Navigating the Israeli Ministry of Health Cloud Computing Circular on AWS

January 18, 2023

Notices

Customers are responsible for making their own independent assessment of the information in this document. This document: (a) is for informational purposes only, (b) represents current AWS product offerings and practices, which are subject to change without notice, and (c) does not create any commitments or assurances from AWS and its affiliates, suppliers or licensors. AWS products or services are provided “as is” without warranties, representations, or conditions of any kind, whether express or implied. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

Contents

Abstract

This document provides information for software vendors who want to use Amazon Web Services (AWS) to provide software to healthcare providers in Israel while complying with key privacy requirements. It reviews general guidelines from the National Cyber Directorate and Ministry of Health describing expectations of health care providers to operate their solutions in the cloud. Key topics include the following:

- The requirements for independent software vendors (ISVs) when they operate a service for healthcare providers
- The geographic locations where customers can store content
- The roles played by the customer and AWS in managing and securing content hosted on AWS

Introduction

This whitepaper focuses on typical questions asked by AWS customers when they are considering the implications of the Israeli Ministry of Health guidelines on their use of AWS services to store or process content containing personal health information. There will also be other relevant considerations for each customer to address, such as contractual commitments that a customer makes to a third party. Soon customers might also need to comply with the new Israeli Protection Of Privacy Law, which is currently passing through the legislation process.

This paper is provided solely for informational purposes. It is not legal advice, and should not be relied on as legal advice. Because each customer's requirements will differ, AWS strongly encourages customers to obtain appropriate advice on their implementation of privacy and data protection requirements, and on applicable laws and requirements relevant to their business.

In this paper, *content* refers to software (including virtual machine images), data, text, audio, video, images, and other content that a customer, or end user, stores or processes using AWS services. For example, a customer's content might include objects stored in an Amazon Simple Storage Service (Amazon S3) bucket, files stored on an Amazon Elastic Block Store (Amazon EBS) volume, or data stored in an Amazon DynamoDB database table. The terms of the AWS Customer Agreement, or any other relevant agreement with us governing the use of AWS services, apply to customer content.

Considerations relevant to privacy and data protection

Storage and processing of content presents software vendors with a number of common practical matters to consider, including:

- Will the content be secure?
- Where will content be stored?
- What laws and regulations apply to the content and what is needed to comply with these?

When using AWS services, each AWS customer maintains ownership and control of their content, including control over:

- What content they choose to store or process using AWS services
- Which AWS services they use with their content
- The AWS Region or Regions where their content is stored
- The format, structure, and security of their content, including whether it is masked, anonymized, or encrypted
- Who has access to their AWS accounts and content, and how those access rights are granted, managed, and revoked

Because AWS customers retain ownership and control over their content within the AWS environment, they also retain responsibilities relating to the security of that content as part of the AWS Shared Responsibility Model. This shared responsibility model is fundamental to understanding the respective roles of the customer and AWS in the context of privacy and data protection requirements that might apply to content that customers choose to store or process using AWS services.

Considerations relevant for using the cloud in a healthcare organization

Health organizations are required by the Israel National Cyber Directorate (INCD) to follow the cybersecurity methodology defined in their Use of Cloud Services guidance. The Use of Cloud Services guidance extends the Defense Methodology document and lists the controls that are relevant for cybersecurity in government organizations.

Definitions

This whitepaper uses the following definitions:

Healthcare organization. A clinic, health maintenance organization (HMO), or hospital

Software vendor. A company that makes and sells software that is deployed on the cloud

Organizational cloud committee. A cybersecurity committee that operates in the healthcare organization and includes at least the following officials:

- A representative of the Chief Executive Officer
- A representative of the organization's legal counsel
- The organization's Chief Information Security and Cybersecurity officer, or their representative
- The organization's Privacy Protection Officer, or their representative, if such appointed
- The organization's Chief Information Systems Officer, or their representative

A healthcare organization may define an existing committee as the organizational cloud committee, provided that it meets the conditions set forth in these provisions. A committee member may hold one or more positions, depending on the definitions of the committee member's professional roles in the organization, provided the committee is composed of at least three members.

