloud Infrastructure

Oracle's mission is to help people see data in new ways, discover insights, and unlock endless possibilities. Oracle provides various cloud solutions tailored to customers' needs. These cloud offerings provide customers the benefits of the cloud, including global, secure, and high-performance environments to run all their workloads. The cloud offerings discussed in this document apply to Oracle Cloud Infrastructure (OCI).

Note: Oracle Cloud software-as-a-service (SaaS) applications, Oracle GBU SaaS, NetSuite, and Advertising SaaS Services are not included in the scope of this document.

OCI is a set of collaborative cloud services that enable customers to build and run a wide range of applications and services in a highly available and secure hosted environment. OCI offers high-performance compute capabilities and storage capacity in a flexible overlay virtual network that is easily accessible from on-premises network. OCI delivers high-performance computing power to run cloud native and enterprise IT workloads. For more information about OCI, see docs.oracle.com/iaas/Content/home.htm.

The Cloud Shared Management Model

From a security management perspective, cloud computing is fundamentally different from on-premises computing. On-premises customers are in full control of their technology infrastructure. For example, they have physical control of the hardware and full control over the technology stack in production. In the cloud, however, customers use components that are partially under the management of the cloud service providers. As a result, the management of security in the cloud is a shared responsibility between the cloud customers and the cloud service provider.

Oracle provides best-in-class security technology and operational processes to Oracle's secure enterprise cloud services. However, customers must also be aware of and manage their security and compliance responsibilities when running their workloads in OCI services. By design, Oracle provides security functions for cloud infrastructure and operations, such as cloud operator access controls and infrastructure security patching. Customers are responsible for securely configuring and using their cloud resources. For more information, see the cloud service documentation.

The following figure illustrates this division of responsibility at high level.

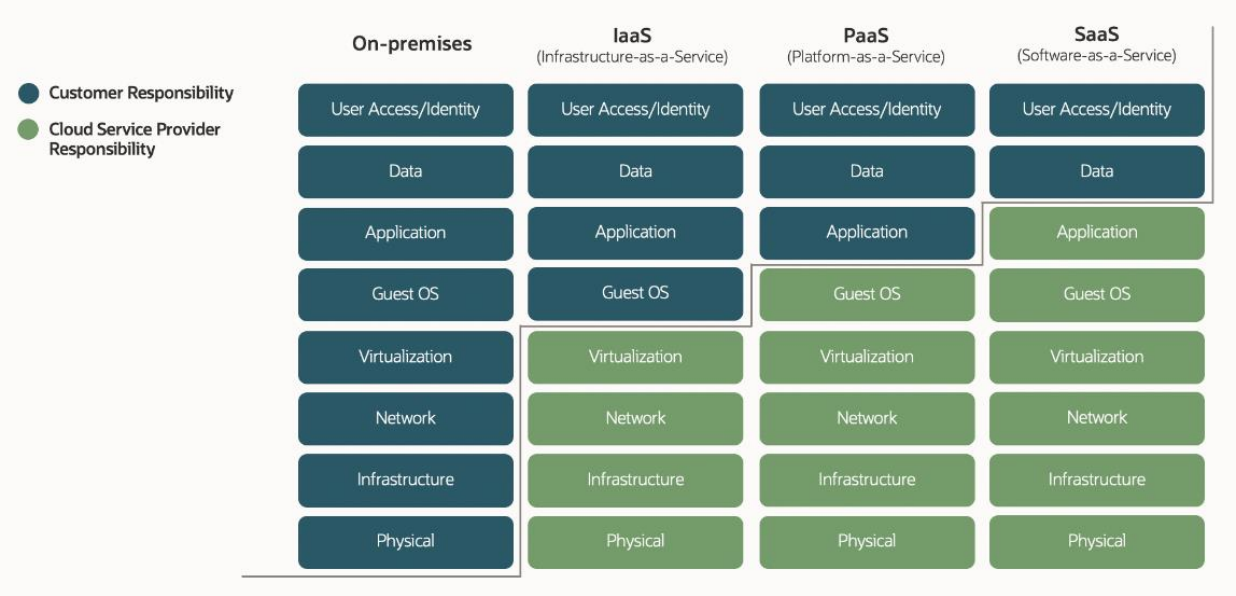

Figure 1: Conceptual Representation of the Various Security Management Responsibilities Between Customers and Cloud Providers

Summary of the UAE Health Data Law

The following table lists a subset of the UAE Health Data Law articles that might be applicable to the use of OCI within the UAE. The Health Data Law consists of 31 articles. For more details, refer to the full Health Data Law, mohap.gov.ae/app_content/legislations/php-law-en-77/mobile/index.html.

