Cloud Security Strategy

[Insert validity time frame]



Table of contents

[Executive Summary 4](#_Toc81312501)

[Terms and abbreviations 4](#_Toc81312502)

[1 Business objectives 5](#_Toc81312503)

[1.1 Vision 5](#_Toc81312504)

[1.2 Motivation and benefits 5](#_Toc81312505)

[2 External drivers 6](#_Toc81312506)

[2.1 Regulatory obligations 6](#_Toc81312507)

[2.2 Data protection 6](#_Toc81312508)

[2.3 Changes in the IT industry 6](#_Toc81312509)

[2.4 Cybersecurity resilience 6](#_Toc81312510)

[3 Organizational impact 7](#_Toc81312511)

[3.1 Cloud Center of Excellence (CCOE) 7](#_Toc81312512)

[4 Risk 7](#_Toc81312513)

[5 Cloud adoption principles 8](#_Toc81312514)

[5.1 Application migration 8](#_Toc81312515)

[5.2 Security architecture 9](#_Toc81312516)

[5.3 Cloud service models 9](#_Toc81312517)

[5.4 Cloud provider selection 9](#_Toc81312518)

[5.5 Data classification 9](#_Toc81312519)

[5.6 Cloud operations 9](#_Toc81312520)

[6 Goals 9](#_Toc81312521)

[6.1 Target Cloud Security Architecture 9](#_Toc81312522)

[6.2 Cloud Foundation 10](#_Toc81312523)

[6.3 Security initiatives 10](#_Toc81312524)

[6.4 EMR system 10](#_Toc81312525)

[6.5 Development environments 11](#_Toc81312526)

[6.6 Clinical solutions 11](#_Toc81312527)

[APPENDIX A 12](#_Toc81312528)

[Definition of cloud computing 12](#_Toc81312529)

[Cloud service models 12](#_Toc81312530)

[Cloud deployment models 12](#_Toc81312531)

[Cloud shared responsibility model 13](#_Toc81312532)

[References 14](#_Toc81312533)

| 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 Cloudsarc Health Clinic cloud security strategy. In the health clinics business plan for 2019 – 2023, important objectives are efficient patient communication, exchange of health information and agility to meet new business requirements. These objectives can be met utilizing cloud based services compliant with the health sector regulations.

The health clinic must become a modern provider of IT services to meet new requirements for communication and innovative service delivery 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 the health clinic, a solid security architecture is necessary to protect sensitive data across all services. A public cloud deployment model is preferred along with a focus on SaaS and PaaS service delivery models. Operations in the cloud will need a Cloud Center Of Excellence (CCOE) who can centralize and automate tasks and stay updated on the latest technology trends.

The health clinics 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.]*

The Cloudsarc Health Clinic has the following high-level business objectives:

* High quality patient treatment
* Patient information confidentiality
* Patient record availability
* Patient data integrity
* EMR operations cost efficiency
* Secure and reliable communications
* Cyber resilience

## Vision

The health clinic shall, through the appropriate use of cloud services, ensure the availability, quality and security of the services, so that the clinics and patients’ needs are supported as efficiently as possible and at the lowest possible cost. The health clinic 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 clinic 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 the clinic

# 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. ]*

## Regulatory 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 clinic needs a clear strategy for handling requirements for vendors that offer 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 for the health clinic.

# 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 clinic must change the way it operates IT to be able to deliver value more rapidly to clinicians and patients. 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 when the clinics organization grows in size. Allowing autonomous user groups will benefit innovation and enable fast-paced projects to deliver more value to the users. The IT organization in the health clinic must establish a governance model that can give guidelines and guardrails for all IT users in the clinic 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 the health clinic organization 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 EMR system have been identified. The table below summarize the most important risk elements along with possible mitigation strategies.

|  |  |  |
| --- | --- | --- |
| **Risk #** | **Risk Scenario** | **Mitigation Strategy** |
| Ri1 | Sophisticated attackers or malicious insiders can steal, modify or delete PHI due to misconfiguration of cloud security settings | Solid understanding of usage scenarios and risk. Protective measures for data, user access and focus on change management. Broad detection capabilities and a verified recovery process. |
| Ri2 | Sophisticated attackers can render data unavailable and by installing ransomware. PHI can be lost because a recovery plan has not been created. | Create a good recovery plan with focus on fast recovery time and establish good communications with the stakeholders |
| Ri3 | Sophisticated attackers and exploit insecure APIs and steal, modify or delete PHI. | Solid understanding of usage scenarios and risk. Protective measures for data, user access and focus on change management. |
| Ri4 | Sophisticated attackers could hijack a user account and steal, modify or delete PHI | Solid understanding of usage scenarios and risk. Protective measures for data, user access and user device management. |
| Ri5 | Due to lack of segregation of responsibilities a malicious insider can read PHI for some patients | Establish a good identity management strategy with focus on access management and separation of duties. |
| Ri6 | Sophisticated attackers can steal, modify or delete PHI due to inadequate security monitoring for detecting suspicious and unauthorized activities. | Solid understanding of usage scenarios and risk. Broad detection capabilities and a competent operations team. |
| Ri7 | Sophisticated attackers can steal, modify or delete PHI by continuing attacks and hiding evidence because logs are not collected and aggregated in a central location | Solid understanding of usage scenarios and risk. Broad detection and analysis capabilities and a competent operations team.Aggregation and protection of logs from unauthorized access. |
| Ri8 | Sophisticated attackers can render data unavailable and by installing ransomware. PHI can be lost because an incident response plan has not been tested. | Solid understanding of usage scenarios and risk. Broad detection capabilities and a verified backup and recovery process |

From these risk mitigation strategies, we can derive some common success factors for the implementation of cloud security:

* Automation of security configuration in environments and for detection and response
* Strong authentication for all users, devices and applications
* Isolation of environment and fine grained access control
* Focus on protection of PHI

# 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. The text below is just an example, and it must be customized based on your specific context. ]*

## Application migration

The health clinic 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 clinic. However, any cloud provider can be chosen if the business requirements are not met using the available services in Azure.

## Data classification

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

## Cloud operations

The principles of standardization, centralization and automation applies to all services. No services in the cloud can be based on manual operations procedures.

# 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 the health clinic 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 for the health clinic. 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 duties
* Least privilege
* Isolation
* Zero trust
* Security by design

## 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

## EMR system

The EMR system for the health clinic can be provided when the following sub-goals are met:

* Governance model for the cloud environment specified
* Governance is established for the EMR system
* All risk mitigation measures are implemented and verified
* The EMR system is testet and approved

## Development environments

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

* Architecture, security and management model prepared for PaaS / IaaS
* A solid DevOps process with focus on security

## 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. |