Sectoral cloud committee. A committee operating in the Ministry of Health, and whose members include:

- A representative of the Director General of the Ministry of Health; a representative of the legal counsel of the Ministry of Health

- Chief Information Security and Cybersecurity Officer of the Ministry of Health
- A representative of the Digital Health Department of the Ministry of Health
- A representative of the National Cyber Directorate
- A representative of the Information and Communications Technology (ICT) Authority
- A representative of the Privacy Protection Authority

Risk assessment process. A procedure in the healthcare organization that assesses the potential risk of deploying the solution provided by the software vendor. The cloud committee that is responsible for approving the solution is determined by the risk level.

Project Nimbus. A large-scale, multi-year flagship project jointly managed by the Government Procurement Administration, Government Computer Authority at the Ministry of Cyber and Digital Matters, Office of Legal Counsel at the Ministry of Finance, National Cyber Security Authority, Budget Department, Ministry of Defense, and Israel Defensive Forces.

Project Nimbus is intended to provide a thorough and comprehensive reference for the provision of cloud services for the Israeli government. The project creates a cloud services supply channel and presents government policy on migration to the cloud, modernization of services, controls, and optimization of activities in the cloud.

Transferring data outside of Israel

The Transfer of Information Regulations states that data from a database in Israel must not be transferred to another country, except if the law of such country ensures a level of protection with respect to personal data that is no less stringent than that provided by Israeli law. On July 1, 2020, the Israeli Data Privacy and Protection Authority (IDPPA) stated its position that the law of the European Union (EU) and United Kingdom (UK) ensures such level of protection, and therefore, transfer of personal data to countries that are or were members of the EU and UK is permitted, provided that those countries continue to comply with the provisions of EU law regarding protection of personal data.

The Ministry of Health circular

The Ministry of Health of Israel regulates software in the healthcare and life sciences industries by defining a process with general guidelines of what is expected from the healthcare provider in order to operate the solution in the cloud, as well as in compliance with the Privacy Protection Law. The process is based on the Use of Cloud Computing in the Israeli Healthcare System circular. To encourage the introduction of advanced technologies for use by healthcare organizations, the circular establishes criteria that healthcare organizations should follow for the proper operation of computing applications using the cloud.

The current process seeks to enable healthcare providers to use tools that can assist them to meet the compliance requirements of the Privacy Protection Law and other information security and cybersecurity standards and to address risks related to information security, privacy, and maintenance of the organization's operational continuity.

The risk assessment process

To deploy software in the cloud or consume software as a service (SaaS) solutions, the HMO needs a procedure to assess risks. Under the circular, the HMO is required to manage and document the risk assessment process, which is described in the following sections. The risk level classification is determined based on the findings of the risk assessment.

Although the HMO is responsible for the risk assessment process, the software vendor needs to share information about the software to support the HMO in this process.

The risk management tool was developed by the Digital Health Department and the IT Department of the Ministry of Health, in order to enable a uniform and complete risk management process in the Israeli healthcare system while assisting organizational cloud committees to comply with cloud regulations. The tool is based on the Cyber Defense Methodology and the specific guidelines of the Cyber Directorate, Government ICT Authority, and Ministry of Health.

Committee selection based on risk

After completing all sheets, the tool calculates the risk for each subtype, as well as for the service overall. The risk score is calculated as follows: low risk, up to 40 points; medium risk, between 40 and 75 points; high risk, above 75 points. The risk score determines which committee you need to contact to receive approval for activation of the cloud services: low and medium risk, organizational committee only; high risk, sectoral committee recommendation followed by organizational committee approval. After that, supplemental process forms, which are also submitted to the appropriate committees, emphasize the description of the system (for example, the interfaces and requested architecture), as well as legal opinion and a description of the compensating controls for the calculated risk.

Aspects examined during the risk assessment process

The assessment examines the following aspects:

Description of the business process

- The business process and the interactions between processes within the organization and systems in the cloud should be described.
- The objective of the system and its usage must be specified, as well as the reasons and expected benefits from the transition to the cloud.

Analysis of information

- A complete review and analysis of the information and applications that are intended to be transferred to the cloud must be performed, which includes examination of the following:
    - **Mapping of information.** The information that is expected to be transferred to the cloud environment must be mapped, including whether it was published to the public, whether it is exposed to external parties, whether the information is classified, whether it will contain personal and private data, whether it will contain data that might affect the proper functioning of the organization and might harm governance, whether it will contain medical data, and the level of its identifiability.
    - **Classification of information.** The sensitivity of the data must be examined.
    - **The scope of the information.** The amount of information expected to be transmitted during the use of the system should be examined.

