Information Security Policy, version 1.0.0

Status: ☐ Working Draft ☒ Approved ☐ Adopted
Document Owner: Ali Clinic Executive Management
Last Review Date: December 2023

Information Security Policy

Introduction

The information security policy of Ali Clinic is a comprehensive framework designed to ensure the utmost protection of sensitive patient data and the integrity of our IT infrastructure. This policy is a cornerstone of our commitment to maintaining the highest standards of data security and privacy, in compliance with healthcare regulations such as HIPAA and HITRUST. It reflects our dedication to safeguarding our digital assets against the ever-evolving landscape of cyber threats.

Purpose

The policy aims to protect patient information and ensure compliance with legal standards.

Audience

The policy is applicable to employees, contractors, and affiliated personnel of Ali Clinic. It governs the conduct of anyone who interacts with our IT systems and handles patient data, emphasizing their roles and responsibilities in upholding our security standards. The policy also extends to our partners and vendors, ensuring that all stakeholders are aligned with our security objectives and practices.

Responsibilities

IT Staff

- Maintain and manage security infrastructure.
- Conduct regular system updates and patches.
- Monitor network for any unusual activity.
- Respond to and resolve security incidents.

Executive Management

- Ensure availability of resources for Ali Clinic that meet it’s cybersecurity initiatives and standards.
- Foster a culture of security awareness.
- Make key decisions on cybersecurity strategies.
- Oversee compliance with relevant regulations.

All Employees, Contractors, and Other Third-Party Personnel

- Adhere to security protocols and procedures.
- Report suspicious activities or security breaches.
- Participate in security training and awareness programs.
- Maintain confidentiality of sensitive information.

Policy

- The information security policy for Ali Clinic is designed to safeguard sensitive patient data and the clinic's IT infrastructure. The policy serves to ensure compliance with healthcare regulatory and legal requirements, along with using well-known and established frameworks. These regulations and standards mandate strict confidentiality, integrity, and availability of patient health information, requiring robust security measures and practices to protect against data breaches and unauthorized access. The regulations and standards are listed below.
    - HIPAA Security Rule,
    - HITRUST
    - State breach notification laws,
    - Information Security best practices, including ISO 27001 and NIST SP 800-53,
    - Contractual agreements,
    - All other applicable federal and state laws or regulations.
- The information security policy is reviewed annually. This regular review process ensures the policy remains up-to-date with evolving security threats, technological advancements, and changes in healthcare regulations. This helps in maintaining the integrity and confidentiality of patient data and remains in compliance with standards like HIPAA and HITRUST.

References

- ISO 27001
- NIST SP 800-53
- HIPAA Security Rule
- HITRUST

Enforcement

Any breaches or non-compliance with the policy will result in appropriate disciplinary action, which include reprimands, suspension, termination of employment, or legal actions, depending on the severity of the breach. This strict enforcement ensures that all staff, contractors, and affiliated personnel understand the importance of the policy and maintain the highest standards of data security and privacy.

Version History

Version	Modified Date	Approved Date	Approved By	Reason/Comments
1.0.0	December 2023		Ali Clinic	Document Creation