HIPAA Compliance Statement

The **Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) Act** defines policies, procedures, and processes that are required for companies that store, process, or handle electronic protected health information (ePHI).

At Saphetor, we take our responsiblities towards customer & patient confidentiality very seriously and have dedicated both resources and time to train our workforce and develop and implement all of the components of our HIPAA Compliance Program.

To ensure we are compliant with HIPAA and HITECH Act, ensure that we have the required safeguards in place to protect ePHI, and demonstrate HIPAA compliance to our clients:

- Saphetor have developed and implemented a comprehensive HIPAA Compliance Program following the HIPAA Privacy and HIPAA Security Rule – focusing on the administrative, physical and technical requirements of the HIPAA Security Rule as it applies to any potential risk associated with the use of PHI in our business.
- Saphetor have a designated HIPAA Privacy and Security Compliance Officer
- Saphetor have provided every member of our staff which also includes new hires, annual training.
- Saphetor have a formal established Employee Sanctions Policy should any HIPAA compliance violations occur.
- Saphetor ensure technological protocols such as: tight access controls, integrity procedures, firewalls, information systems activity monitoring and other audit mechanisms to record access in information systems that use ePHI, use of encryption, automatic logoffs, password management procedures, and VPN tunnel.
- Saphetor have conducted a formal risk assessment to identify and document any area of risk associated with the storage, transmission, and processing of ePHI and have analyzed the use of our administrative, physical, and technical controls to eliminate or manage vulnerabilities that could be exploited by internal or external threats.
- Saphetor have limited access to ePHI.

We are Dedicated to:

- Ensuring we are compliant with the regulatory requirements of HIPAA/HITECH
- Continuing to develop our safeguards to prevent unauthorized access to PHI.
- Adhering to the requirement to encrypt PHI
- Maintaining PHI in a secure environment
- Monitoring access to both the secure environment and the data

Our HIPAA policies include, but are not limited to, the following key areas:

- Security Management Policy
    - Risk Analysis Policy
    - Risk Management Policy
- HIPAA Compliance Officer Job Description
- Workforce Security Policy
    - Authorization and Supervision of Staff Procedure
    - Workforce ePHI Access Authorization Procedure
    - Termination Procedure
    - Business Associate Policy
- Information Access Management
    - Access to ePHI Modification
- Security Awareness Training
    - Security Training
    - Password Management
    - Oral Disclosures of PHI
- Security Incident Procedures
    - Incident Investigation Procedure
- Contingency Plan
    - Backup Plan
    - Disaster Recovery Plan
    - Emergency Mode Operation
    - Applications and Criticality Analysis
- Evaluation of the HIPAA policies and procedures
- Business Associates
- Physical Safeguards Standards and Policy
- Workstation Use
- Device and Media Controls
    - Disposal of ePHI
    - Media Re-Use
    - Accountability
    - Data Backup and Storage
- Technical Safeguards Standards Policy
    - Access Control
        - Unique User Identification
        - Emergency Access Procedure
        - Automatic Logoff

        - Encryption
        - Antivirus and Firewalls
        - VPN Protocol
        - Additional Safeguards Employed
    - Audit Controls
    - Sanctions Policy

We are Confident that Our Comprehensive HIPAA Policies and Procedures Will:

- Ensure the confidentiality, integrity, and availability of all e-PHI we receive, maintain or transmit
- Identify and protect against reasonably anticipated threats to the security or integrity of the information
- Protect against reasonably anticipated, impermissible uses or disclosures
- Ensure compliance of our workforce.

This Compliance Statement is valid from: 30.11.2019

Stelios Voutsadakis, QAM

This document is electronically signed by Stelios Voutsadakis according to the provision of our Quality Management Systea