System analysis

- **Interface mapping.** The external interfaces of the internal network and the external interfaces of other third parties should be examined. This includes the frequency of the connection to the interface, the direction of the connection, the protocol, the type of authentication and authorization, and the nature of the communication.
- **User mapping.** The parties that use the application, the permissions required for them, and the parties that will have access to the cloud must be mapped and defined. User classification, number of users, administrators, user definition and permissions, and access to the system must be addressed.
- **Existing cloud infrastructure.** The existing cloud systems of the healthcare provider and how they can integrate with the solution should be examined.

- **Communications provider to and from the cloud.** The communications provider, its infrastructure, applicable regulations, the defined level of service, and protection measures should be examined.
- **Characteristics of the requested service.** The infrastructure of the vendor should be examined, including backup procedures, data storage, data durability, encryption (minimum AES256), data monitoring, system monitoring, migration process, performance, and penetration tests.

Risk analysis

- All possible risks that arise from using the application based on the preceding analysis should be mapped. The risk analysis should address the individual risks arising from the use of medical information and from the application.
- Each risk should relate the probability of its occurrence, the severity of the damage, and the controls to be implemented to reduce the probability of occurrence and the severity of the damage.
- The risks should be examined according to the values of confidentiality, availability, and integrity of the information and in accordance with the cloud usage model—for example, SaaS, platform as a service (PaaS), and infrastructure as a service (IaaS)—and the shared responsibility between the cloud provider and the healthcare organization.
- The level of risk is determined by assessing the following parameters: the type of information and its sensitivity; the scope of the data transmitted to the cloud—both in terms of the number of records and the type of information in each record; and the duration that the information will be stored in the cloud.
- For each risk, the healthcare provider must define the measures that will be implemented to reduce and respond to the risk.

Proposed architecture

- The proposed architecture for the solution must be presented, including the solution components, the interfaces, the security mechanisms that will be activated, and the method of their implementation.
- Many of the architectural aspects are addressed as part of the AWS Well-Architected Framework, which describes the key concepts, design principles, and architectural best practices for designing and running workloads in the cloud.

Examples of threats while transitioning to a public cloud

The ministry of health provides examples with regards to HMOs' usage of a cloud environment. These examples are published in Addendum B of the *Use of Cloud Computing in the Israeli Healthcare System* circular. The examples refer to risks and threat scenarios when approaching an HMO and considering the architecture of the application.

Examples of threats

The following are some examples of risks and threat scenarios whose impact and related concerns should be considered when formulating a decision to move to a cloud environment, and when assessing the control processes for risk mitigation. These examples are from the *Government Cyber Security Guidance No. 5.5: Securing information for moving to a public cloud*. Note that these are only examples, and not an exhaustive list, of the risks and threat scenarios. You should examine additional risks and threats of using a public cloud, depending on the type of service and its characteristics, and the type of system and information transmitted to the cloud.

Disclosure or leakage of data

- Disclosure of information resulting from an inefficient separation between cloud customers (tenants) who share computing resources.
- Information disclosure due to a court order of a foreign government. Retention of information in a jurisdiction other than the State of Israel, exposes the information to the laws and regulations of the governments in which the data is stored.
- Leakage of databases and sensitive information that have been left in the cloud after engagement with the ISV has ended.
- Information disclosure by the employees of the ISV or a third party, who have the ability to access the information and might not be bound by contract to confidentiality of the information and to its owners.
- Disclosure of information due to unauthorized access into a mobile device which might store data in the cloud. Unauthorized access into such devices might result in information disclosure if the device is not protected by appropriate means.
- Loss or disruption of data. The threat should be examined under the following scenarios:
    - Information is lost or disrupted on the cloud provider side.
    - Information is lost or disrupted due to unauthorized access to the cloud environment.

- The ISV ends its services.
- The data is intercepted while in transit to the cloud.

Loss of data availability

- A distributed denial of service (DDOS) attack occurred.
- The ability to connect to the cloud was lost due to a network connection failure.
- The ISV account was blocked due to a malfunction, attack, or violation of the terms of service.
- The ISV does not meet the required performance or service level agreement (SLA).

Mitigations and proposed best practices

The following section describes the best practices for implementing secure environments on AWS.

