Ministry of Health

General Manager Circular

This is an unofficial translation of the Circular.

In any discrepancies or inaccuracy between the English version and the Hebrew Version – the Hebrew version shall apply

February 21st, 2021
Number: 2/2021

Subject: Use of Cloud Computing in the Israeli Healthcare System

1. Background

In recent years, the trend of transitioning to utilizing cloud services in many industries is increasing worldwide. Cloud technology is an important component in bringing in innovation to the organization. It enables the organization to have an operational flexibility and the capability to effectively maximize the use of the computing resources available to it, as well as costs saving in operating these services in the organization. In addition, cloud technology can assist health care organizations develop advanced operational and research capabilities, and enhance digital health in the healthcare system, as well as implement innovative solutions, many of which currently operate only in the cloud.

Operating applications through cloud computing has to be done in an intelligent and balanced way. Thus, the current regulation seeks to enable healthcare organizations to use tools and devices that if properly applied, can assist them meet the compliance requirements applicable to them by the provisions of the Privacy Protection Law and other information security and cyber security Standards, and deal with risks related to information security, privacy and maintaining the organization's operational continuity.

The Ministry of Health sees great importance in expanding the use of cloud computing by the healthcare organizations as a tool to address the infrastructural, organizational, technological, and economic challenges they face; and encourages strengthening of the technological capabilities of healthcare organizations as an important component in the promotion of digital health, and also to be aligned with similar organizations and systems around the world.

In the Government decision number 2443 of Feb 15, 2015 about "promoting national regulation and government leadership in cyber security", the Director Generals of the government ministries and the auxiliary units, have been instructed to work to improve the level of cyber security within their ministries. Further to the government's decision, the Ministry of Health appointed a Chief Cyber Security Officer. Subsequently, a Cyber Unit was established in the Ministry of Health, which is responsible for providing guidance to healthcare organizations in Israel regarding information security and cyber security, including their implementation when using cloud computing.

2. Objective

Establishing criteria for the proper operation of computing applications using cloud computing by healthcare organizations to encourage the introduction of advanced technologies for use by healthcare organizations.

3. Definitions

3.1. "**Healthcare organization**" – Clinic, HMO or Hospital;

3.2. "**Organizational Cloud Committee**" – A committee that operates in the healthcare organization and includes at least the following officials: a representative of the CEO; a representative of the organization's legal counsel; the organization's chief information security and cyber security officer, or his representative; the organization's privacy protection officer, or his representative, if such appointed, and the organization's chief information systems officer, or his representative. A healthcare organization may define an existing committee as the organizational cloud committee, provided that it meets the conditions set forth in these provisions. A committee member may hold one or more positions, depending on the definitions of his professional roles in the organization, provided the committee composed of at least 3 members;

3.3. ""**Sectoral cloud committee**" – A committee operating in the Ministry of Health, and whose members will include: a representative of the Director General of the Ministry of Health; a representative of the Legal Counsel of the Ministry of Health; Chief Information Security and Cyber Security Officer of the Ministry of Health; Representative of the Digital Health Department of the Ministry of Health; Representative of the National Cyber Directorate; Representative of the ICT Authority; And a representative of the Privacy Protection Authority;

3.4. "**Cloud computing**" – Computing infrastructures and resources (such as servers, storage devices, networks, applications and services), which are accessed via the Internet and/or a dedicated communication line, on demand and by use;

3.5. "**Cloud computing provider**" – A commercial company that provides cloud computing services (Vendor) or cloud computing infrastructure (Provider) to the healthcare organization;

4. <u>Organizational cloud policy</u>

4.1. The Organizational Cloud Committee will formulate an organizational cloud policy in accordance with these provisions as a condition for operating an Organizational Cloud Committee. The cloud policy will be brought for approval by the management of the healthcare organization.

