Cloud Security Strategy

[Insert validity time frame]



Table of contents

[Executive Summary 4](#_Toc69291493)

[Terms and abbreviations 4](#_Toc69291494)

[1 Business objectives 5](#_Toc69291495)

[1.1 Vision 5](#_Toc69291496)

[1.2 Motivation and benefits 5](#_Toc69291497)

[2 External drivers 5](#_Toc69291498)

[2.1 Legal obligations 5](#_Toc69291499)

[2.2 Data protection 6](#_Toc69291500)

[2.3 Changes in the IT industry 6](#_Toc69291501)

[2.4 Cybersecurity resilience 6](#_Toc69291502)

[3 Organizational impact 6](#_Toc69291503)

[3.1 Cloud Center of Excellence (CCOE) 7](#_Toc69291504)

[4 Risk 7](#_Toc69291505)

[5 Cloud adoption principles 8](#_Toc69291506)

[5.1 Application migration 8](#_Toc69291507)

[5.2 Security architecture 8](#_Toc69291508)

[5.3 Cloud service models 8](#_Toc69291509)

[5.4 Cloud provider selection 9](#_Toc69291510)

[5.5 Hybrid networking 9](#_Toc69291511)

[5.6 Data classification 9](#_Toc69291512)

[6 Goals 9](#_Toc69291513)

[6.1 Target Cloud Security Architecture 9](#_Toc69291514)

[6.2 Cloud Foundation 9](#_Toc69291515)

[6.3 Security initiatives 10](#_Toc69291516)

[6.4 Communication platform 10](#_Toc69291517)

[6.5 Research and analysis 10](#_Toc69291518)

[6.6 Development environments 10](#_Toc69291519)

[6.7 Clinical solutions 10](#_Toc69291520)

[APPENDIX A 11](#_Toc69291521)

[Definition of cloud computing 11](#_Toc69291522)

[Cloud service models 11](#_Toc69291523)

[Cloud deployment models 11](#_Toc69291524)

[Cloud shared responsibility model 12](#_Toc69291525)

[References 13](#_Toc69291526)

| Version | Date | Change comments | Author | Approved |
| --- | --- | --- | --- | --- |
| 0.1 | 01.01.2021 | First edition | Lead architect | CEO |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Executive Summary

*[Create a summary of all the important aspects throughout the remainder of the cloud security strategy document. Share this section with the executive team to communicate the essence of your cloud security strategy. The text below is just an example, and it must be customized based on your specific context.]*

This document defines the health sector cloud security strategy. In the health sectors business plan for 2019 – 2023, important objectives are communication across health entities, exchange of health information and patient communications. These objectives can be met utilizing cloud based services compliant with the health sector regulations.

The health sector must become a modern provider of IT services to the clinical institutions throughout the nation and must therefore adapt to the market and the need to be able to deliver services faster and in new ways. At the same time, the threat landscape is changing and more resources and competencies are needed to stay secure and compliant in the cloud.

To deliver cloud services to clinics in the health sector a solid security architecture is necessary to protect sensitive data across all services. A hybrid cloud deployment model is preferred along with a focus on SaaS and PaaS service models. Operations in the cloud will need a CCOE who can centralize and automate tasks and stay updated on the latest technology trends.

The health sectors strategy for using cloud services follows these principles:

* Cost efficiency
* Flexibility and capacity
* Quality
* Security

## Terms and abbreviations

|  |  |
| --- | --- |
| **Term** | **Description** |
| SaaS | Software As A Service  |
| PaaS | Platform As A Service  |
| IaaS | Infrastructure As A Service  |
| CSA CCM | Cloud Security Alliance Cloud Controls Matrix |
| GDPR | General Data Protection Regulation |
| PHI | Protected Health Information |
| NIST CSF | National Institute of Standards and Technology Cybersecurity Framework |
| IaC | Infrastructure as Code |
| DevOps | DevOps is a set of practices that combines software development (Dev) and IT operations (Ops). |
| CCOE | Cloud Center Of Excellence |
| SOC | Security Operations Center |

# Business objectives

*[Share your vision with your stakeholders and communicate the objectives behind the cloud security strategy to the organization. In this section, you must describe the vision, goals and benefits for your strategy. The text below is just an example, and it must be customized based on your specific context.]*

## Vision

The health sector shall, through the appropriate use of cloud services, ensure the availability, quality and security of the services, so that the sector and the needs of the clinics are supported as efficiently as possible and at the lowest possible cost. The health sector will also facilitate the use of relevant services that are available as cloud services only.