AWS Shared Responsibility Model

Moving IT infrastructure to AWS creates a shared responsibility model between the customer and AWS, as both the customer and AWS have important roles in the operation and management of security. AWS operates, manages, and controls the components from the host operating system and virtualization layer down to the physical security of the facilities in which the AWS services operate. The customer is responsible for management of the guest operating system (including updates and security patches to the guest operating system) and associated application software, as well as the configuration of the AWS-provided security group firewall and other security-related features. The customer generally connects to the AWS environment through services that the customer acquires from third parties (for example, internet service providers). AWS does not provide these connections, and they are therefore part of the customer's responsibility. Customers should consider the security of these connections and the security responsibilities of such third parties in relation to their systems. The respective roles of the customer and AWS in the shared responsibility model are shown in Figure 1.

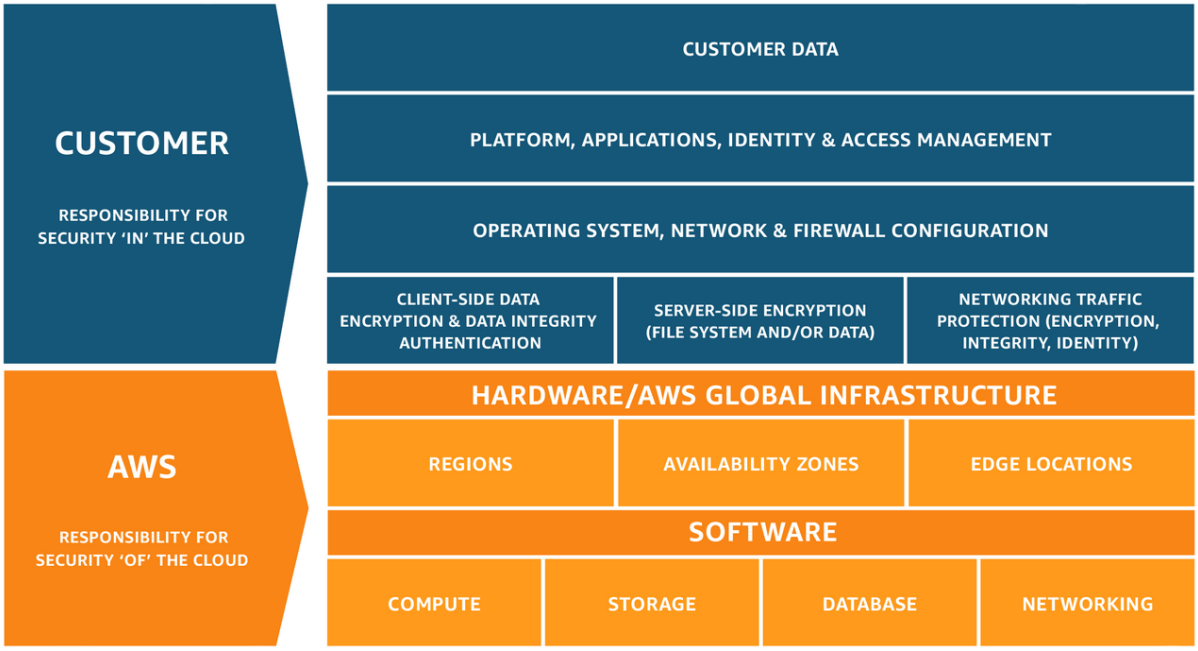

Figure 1 – AWS Shared Responsibility Model

What does the shared responsibility model mean for the security of customer content?

When evaluating the security of a cloud solution, it is important for customers to understand and distinguish between:

- Security OF the cloud – Security measures that the cloud service provider (AWS) implements and operates.
- Security IN the cloud – Security measures that the customer implements and operates, related to the security of customer content and applications that make use of AWS services.

Although AWS manages security of the cloud, security in the cloud is the responsibility of the customer because customers retain control of the security measures that they choose to implement to protect their own content, applications, systems, and networks – just as they would for applications in an on-site data center.