4.2. The organizational cloud policy shall address, at the very least, the following issues:

4.2.1. The guidelines and criteria for determining the types of applications that can be used in cloud computing;

4.2.2. The organizational procedures and the hierarchy of organizational authorities for approving the use of cloud computing, including the organization's risk management methodology;

4.2.3. Authorities and responsibilities of the various officials with respect to the use of cloud computing, including maintenance, monitoring and data security and cyber security;

4.2.4. Principles of engagement with a cloud computing provider, including the means and mechanisms for monitoring and controlling suppliers;

4.2.5. information security, cyber security and privacy protection policies of the organization, with respect to the use of cloud computing, including the controls to be implemented by the organization;

4.2.6. The life cycle of the processes of cloud computing usage, including the termination of its usage;

4.2.7. Other relevant issues given the characteristics of the healthcare organization.

4.3. 4.3 .The Organizational Cloud Committee shall hold a meeting once a year regarding the implementation of the organizational cloud policy, including an examination of the need to update the policy based on the technological developments and regulatory, organizational and business changes in the previous year.

4.4. 4.4 .The management of the healthcare organization shall hold a meeting regarding the organizational cloud policy whenever a substantial change or update of the policy is made, but not less than once every two years.

4.5. 4.5 .It is the responsibility of the healthcare organization to provide the organizational cloud policy document to the Chief Information and Cyber Security Officer of the Ministry of Health once it is approved by the organization for the first time and after any substantial update or change.

5. Application activation in cloud computing

5.1. A healthcare organization may use a cloud computing application in accordance with these provisions.

5.2. The Director General of the healthcare organization shall appoint the members of the Organizational Cloud Committee in accordance with the guidelines of this circular and the organizational cloud policy. It is the responsibility of the healthcare organization to inform the Chief Information and Cyber Security Officer of the Ministry of Health of the appointment of the members for the organizational committee before the commencement of the committee's activities and with any changes in its members.

5.3. When using a cloud computing application, it must be ensured that the healthcare organization has full ownership of the transmitted information as well as the ability to restrict how it is used.

5.4. Using a cloud computing application will be possible only **after** an organizational internal procedure for examining the transition to cloud computing usage has been implemented. The examination procedure will address at least the following aspects:

5.4.1. The business process in which the system or information requested is transferred to the cloud, including the significance and advantages for the organization or patients in the transition to cloud computing;

5.4.2. Analysis of the information and system, including mapping and classification of the information, the users, and the requested cloud computing provider;

5.4.3. Compliance of the cloud computing usage pursuant to any law, and in particular the Privacy Protection Law and the Ministry of Health's guidelines on these issues;

5.4.4. Assessment and management of the risks from the use of cloud computing in accordance with the organizational policy as approved pursuant to the provisions of Section 4.2 and in accordance with the principles set forth in Addendum A;

5.4.5. The architecture, interfaces and requirements of information security and cyber security;

5.4.6. Presenting compensating controls vis-a-vis the risk management process.

5.5. The risk level classification for using the cloud computing application will be determined based on the findings of the risk assessment process specified in Section 5.4.4 above. The determination of said classification level shall be approved by the organization's chief information and cyber security

officer, the legal counsel and the privacy protection officer of the organization, or their representatives.

5.5.1. If the results of the risk assessment showed that the risk level of operating of the cloud computing application is low or moderate, the body approving the operation of the cloud computing application will be the organizational cloud committee.

5.5.2. .If the results of the risk assessment showed that the risk level in operating the cloud computing application is high, the body approving the operation of the application shall be the organizational cloud committee, provided that the opinion of the sectoral cloud committee regarding the operation of the application was obtained.

5.6. The Sectoral Cloud Committee may be authorized to determine that:

5.6.1. The operation of a particular cloud computing application in a high risk level may be approved by the organizational cloud committee alone, subject to conditions determined by the sectoral cloud committee;

5.6.2. An organizational cloud committee may approve the operation of cloud computing application and/or matters that have been found to be at high risk without the need for the sectoral cloud committee's opinion, subject to condition determined by the sectoral cloud committee;

5.6.3. An organizational cloud committee may approve the operation of cloud computing applications that have been found to be at low or moderate risk, only after the opinion of the sectoral cloud committee has been obtained.

5.7. 5.7 The approval of the organizational cloud committee will be required for the first operation of a cloud computing application and in any substantial change in the operating mode, including the architecture, infrastructure and technology being used.

6. Engagement with a cloud computing provider

6.1. A healthcare organization shall not use cloud computing unless an agreement has been signed between it and the cloud computing provider, and as long as said agreement is in effect.

