# HIPAA Privacy and Security Policy and Procedures

I. Assignment of HIPAA Privacy/Security Officer

Mr. Yossi Shteingart (MCSE), has been designated as our HIPAA Officer by the CEO and has authority to establish, implement, and enforce these policies and procedures for the security and privacy of our patients protected health information (PHI).

II. Risk Assessment

HIPAA Officer is responsible for conducting annual HIPAA privacy and security risk assessment. The assessment will be completed with the assistance of at least two other employees.

Additional risk assessments may be necessary each time (1) new software or hardware is acquired and placed in service; (2) when a new service or procedure is initiated; (3) when there is a significant change in an existing service or procedure; or (4) when there is a change or addition to the physical layout of our office.

The HIPAA Officer will periodically but at least quarterly review the DHHS's HIPAA website to determine if there have been any changes in the HIPAA rules and regulations and to determine if any changes or modifications to this policy and procedure is necessary due to changes in HIPAA rules, regulations or regulatory interpretations.

III. Policy regarding physical access to building

Employees access our office via main entrance to building and then our offices. Main entrance to building is manned 24/7 by an armed guard. The office entrance is locked after hours and is also manned 24/7 by an employee of the NOC. Entrance to the office by employees is via a Biometric entry system.

NOC employee has the key to entrance and is responsible for unlocking main entrance each morning. Employee entrance is accessed only via the Biometric system. Employees or service personal may gain entrance through the employee entrance by ringing the entrance bell which rings into the office manager and if no answer routes to the NOC center.

IV. Policy regarding confidentiality of all forms of PHI

All PHI regardless of its form, mechanism of transmission, or storage is to be kept confidential. Only individuals with a business need to know are allowed to view, read, or discuss any part of a patient's PHI. During initial new hire orientation and at annual HIPAA training employees are reminded that any viewing, reading, or discussions of PHI that is not for business purposes is prohibited. An employee who violates this confidentiality policy will be subject to sanctions up to immediate termination. All new employees are required to verify in writing that they have read and will comply with our policy regarding confidentiality of all forms of PHI.

V. Policy regarding Security of electronic PHI (e-PHI)

Employees whose job functions require access to our computer system will be given a secure, unique password to access the system. Passwords will consist of at least five characters, upper and lower case, alpha numeric and shall be changed at least every 90 days.

Access will be immediately terminated for employees who leave our employment.

All PHI transmitted to third parties will be transmitted on secured lines. The security of transmission lines will be verified via contract with third party responsible for transmitting our patient's PHI.

No digitally stored PHI shall leave this facility without being first encrypted; this includes laptops, flash drive devices, CDs, and e-mail.

VI. Patient request for accounting of all disclosures made by TeleMessage

Patients have a right to request an accounting of all disclosures of their PHI made by TeleMessage. When a patient makes such a request, Yossi Shteingart will be notified. The patient will be told when the information will be available and given the option of waiting or returning to pick-up the data.

VII. Patient request for restriction of PHI paid for "out of pocket"

Patients who pay for a service out of pocket (fully paid for by patient with no reimbursement or additional payment by a third party), have a right to have all information regarding such procedure/test held confidentially and not released to

third parties. To exercise this right the patient must (1) pay for test/procedure and (2) make known to TeleMessage their desire to have information regarding the procedure/test held in confidence and not released to third parties. Any employee who receives such a request must immediately inform Yossi Shteingart who will flag the information as being restricted. HIPAA allows for the release of restricted PHI (1) in compliance to a subpoena; (2) in compliance to statutory reporting requirement; or (3) upon receiving an unrestricted, HIPAA compliant authorization for release of medical records from the patient, patient's legal representative, or executor of deceased patient's estate.

## VIII. Business continuity

TeleMessage is strongly committed to deliver a secure and reliable service 365 days a year 24 hours a day

TeleMessage takes all the necessary actions in order to maintenance an operational disruption free service, never the less it should taken into account that the message flow is passing routes outside TeleMessage control.
The DRP / BCP plan makes sure TeleMessage infrastructure is robust and failsafe but a redundant path for the customers SMSC's with a proper configured routing rules on the customer location is required in order to achieve a fully redundant and failsafe paths.

Structure elements redundancy

Datacenter:
The service is distributed across 2 separate datacenters. Each datacenter supports 75% of the peak capacity. Both datacenters provide Physical security measurements 24x7, Redundant 24x7 power supply, Redundant, low latency back bone Internet links, On site 24x7 NOC staff to attend urgent hand in cage and network related incident within the hosting facility. Both sites are interconnect on a reliable network connect.

Sites are working in Active/Active scheme excluding the Oracle database which works in an Active/Passive scheme.

Hardware:
All hardware is fully redundant on each site separately. Every role executed on 2 servers per site. Hardware failure resilience is achieved by the following measurements. Dual power supply on all servers. Various RAID levels to ensure no single disk failure will degrade the server or service.

Network links:
Servers have dual NIC's, each connected to a different network switch. 2

physical network switch per subnet. Clustered firewall to maintain uplink uptime. Database on protected storage with hot and cold backups. Recovery time is up to 4 hours in case of a cold backup recovery.

Database:

The Oracle HA architecture TeleMessage use is Data Guard. The primary site contains a production database while the secondary site contains one or more read only standby databases. In case of a failure on the primary site failure or primary site database failure, TeleMessage engineers will divert the system to use secondary standby database.

NOC:
TeleMessage has a trained NOC staff (TeleMessage Control Center). The NOC is being populated 24 hours a day, 365 days a year. NOC responsibilities are:
Monitor the service statistic information to determine meeting customer SLA.
Actively run tests on a per-defined intervals and message flow. Manage and escalate service degradation, disruption or failure. 24x7 customer emergency support line.
TeleMessage NOC has a 24x7 engineer on duty at their disposal that can be reached at all time for escalations scenarios beyond the NOC scope.

## X. HIPAA Incident/Breach Investigation

Any incident in which the privacy/security of a patient's PHI may have been compromised will be immediately reported to Guy Levit, CEO. An incident investigation will be initiated without unreasonable delay. The HIPAA Officer will establish an Incident Response Team (IRT) to investigate incidents and determine if the incident rises to the level of a breach.

## XI. Sanction Policy

All employees will receive training regarding TeleMessage's policy for sanctioning employees who violate our HIPAA privacy/security policy. Employees shall receive training prior to assuming work duties and annually thereafter.

## XII. Document Retention Policy

All HIPAA documentation such as policy and procedures, risk assessment, incident investigation, breach notification, and training records will be maintained for at least six years in the HIPAA records and documentation section of this policy.