Understanding security OF the cloud

AWS is responsible for managing the security of the underlying cloud environment. The AWS Cloud infrastructure has been architected to be one of the most flexible and secure cloud environments available, designed to provide optimum availability while providing complete customer segregation. It provides extremely scalable, highly reliable services that are designed to help customers deploy applications and content quickly and securely, at massive global scale if necessary. AWS services are content agnostic, in that they offer the same high level of

security to all customers, regardless of the type of content being stored, or the geographical region in which they store their content. AWS has world-class, highly secure data centers that use state-of-the-art electronic surveillance and multi-factor access control systems. Data centers are staffed 24/7 by trained security guards, and access is authorized strictly on a least privileged basis. For a complete list of the security services and measures built into the core AWS Cloud infrastructure, see the AWS Security Documentation.

We are vigilant about our customers' security and have implemented sophisticated technical and physical measures against unauthorized access. Customers can validate the security controls in place within the AWS environment through AWS certifications and reports, including the AWS System and Organization Controls (SOC) 1, 2, and 3 reports; International Organization for Standardization (ISO) 27001, 27017, 27018, and 9001 certifications; and Payment Card Industry Data Security Standard (PCI DSS) Attestation of Compliance. Our ISO 27018 certification demonstrates that AWS has a system of controls in place that specifically address the privacy protection of customer content. These reports and certifications are produced by independent third-party auditors and attest to the design and operating effectiveness of AWS security controls. You can request AWS compliance certifications and reports on the AWS Compliance Contact Us page. For more information on AWS compliance certifications, reports, and alignment with best practices and standards, see AWS Compliance.

Understanding security IN the cloud

Customers retain ownership and control of their content when using AWS services. Customers, rather than AWS, determine what content they store or process using AWS services. Because it is the customer who decides what content to store or process using AWS services, only the customer can determine what level of security is appropriate for the content that they store and process using AWS. Customers also have complete control over which services they use and whom they empower to access their content and services, including what credentials are required. Customers control how they configure their environments and secure their content, including whether they encrypt their content—at rest and in transit—and what other security features and tools they use and how they use them. AWS does not change customer configuration settings because these settings are determined and controlled by the customer. AWS customers have the freedom to design their security architecture to meet their compliance needs. This is a key difference from traditional hosting solutions where the provider decides on the architecture. AWS enables and empowers the customer to decide when and how to implement security measures in the cloud, in accordance with each customer's business needs.

For example, if a customer needs a higher availability architecture to protect their content, the customer can add redundant systems, backups, locations, or network uplinks to create a more resilient, high availability architecture. If the customer needs restricted access to their content, AWS enables the customer to implement access rights management controls both on a systems level and through encryption on a data level.

To assist customers in designing, implementing, and operating their own secure AWS environment, AWS provides a wide selection of security tools and features that customers can use. Customers can also use their own security tools and controls, including a wide variety of

third-party security solutions. Customers can configure their AWS services to use a range of such security features, tools, and controls to protect their content, including sophisticated identity and access management tools, security capabilities, encryption, and network security. Examples of steps that customers can take to help secure their content include the following:

- Implement strong password policies, assign appropriate permissions to users, and take robust steps to protect their access keys.
- Apply appropriate firewalls and network segmentation, encrypt content, and properly architect systems to decrease the risk of data loss and unauthorized access.

Because customers, rather than AWS, control these important factors, customers retain responsibility for their choices, and for security of the content that they store or process using AWS services, or that they connect to their AWS infrastructure, such as the guest operating system, applications on their compute instances, and content stored and processed in AWS storage, databases, or other services.

AWS provides an advanced set of access, encryption, and logging features to help customers manage their content effectively, including AWS Key Management Service (AWS KMS) and AWS CloudTrail. To assist customers in integrating AWS security controls into their existing control frameworks and help customers design and run security assessments of their organization's use of AWS services, AWS publishes whitepapers on security, governance, risk, and compliance; as well as checklists and best practices. Customers can also design and conduct security assessments according to their own preferences, and request permission to conduct scans of their cloud infrastructure, as long as those scans are limited to the customer's compute instances and do not violate the AWS Acceptable Use Policy.

For more details, see the Shared Responsibility Model page.

Building a secure solution on AWS

AWS customers can consider the following best practices when engaging with HMOs. The AWS Well-Architected Framework describes key concepts and provides guidance to help customers apply best practices in the design, delivery, and maintenance of AWS environments.

The security pillar of the AWS Well-Architected Framework encompasses the ability to protect data, systems, and assets to take advantage of cloud technologies to improve your security.