SECTION	REQUIREMENT
Article 4	**ICT Use Obligations** The following conditions shall be adhered to when using ICT in health fields: 1. Keeping all health data and information confidential and allowing their circulation only in the permitted cases; 2. Ensuring the validity and credibility of the health data and information, by protecting the integrity thereof from destruction or unauthorized amendment, alteration, deletion or addition; 3. Ensuring the availability of the health data and information to the authorized parties and facilitating access thereto when needed.
Article 13	**Storage and Transfer of Health Information and Data Outside the State** The health information and data related to the health services provided in the State may only be stored, processed, generated or transferred outside the State in the cases prescribed by virtue of a decision issued by the Health Authority in coordination with the Ministry.
Article 16	**Confidentiality of Information Related to Patients and Exclusions** Without prejudice to any legislation in force, whoever circulates information related to patients shall keep them confidential and shall abstain from using them for non-health purposes without obtaining a written approval of the patient, the following cases shall be excluded: 1. The health information or data required by health insurance companies or any entity funding the provisions of health services received by the patient, for the purposes of auditing, approving or verifying the financial benefits related to those services; 2. Scientific and clinical research purposes, provided that the identity of patients is not disclosed and that the ethics and rules of scientific research are respected; 3. Taking preventative and curative measures related to the public health or for the sake of protecting the health and safety of the patient or any other related person; 4. Upon request of the competent judicial entities;

SECTION	REQUIREMENT
	5. Upon request of the Health Authority for the purposes of control, inspection and protection of public health.
Article 20	**Keeping Health Information and Data** 1. Keeping health information and data through ICT shall be as per the following: a. The period during which health information and data are kept shall commensurate with the need thereof, provided that it is no less than 25 (twenty-five) years as of the date of the last health procedures provided to the person concerned with such health information and data; b. Ensuring the application of confidentiality, validity and credibility standards of such health information and data; 2. The Executive regulation of this Law shall prescribe the controls and procedures for the implementation of the provisions of this Article.

Description of Oracle's Policies and Practices

This section describes OCI operational and security practices and services in the context of the preceding Health Data Law articles.

Article 4: ICT Use Obligations

Oracle is a data processor, and UAE health entities and authorities who subscribe to Oracle cloud services are data controllers. As data controllers, customers own their data that's processed or stored in Oracle cloud services. As the data controller, UAE health entities and authorities are responsible for the direct protection of their data, including security measures that restrict access to the ICT. For more information, see oracle.com/a/ocom/docs/oci-privacy-features.pdf.

Oracle's Information Security Policy help establish the principles to protect, manage, and secure information assets, in accordance with business, legal, regulatory, and contractual requirements.

Oracle provides the following resources related to OCI security services, features, and recommendations:

- Oracle Corporate Security Practices: oracle.com/assets/corporate-security-practices-4490843.pdf
- OCI Security Services and Features: docs.oracle.com/iaas/Content/Security/Concepts/security_features.htm
- OCI Security Overview: docs.oracle.com/iaas/Content/Security/Concepts/security_overview.htm
- OCI Security Guide: docs.oracle.com/iaas/Content/Security/Concepts/security_guide.htm

Article 13: Storage of Health Information and Data Outside the State

Oracle currently operates data centers in the UAE. UAE health entities can use OCI services to address data storage, process, generation, or transfer requirements in the context of your content that is stored in or run through the OCI services (Content). For information about data center locations, see oracle.com/cloud/architecture-and-regions/.

Oracle is transparent about where your data is processed and stored. When setting up your OCI account, you choose a home region in which your tenancy is located. Your data stays within that region unless you choose to move it outside the region. Through the Oracle Cloud Console user interface and API documentation, you have visibility into when actions cause data to move to another region or tenancy. For more information, see the following topics:

- Regions and Availability Domains: docs.cloud.oracle.com/iaas/Content/General/Concepts/regions.htm
- Setting Up Your Tenancy: docs.cloud.oracle.com/iaas/Content/GSG/Concepts/settinguptenancy.htm

Article 16: Confidentiality of Information Related to Patients and Exclusions

The Oracle Services Privacy Policy and Data Processing Agreement for Oracle Services provide transparency into Oracle's overall approach to the handling of customer Content. However, under the infrastructure-as-a-service (IaaS) model, Oracle generally has no insight into the data that customers store and process in OCI, such as patient health information. The customer must evaluate any assessment of whether the data is subject to any other confidentiality requirements of the Health Data Law.

However, Oracle offers encryption capabilities and a key management service to help protect your data, including where appropriate health data.

Encryption

The encryption described in this section occurs by default regardless of the nature of the underlying data. OCI doesn't have insight into the nature of your data, whether personal data, sensitive data, or otherwise.

- **Block Volume**: Data is encrypted at rest by default, and the backups are also encrypted in Object Storage.

  See Block Volume Encryption at docs.cloud.oracle.com/iaas/Content/Block/Concepts/overview.htm#BlockVolumeEncryption.

- **Object Storage**: Each object is encrypted with its own key. Encryption is enabled by default.