6.2. Before the healthcare organization's signs an agreement with the cloud computing provider, the healthcare organization must examine and evaluate the provider's ability to provide the requested services regarding, among other things, the following issues and in accordance with the cloud computing model used:

6.2.1. Its professional competence and its technological capabilities to provide the requested services and meet its commitments under the agreement;

6.2.2. The information security, cyber security and privacy protection means implemented by the supplier;

6.2.3. The economic means and its financial ability to fulfill his commitments to the healthcare organization;

6.2.4. The means provided by the cloud computing provider to the healthcare organization to enable the healthcare organization to comply with the requirements of Israeli law and the regulatory guidelines that apply to it with regard to the use of cloud computing;

6.2.5. The implications of the use of cloud computing outside the borders of the State of Israel, including the application of foreign law to the information in this case.

6.3. The agreement between the healthcare organization and the cloud computing provider shall address, at the very least, the following issues:

6.3.1. The division of responsibilities between the healthcare organization and the cloud computing provider according to the type of service and the cloud computing model he provides;

6.3.2. The mechanisms and means of information security, cyber security and privacy protection to be implemented by each of the parties in accordance with the division of responsibilities between them and the cloud computing model;

6.3.3. The means that will be provided to the healthcare organization to monitor the use of cloud computing and the cloud computing provider, including its subcontractors and/or third parties on its behalf and their activities, and/or to obtain information on tests and audits on said issues;

6.3.4. The arrangements to be implemented by the cloud computing provider for dealing with and handling a cyber event or an emergency event, including the manner and frequency of reports submitted to the healthcare organization on these events;

6.3.5. The agreement period, arrangements for termination of the agreement and resolution of disputes, and migrating the information to another cloud computing provider, and instructions regarding how the information is returned to the healthcare organization or destroyed in the most complete and comprehensive way possible at the end of the engagement period;

6.3.6. The business continuity mechanism of the cloud computing provider.

6.4. The healthcare organization shall periodically review and re-evaluate the cloud computing provider and the cloud computing services provided by it in accordance with technological, regulatory, organizational and business changes, but no less than once every two years.

6.5. As a guiding principle, it is possible to use cloud computing located in a country that meets the requirements of the Privacy Protection Regulations (Transfer of Information to Databases Outside the Country's Borders) (Hebrew year 5762)-2001.

7. Monitoring and control

The healthcare organization must monitor and take supervisory and control activities with respect to the use of cloud computing, pursuant to the principles outlined in the organizational cloud policy, the risk management findings and controls that were defined at the time of its approval, as well as according to the Ministry of Health guidelines.

8. Documentation, reporting and document retention

8.1. The healthcare organization shall document all stages of the approval processes of the use of cloud computing, and also address all relevant factors (if required), and decisions made. The documentation will be kept for a period of no less than 7 years from the end of the usage period of cloud computing.

8.2. The healthcare organization shall regularly report to the Chief Information and Cyber Security Officer of the Ministry of Health about any new use of cloud computing approved by the organization, and attach the approval documents and the minutes of the meeting of the organizational cloud committee, within 30 days from the date agreement with the cloud computing provider was signed.

8.3. The healthcare organization shall report once a year on all uses of cloud computing that were discontinued in the year prior to the report date, and to the extent the reason for discontinuation relates to information security or privacy protection matters - the reasons thereof.

8.4. The Ministry of Health may, at its discretion, demand to receive additional information and documents regarding any use of cloud computing that has been approved or discontinued.

9. General

9.1. To meet these requirements, the healthcare organization may utilize an external consultants with recognized expertise and proven experience in cloud computing.

9.2. The provisions of this circular will also apply to the usage of cloud computing for research of health data within the scope of the Director General's Circular 1/2018 (and/or any other circular that may replace it), in which access to health data is provided in a secure environment managed by a healthcare organization.

9.3. The technical guidelines set forth in Addendum B of this document shall be followed, and the guidelines and professional documents periodically published by the Ministry of Health, the ICT Authority, the Government Cyber Security Unit, and the National Cyber Directorate regarding the use of cloud computing, as applicable to the healthcare organization, should be used.