Disclosure or leakage of data mitigations

You need to manage permissions to control access to people and machine identities that require access to AWS and your workload. Permissions control who can access what, and under what conditions.

On AWS, the following practices facilitate access control:

- **Define access requirements.** Each component or resource of your workload needs to be accessed by administrators, end users, or other components. Have a clear definition of who or what should have access to each component and choose the appropriate identity type and method of authentication and authorization.
- **Grant least privilege access.** Grant only the access that identities require by allowing access to specific actions on specific AWS resources under specific conditions. Use groups and identity attributes to dynamically set permissions at scale, rather than defining permissions for individual users. For example, you can allow a group of developers access to manage only resources for their project. This way, when a developer is removed from the group, access for the developer is revoked everywhere that the group was used for access control, without requiring changes to access policies.
- **Establish an emergency access process.** A process that allows emergency access to your workload in the unlikely event of an automated process or pipeline issue. This will help you use least privilege access, but enable users to obtain the right level of access when they require it. For example, you can establish a process for administrators to verify and approve their request.
- **Reduce permissions continuously.** As teams and workloads determine what access they need, remove permissions that they no longer use and establish review processes to achieve least privilege permissions. Continuously monitor and reduce unused identities and permissions.
- **Define permission guardrails for your organization.** Establish common controls that restrict access to identities in your organization. For example, you can restrict access to specific AWS Regions, or prevent your operators from deleting common resources, such as an AWS Identity and Access Management (IAM) role used for your central security team.
- **Manage access based on lifecycle.** Integrate access controls with the operator and application lifecycle and your centralized federation provider. For example, remove a user's access when they leave the organization or change roles.
- **Analyze public and cross-account access.** Continuously monitor findings that highlight public access and cross-account access. Reduce public access and cross-account access to only resources that require this type of access.
- **Share resources securely.** Govern the consumption of shared resources across accounts or within your organization in AWS Organizations. Monitor shared resources and review shared resource access.

For more details, see the Identity and Access Management section of the AWS Well Architected Framework.

Protecting from cross-tenant access in multi-tenant environments

To facilitate multi-tenant architectures, AWS has developed and implemented powerful and flexible logical security controls to create strong isolation boundaries between customers. The AWS logical security capabilities, as well as security controls in place, address the concerns driving physical separation to protect your data. The provided isolation combined with the automation and flexibility added offers a security posture that matches or surpasses the security controls seen in traditional, physically separated environments. For detailed information on logical separation on AWS, see the Logical Separation on AWS whitepaper.

Tenant isolation is one of the fundamental topics that every SaaS provider must address and determine how their multi-tenant environments will prevent tenants from accessing another tenant's resources.

Although the need for tenant isolation is viewed as essential to SaaS providers, the strategies and approaches to achieving this isolation are not universal. There are a wide range of factors that can influence how tenant isolation is realized in a SaaS environment. For detailed information about the different tenant separation strategies and key tenets of the separation, see the Infrastructure Protection section of the AWS Well Architected Framework.

Loss or disruption of data mitigations

Data protection includes the following components:

- **Data classification.** Classification provides a way to categorize data, based on criticality and sensitivity in order to help you determine appropriate protection and retention controls.
- **Data protection at rest.** Protect your data at rest by implementing multiple controls, to reduce the risk of unauthorized access or mishandling.
- **Data protection in transit.** Protect your data in transit by implementing multiple controls to reduce the risk of unauthorized access or loss.

On AWS, the following practices facilitate protection of data:

- As an AWS customer, you retain full control over your data.
- AWS makes it simpler for you to encrypt your data and manage keys, including regular key rotation, which AWS can automate or you can maintain.
- Detailed logging that contains important content, such as file access and changes, is available.

- AWS has designed storage systems for exceptional resiliency. For example, Amazon S3 Standard, S3 Standard–IA, S3 One Zone-IA, and Amazon S3 Glacier are designed to provide 99.999999999% durability of objects over a given year. This durability level corresponds to an average annual expected loss of 0.000000001% of objects.
- Versioning, which can be part of a larger data lifecycle management process, can protect against accidental overwrites, deletes, and similar harm.
- AWS never initiates the movement of data between AWS Regions. Content placed in a Region will remain in that Region unless you explicitly enable a feature or use a service that provides that functionality.

How do you protect your data at rest?