## Motivation and benefits

Cloud services [1] is a collective term for everything from data processing and data storage to software on servers available from external datacenters connected to the Internet. The datacenters are typically established to offer dynamic scaling so that computing power can be offered to the customer as needed. The customer only pays for the use of the capacity consumed in the cloud.

Motivation for using cloud services:

* Expanded capacity and scalability for health sector services
* Faster deliveries of new services to patient groups
* Manage communication across user groups more securely
* Lower cost for temporary use
* Be able to use services that are only delivered in the cloud
* Improve the security posture for clinics

# External drivers

*[External drivers will influence your strategy and must be taken into account when prioritizing the strategy goals. In this section, you must describe all external obligations and expectancies that may have an impact on your strategy. The text below is just an example, and it must be customized based on your specific context. ]*

## Legal obligations

All entities in the health sector must comply with regulations, such as HIPAA [2]. There are three components of HIPAA security rule compliance. Keeping patient data safe requires healthcare organizations to exercise best practices in three areas: administrative, physical security, and technical security. Operating services provided by external providers, such as cloud services, must satisfy the requirements of the relevant regulations.

The European Privacy Regulation, General Data Protection Regulation (GDPR) [3] is the current European law. The regulation applies throughout the EU and the EEA area and is intended to give citizens greater control over their own personal data. The rules include provisions on built-in privacy, which implies that privacy is built into services and solutions from the earliest phase of development. It is important that applications hosted in the cloud are compliant with this regulation.

## Data protection

Regulations such as HIPAA requires the health sector entities to stay compliant. Even when compliant it does not mean that patients PHI is secure. Implementing information security in the cloud is a vast undertaking and requires effort in many areas within organization, legal and technical. The NIST CSF [4], developed by NIST as a non-regulatory federal agency, provides a cohesive framework to implement a comprehensive security program. By actively using NIST CSF and other frameworks, the sector can stay compliant and help clinics protect sensitive data.

## Changes in the IT industry

The IT industry is changing rapidly and operations are often centralized and moved to large cloud service providers. This also applies to IT system vendors and services provided to the health sector. The health sector needs a clear strategy for handling requirements for vendors that offer cloud services. Clinics also need to adapt operations so that operations in local data centers can coexist with operations externally in various forms of cloud services.

## Cybersecurity resilience

The strategy must go beyond attack prevention and enable rapid attack detection, response, and recovery to increase resilience. Organizations in the health sector must assume that attackers will compromise some resources and work to ensure that resources and technical designs are balanced between attack prevention and attack management.
The NIST CSF will serve as a useful guide on how to balance investments between the complementary activities of identify, protect, detect, respond, and recover in a resilient strategy for cloud services in the health sector.

# Organizational impact

*[Describe the impact the use of cloud services will have on your organization. You must outline which organizational changes will be needed to support the strategy. The text below is just an example, and it must be customized based on your specific context. ]*

The health sector must change the way it operates IT to be able to deliver value to the clinics within the sector. Operating in the cloud requires organizational transformation and acquisition of new knowledge. The use of cloud services will enable self-service for many user groups. Allowing autonomous user groups will benefit innovation and enable fast-paced projects to deliver more value to the users. The IT organizations in the health sector must establish a governance model that can give guidelines and guardrails for IT users in the sector to avoid risky use of cloud services.

To be able to scale the operation for cloud services the principles of standardization, centralization and automation applies to all services.

## Cloud Center of Excellence (CCOE)

The strategy for governing cloud services is based on creating a virtual team, as this will benefit collaboration across professional groups and organizational units. A CCOE is the preferred short-term model.

Further growth in the use of cloud services will give organizations in the health sector the necessary experience to determine what type of organizational model that will work best over time.

# Risk

*[Insert your own risks from the risk analysis conducted in your organization. List multiple potential mitigation strategies for each risk, this will help reducing the overall risk. These mitigation strategies should be reflected in your strategy goals under security initiatives. The text below is just an example, and it must be customized based on your specific context. ]*

A risk analysis has been carried out in collaboration with all stakeholders. The following risks related to adoption of cloud based services have been identified. The table below summarize the most important risk elements along with possible mitigation strategies.