  See Object Storage Features at docs.cloud.oracle.com/iaas/Content/Object/Concepts/objectstorageoverview.htm#features.

- **File Storage**: Customer data is encrypted at rest by default.

  See Encryption for File Storage at docs.cloud.oracle.com/iaas/Content/File/Concepts/filestorageoverview.htm#encryption.

- **Bare metal and virtual machine (VM) database systems**: Encryption of user-created tablespaces is enabled by default using Transparent Data Encryption (TDE).

  See Transparent Data Encryption at docs.cloud.oracle.com/iaas/Content/Database/Tasks/configuringDB.htm?#Transparent_Data_Encryption.

- **Exadata Cloud Service**: All new tablespaces that you create in the Exadata Cloud Service database are encrypted by default.

  See Managing Tablespace Encryption (Exadata) at docs.cloud.oracle.com/iaas/Content/Database/Tasks/exaconfiguring.htm#Managing_Tablespace_Encryption.

Vault

The Vault key management service provides centralized management of the encryption of customer data with keys that you control. You can use it for the following tasks:

- Create master encryption keys and data encryption keys.
- Rotate keys to generate new cryptographic material.
- Enable or disable keys for use in cryptographic operations.
- Assign keys to resources.
- Use keys for encryption and decryption to safeguard data.

The Block Volume, Object Storage, File Storage, and Streaming services integrate with Vault to support the encryption of data in those services. The integration of Vault with Identity and Access Management (IAM) lets you control who and what services have access to your keys. The Audit service lets you track administrative actions on your keys and vaults.

See an overview of Vault at docs.cloud.oracle.com/iaas/Content/KeyManagement/Concepts/keyoverview.htm.

Article 20: Keeping Health Information and Data

In OCI, Oracle generally has no insight into customer content that customers collect, process, or store in Oracle cloud services. Any assessment of whether data contains health information that must meet specific data retention requirements, the customer as the data controller must determine. This assessment includes a customer evaluation of whether a particular service and or region is suitable for their workload and data. However, OCI provides numerous storage, encryption, and key management services to help protect customer content, including where appropriate patient health data. For more information, see the following topics:

- **Archive Storage** is designed for storing data that's seldom accessed but requires long retention periods. See docs.oracle.com/iaas/Content/Archive/Concepts/archivestorageoverview.htm.
- **Block Volume** lets you use a block volume as a regular hard drive when it's attached and connected to a compute instance. Data durability is enhanced by automatically replicating volumes to help protect against data loss. See docs.oracle.com/iaas/Content/Block/Concepts/overview.htm.
- **Object Storage** lets you store unstructured data of many content types. It actively monitors technical data integrity using checksums intended to automatically detect and repair damaged data. Object Storage actively monitors and provides data redundancy. If a redundancy loss is detected, Object Storage is designed to automatically create more data copies. See docs.oracle.com/iaas/Content/Object/Concepts/objectstorageoverview.htm.

Also, as specified in the Oracle Data Processing Agreement, customers can provide extra written instructions to Oracle regarding the processing of personal information in accordance with applicable data protection laws.

Conclusion

Oracle allows UAE healthcare entities and authorities to become more agile, collaborative, and insightful while meeting their obligations under the Health Data Law. Oracle's data centers, security policies and practices, and cloud services can accelerate innovation for healthcare entities and authorities operating in the UAE.

References

- Federal Law No. 2 of 2019 Concerning the Use of Information and Communication Technology in Health Fields: mohap.gov.ae/FlipBooks/PublicHealthPolicies/PHP-LAW-EN-77/mobile/index.html#p=1
- Oracle Services Privacy Policy: oracle.com/legal/privacy/services-privacy-policy.html
- Data Processing Agreement and related documentation for Oracle services: oracle.com/corporate/contracts/cloud-services/contracts.html#data-processing
- Oracle Cloud Services Hosting and Delivery Policies: oracle.com/corporate/contracts/cloud-services/hosting-delivery-policies.html
- Oracle Cloud Services Contracts: oracle.com/corporate/contracts/cloud-services/contracts.html
- Oracle Cloud Services Agreement: oracle.com/corporate/contracts/cloud-services/contracts.html - ct07tabcontent4

Other Resources

- Oracle Corporate Security Practices: oracle.com/corporate/security-practices
- Oracle Cloud Infrastructure Security Architecture: oracle.com/a/ocom/docs/oracle-cloud-infrastructure-security-architecture.pdf
- Oracle Cloud Infrastructure Privacy Features: oracle.com/a/ocom/docs/oci-privacy-features.pdf
- Oracle Cloud Compliance: oracle.com/corporate/cloud-compliance/

- Welcome to Oracle Cloud Infrastructure: docs.oracle.com/iaas/Content/GSG/Concepts/baremetalintro.htm
- Documentation about Oracle Cloud Infrastructure: docs.oracle.com/iaas/Content/home.htm

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 facebook.com/oracle twitter.com/oracle