- **Implement secure key management.** Encryption keys must be stored securely, with strict access control—for example, by using a key management service such as AWS KMS. Consider using different keys, and access control to the keys, combined with IAM and resource policies, to align with data classification levels and segregation requirements.
- **Enforce encryption at rest.** Enforce your encryption requirements based on the latest standards and recommendations to help protect your data at rest.
- **Automate protection of data at rest.** Use automated tools to help validate and enforce protection of data at rest—for example, verify that there are only encrypted storage resources.
- **Enforce access control.** Enforce access control with least privileges and other mechanisms, including backups, isolation, and versioning, to help protect your data at rest. Prevent operators from granting public access to your data.
- **Use mechanisms to keep people away from data.** Keep all users away from directly accessing sensitive data and systems under normal operational circumstances. For example, provide a dashboard instead of direct access to a data store to run queries. Where continuous integration and continuous delivery (CI/CD) pipelines are not used, determine which controls and processes are required to adequately provide a break-glass access mechanism that is usually disabled.

How do you protect your data in transit?

- **Implement secure key and certificate management.** Store encryption keys and certificates securely and rotate them at appropriate time intervals while applying strict access control—for example, by using a certificate management service, such as AWS Certificate Manager (ACM).
- **Enforce encryption in transit.** Enforce your defined encryption requirements based on appropriate standards and recommendations to help you meet your organizational, legal, and compliance requirements.

- **Automate detection of unintended data access.** Use tools such as Amazon GuardDuty to automatically detect attempts to move data outside of defined boundaries based on data classification level—for example, to detect a trojan that is copying data to an unknown or untrusted network using the DNS protocol.
- **Authenticate network communications.** Verify the identity of communications by using protocols that support authentication, such as TLS or IPsec.

For more details, see the Data Protection section of the AWS Well Architected Framework.

Network topology planning

Workloads often exist in multiple environments. These include multiple cloud environments (both publicly accessible and private) and possibly data center or hospital infrastructure. Plans must include network considerations such as intra- and inter-system connectivity, public IP address management, private IP address management, and domain name resolution.

- **Use highly available network connectivity for your workload public endpoints.** These endpoints and the routing to them must be highly available. To achieve this, use highly available DNS, content delivery networks (CDNs), API gateways, load balancing, or reverse proxies.
- **Provision redundant connectivity between private networks in the cloud and on-premises environments.** Use multiple AWS Direct Connect connections or VPN tunnels between separately deployed private networks. Use multiple Direct Connect locations for high availability. If you are using multiple Regions, ensure redundancy in at least two of them. You might want to evaluate AWS Marketplace appliances that terminate VPNs. If you use AWS Marketplace appliances, deploy redundant instances for high availability in different Availability Zones.
- **Ensure IP subnet allocation accounts for expansion and availability.** Amazon Virtual Private Cloud (Amazon VPC) IP address ranges must be large enough to accommodate workload requirements, including factoring in future expansion and allocation of IP addresses to subnets across Availability Zones. This includes load balancers, Amazon Elastic Compute Cloud (Amazon EC2) instances, and container-based applications.
- **Use hub-and-spoke topologies over many-to-many mesh.** If more than two network address spaces (for example, VPCs and on-premises networks) are connected through VPC peering, Direct Connect, or VPN, then use a hub-and-spoke model, like that provided by AWS Transit Gateway.
- **Enforce non-overlapping private IP address ranges in all private address spaces where they are connected.** The IP address ranges of each of your VPCs must not overlap when peered or connected by VPN. You must similarly avoid IP address conflicts between a VPC and on-premises environments or with other cloud providers that you use. You must have a way to allocate private IP address ranges when needed.

For more details, see the Network Topology Planning section of the AWS Well Architected Framework.

Distributed denial of service attack

AWS customers can benefit from the automatic protections of AWS Shield Standard at no additional charge. AWS Shield Standard helps defend against the most common and frequently occurring network and transport layer DDoS attacks that target your website or applications. This protection is always on, preconfigured, static, and provides no reporting or analytics. It is offered on all AWS services and in every AWS Region. In AWS Regions, DDoS attacks are detected and the Shield Standard system automatically baselines traffic, identifies anomalies, and, as necessary, creates mitigations. You can use AWS Shield Standard as part of a DDoS-resilient architecture to protect both web and non-web applications.