|  |  |
| --- | --- |
| **Risk Description** | **Mitigation Strategy** |
| Resistance to the use of cloud services within the organization | Seek executive sponsorship and educate personnel on the use of cloud services |
| Vendor lock-in. Relying strongly on the services of one provider can lead to severe difficulties in changing the provider.  | Use IaaS or PaaS services applying open standardsCreate an exit strategy for migrating to a different cloud provider |
| Lack of relevant skills  | Build an internal training program to develop the required skill setHire consultants temporarily and seek help from cloud experts in the cloud provider organization |
| Loss of Governance. When using Cloud services, the Cloud Consumer necessarily cedes control to the Cloud Provider on a number of issues which may affect security. | Scrutinize compliance reports from third-party auditorsApply best practices for governance and monitoring of the environment |
| Cloud providers may change their terms in our disfavor or raise their prices | Develop a multicloud strategy with a focus on exit from one provider and migration to another |
| Cloud service misconfiguration leads to successful attacks and exposure of sensitive data | Develop a holistic security architecture and governance modelDevelop internal cloud security competencies |
| The customer management interfaces of public cloud providers are Internet accessible and mediate access to larger sets of resources and therefore pose an increased risk especially when combined with remote access and web browser vulnerabilities | Apply multi-factor authentication on all accounts having administrative privileges.Create a least privilege authorization schemeEncrypt all traffic to the cloud environment. |
| Some parts of the organization can overspend in certain cloud services | Create good governance processes for public cloud usageAssign and enforce budget limits for all user groupsApply policies restricting the use of expensive services |

# Cloud adoption principles

*[Provide information on the core decisions that will set a direction for your use of cloud services. List five to 10 key decisions and principles that will govern them as you move into implementation. In this section, you must describe the vision, goals and benefits for your strategy. The text below is just an example, and it must be customized based on your specific context. ]*

## Application migration

The health sector will only migrate applications that are re-architected to cloud native applications.

## Security architecture

The security architecture will follow a Zero Trust [5] approach guarding sensitive data in compliance with health regulations

## Cloud service models

The priority of the chosen cloud service models is as follows:

1. SaaS
2. PaaS
3. IaaS (only when SaaS and PaaS cannot meet the requirements)

## Cloud provider selection

Microsoft Azure is the preferred provider for the health sector. However, any cloud provider can be chosen if the business requirements are not met using the available services in Azure.

## Hybrid networking

The network architecture will make a hybrid infrastructure available to the users. A secure private connection from on-premises to the cloud will protect traffic to and from the cloud service provider’s datacenter.

## Data classification

Before any data is uploaded to the cloud services it must be classified, labeled and protected according to its classification.

# Goals

*[State the goals for your cloud security strategy. These goals must be the highest prioritized initiatives to fulfill your strategy objectives. The text below is just an example, and it must be customized based on your specific context. ]*

The goals in the strategy, as listed below, are aligned with the business plan. Stakeholders from multiple organizations within the health sectors have given input to the strategy goals and priorities.

## Target Cloud Security Architecture

A holistic architecture must be created including principles, criteria and requirements for the choice and use of cloud solutions in the health sector. Principles applies to how services are organized, designed, secured and delivered. It must be stated how different delivery models should be organized and integrated into the total service offering, information management and application architecture.

The architecture will be based on the following security principles:

* Completeness of design
* Layered defense
* Separation of privilege
* Least privilege
* Isolation
* Zero trust
* Security by design

[Read more about security architecture here: [What is information security architecture? - Cloud Security Architecture (cloudsarc.org)](https://www.cloudsarc.org/2021/03/30/what-is-information-security-architecture/)]

## Cloud Foundation

A Cloud Foundation framework must be established before services are offered to end-users. The Cloud Foundation framework requires the following:

* Identity management and governance model established for cloud services
* Security requirements for cloud services specified
* Economy model established
* New management model prepared
* Organizational changes implemented

## Security initiatives

The following security initiatives must be completed before cloud services are deployed:

* The chosen cloud provider’s security practices following the shared responsibilities model (as described in Appendix A) and the CSA CCM are verified
* Infrastructure and application security are modernized and cloud native by using IaC and DevOps
* A modern perimeter using centrally managed identity controls to protect data, devices and accounts is established
* A SOC covering detection and response for cloud security incidents is created
* Other security measures from the risk analysis in chapter 4:
	+ Investigate cloud provider IaaS and PaaS services for portability
	+ Enforce policies for multifactor authentication
	+ Enforce least privilege for authorization of personnel
	+ Encrypt all traffic to the cloud environment
	+ Develop internal cloud security competencies

## Communication platform

The communication platform for the health sector can provided when the following sub-goals are met:

* Security and management model for the communication platform specified
* Governance is established for the communication platform

## Research and analysis

Using cloud services for research and analysis has a big potential and is a priority within the health sector. These sub-goals must be met before the launch of services to research communities:

* Security architecture prepared for research and analysis
* Analysis and machine learning framework established in the cloud

## Development environments

Developers need a hybrid deployment model to utilize the cloud for development of new healthcare solutions. The following must be completed:

* Architecture, security and management model prepared for PaaS / IaaS
* Cloud solutions are part of the hybrid infrastructure for development in the health sector

## Clinical solutions

Clinical solutions offered to patients is an important goal in the strategy but requires data protection and compliance. Architectural work needs to be completed before services are developed and deployed.

* Architecture, security and management model are prepared for clinical solutions
* Platform for virtual health services established as a cloud service

# APPENDIX A

## Definition of cloud computing

NISTs definition of cloud computing [1]:

«Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.»

Source: NIST SP 800-145

## Cloud service models

* **Infrastructure as a service (IaaS).** IaaS is a standardized, highly automated service offering in which computing resources are always owned by a service provider. The service includes storage and networking capabilities that are offered to customers on demand. Resources are scalable and elastic and metered by use. Self-service interfaces, including an API and a graphical user interface (GUI), are exposed to customers.
* **Platform as a service (PaaS).** A PaaS is a collection of application infrastructure services such as application platform, integration, business process management and database services. You, as a cloud customer, develop your own applications and deploy them on top of the PaaS offering. Examples of PaaS offerings include Microsoft Azure, IBM Cloud, Heroku and OpenShift.
* **Software as a Service (SaaS).** Software offered to the customer directly over the internet. The cloud provider owns the software in its entirety. The service is delivered and managed remotely by one or more providers. The provider delivers software based on common code that is consumed in a one-to-many model by all contracted customers at any time on a pay-for-use basis or as a subscription based on use metrics. Examples of SaaS offerings include Microsoft Office 365, Google Apps and Salesforce

## Cloud deployment models

Cloud services can be divided into deployment models such as:

* **Public Cloud**
The public cloud deployment model supports all users who want to make use of a computing resource, such as hardware (OS, CPU, memory, storage) or software (application server, database) on a subscription basis.
* **Private Cloud**
A private cloud is typically infrastructure used by a single organization. Such infrastructure may be managed by the organization itself to support various user groups, or it could be managed by a service provider that handles operations either on-site or off-site. Private clouds are more expensive than public clouds due to the capital expenditure involved in acquiring and maintaining them.
* **Hybrid cloud**
Hybrid cloud can be a mixture of the models above where a combination of operation in the company's own data center and public cloud is most common.
* **Community cloud**
This deployment model supports multiple organizations sharing computing resources that are part of a community. Access to a community cloud environment is typically restricted to the members of the community.

## Cloud shared responsibility model

A significant amount of security configuration, implementation and attack surface defense is the responsibility of the cloud customer. The time and resources needed to invest for each cloud deployment should not be underestimated, including any necessary training to bring your team up to speed.



**IaaS**: In this tier, the security burden on the cloud service provider (CSP) includes virtualization security and infrastructure security. Areas such as data security, application security, middleware security and host security fall to the IaaS customer. Simply put: users are responsible for the guest OS and everything inside of it.

**PaaS**: In this tier, the CSP’s responsibilities are broader, including security configuration, management, operating monitoring, and emergency response of infrastructure; security of virtual networks; security of the platform layer, such as the security of operating systems and databases; and security of application systems. The PaaS customer is responsible for data security and application security.

**SaaS**: In this tier, the CSP is responsible for security of the application and underlying components. The SaaS customer is responsible for data security and endpoint device protection.

# References

|  |  |
| --- | --- |
| [1]  | National Institute of Standards and Technology, "The NIST Definition of Cloud 800-145," September 2011. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf. |
| [2]  | U. D. o. H. &. H. Services, "Health Insurance Accountability and Portability Act," [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/index.html. |
| [3]  | E. Union, "General Data Protection Regulation," [Online]. Available: https://gdpr-info.eu/. |
| [4]  | N. I. o. S. a. Technology, "NIST CYBERSECURITY FRAMEWORK," [Online]. Available: https://www.nist.gov/cyberframework. |
| [5]  | N. I. o. S. a. Technology, "Zero Trust Architecture," [Online]. Available: https://www.nist.gov/publications/zero-trust-architecture. |