You can also use AWS services that operate from edge locations, such as Amazon CloudFront, AWS Global Accelerator, and Amazon Route 53 to build availability protection against known infrastructure layer attacks. These services are part of the AWS Global Edge Network and can improve the DDoS resilience of your application when serving application traffic from edge locations distributed around the world. You can run your application in any AWS Region and use these services to help protect your application availability and improve the performance of your application for legitimate end users.

Mitigation techniques and best practices include the following:

- Infrastructure layer defense**.** Make sure that enough capacity and diversity are available, and protect AWS resources, like Amazon EC2 instances, against attack traffic.
- Use load balancers to distribute traffic to a number of EC2 instances that are configured to automatically scale to handle sudden traffic surges due to an application-layer DDoS attack.
- Offload TLS negotiation to CloudFront or to an application load balancer or network load balancer.
- Use both Amazon CloudFront and AWS WAF to help defend against application-layer DDoS attacks.
- Use AWS WAF to filter and block requests based on request signatures on your CloudFront distributions or application load balancers.
- Use AWS Firewall Manager to centrally configure and manage security rules, such as Shield Advanced protections and AWS WAF rules, across your organization.

If you subscribe to AWS Shield Advanced, you can engage the AWS Shield Response Team (SRT) to help you create rules to mitigate an attack that is impacting your application's availability.

For more details, see the AWS Best Practices for DDoS Resiliency whitepaper.

Nimbus agreement

The government of Israel has selected AWS as the primary cloud provider. *Nimbus* is a General Procurement Administrator Agreement (GPAA) between AWS and the government of Israel that was signed in May 2021. Nimbus enables government departments, agencies, and public sector organizations to purchase AWS cloud services at discounted rates on pre-agreed, common contract terms. To support Nimbus customers and other customers who want to host their data locally, AWS is developing an AWS Region in Israel, which will include multiple data centers at three different sites. This Region is expected to launch by mid 2023. In the interim, Nimbus customers can consume AWS services in the Regions specified in Nimbus.

What are the advantages of purchasing AWS services through Nimbus?

Under a normal procurement, you need to define the service that you want to purchase, create a tender document, answer clarification questions, evaluate responses, select a supplier, define and agree to terms and conditions or terms of engagement, and set up a billing and payments process.

Under Nimbus, AWS has been prescreened and approved by the Ministry of Finance. You can access AWS services without having to negotiate separate terms and conditions. Because the government's spending is aggregated, even smaller projects benefit.

In order for an ISV to be part of Nimbus, a subaccount needs to be added in the hospital's Nimbus environment using AWS Control Tower. The ISV should contact the account manager of the healthcare organization. The ISV should open an opportunity through the APN Customer Engagements portal. Enterprise support is provided automatically as part of Nimbus.

How software vendors can use Nimbus

The software vendor needs to contact the healthcare organizations and ask them to create an AWS account under their organization in AWS Organizations. In addition, Nimbus has a private marketplace that allows software vendors to sell their solutions to the Israeli government. To join the AWS Marketplace, contact your AWS account manager for more information.

Regions

AWS data centers are built in clusters in various global regions. We refer to each of our data center clusters in a given country as an AWS Region.

Region selection - where will content be stored?

Customers have access to a number of Regions around the world, including Regions in the EU. Customers can choose to use any combination of Regions.

Planned Region in Israel

The AWS Israel (Tel Aviv) Region is under development and is expected to launch in mid 2023. The Region will have three Availability Zones and will give AWS customers in Israel the ability to run workloads and store data that must remain in-country.

Conclusion

With more than a million active customers and a global cloud presence, AWS has broad experience helping organizations migrate and deploy workloads to the cloud, so that organizations can benefit from IT cost savings, improvements in productivity, business agility, and operational resilience.

This document highlights some common considerations and steps that HCLS companies should follow in order to operate within the Israeli healthcare market. Meeting these requirements set out by the Israeli government can help a healthcare business to successfully deploy its workloads on the AWS Cloud.

Contributors

Contributors to this document include:

- Dima Breydo, Senior Startup Solutions Architect, Amazon Web Services
- Aner Gez, Senior Startup Account Manager, Amazon Web Services
- Adam McCarthy, Europe, Middle East, and Africa (EMEA) Senior Startup Solutions Architect, Amazon Web Services

Document revisions

Date	Description
January 2023	First publication