9.4. These provisions do not detract from the obligations applicable to healthcare organizations pursuant to the Privacy Protection Law, (Hebrew Year 5741)-1981 and the regulations thereunder, including with regard to outsourcing activities.

9.5. The use of cloud computing shall not detract from the responsibility of the healthcare organization to maintain the integrity, availability and confidentiality of the information, and to implement the information security and privacy protection requirements that apply to it as the owner and/or possessor of the data pursuant to any law.

9.6. Any reports in accordance with this circular shall be submitted to - infosec@moh.gov.il .

10. Implementation responsibility

The Director General of the healthcare organization is responsible for the implementation of these provisions in his organization.

11. Audits

The implementation of these guidelines shall be reviewed during ongoing audits of the Ministry of Health in healthcare organizations.

12. Applicability

12.1. A healthcare organization shall act pursuant to these instructions, at the latest, within 6 months from the date of its publication.

12.2. Notwithstanding the provisions of Section 12.1 above, with respect to usage of cloud computing that has begun before the publication of this circular, these provisions shall enter into effect on the time of renewal of the engagement with the cloud computing provider, or at the end of two years from the date these provisions entered into effect, whichever is earlier.

With regards

Prof Hezi Levi

MoH GM

Cc:

MK Yully Edelshtain, Minister of Health

114710817

Addendum A - A Risk Assessment Process for Operating a Cloud Computing Application in the Healthcare System

The process of assessing the transition to cloud computing shall address, at least, the aspects listed below. The risk management tool that was developed by the Ministry of Health, the National Cyber Directorate, the Privacy Protection Authority and the ICT Authority, can be used by healthcare organization as is or to be adapted to the characteristics of the organization.

1. Description of the business process

    1.1. The business process in which there will be use of the system or information requested to be transferred to cloud computing, as well as the interactions between processes within the organization and systems tangent to the cloud or to the healthcare organization, shall be elaborated.

    1.2. The objective of the system and its usage purposes must be specified, as well as the reasons and expected benefits from the transition to the use of cloud computing.

2. Analysis of information and applications

    2.1. A complete review and analysis procedure of all the information and applications that are intended to be transferred to cloud computing, must be performed, and the following must be examined:

        2.1.1. **Mapping the information**. The information that is expected to be transferred to the cloud environment must be mapped, including whether it was published to the public, whether it is exposed to external parties, whether the information is classified, whether it will contain personal and private data, whether it will contain data that may affect the proper functioning of the organization and may harm governance, whether it will contain medical data, and the level of its identifiability etc.

        2.1.2. **Classification of information**. The sensitivity of the data must be examined according to, among others, the procedure of data classification for the healthcare sector (A.8), as will be in effect.

        2.1.3. **The scope of the information**. The amount of information expected to be transmitted during the use of the system should be examined.

3. System analysis

    3.1. **Interface mapping**. The external interfaces of the internal network and the external interfaces of other suppliers should be examined. Thus, the frequency of the link to the interface, the direction of the interface, the protocol, the type of verification and the nature of the reading should be addressed in addition to the information security controls that will be provided to the system.

    3.2. **Users**. The parties that use the application and the permissions required of them, and the parties that will have access to cloud computing must be mapped and defined. Users' classification, number of users, administrators, user definition and permissions, and access to the system must also be addressed.

    3.3. **Existing organizational infrastructures**. The existing systems or cloud environments in the organization should be specified and examined; Possible interfacing of the system with other systems in the organization; And past experience versus transferring systems to cloud application in the organization.

    3.4. **Communications Provider to/from the cloud computing**. The following must be examined: Who is the provider? What are its infrastructures? What regulations apply to it and to the infrastructures?

What is the defined level of service? What internal and external protection measures does the provider allows? Who will have access to cloud computing? And what is the requested service model.

3.5. **Characteristics of the requested service and mode of application**. The supplier and the organization's existing infrastructure with respect to the operation of the requested application, should be examined, as well as the options for backup, durability, and monitoring of information and the system, in addition to the way of data storage and encryption, migration processes at the end of the usage, and performance of penetration tests, if relevant.

4. Regulatory and legal compliance

Ensuring that the required processes meet the legal requirements in addition to the guidelines of the Ministry of Health, the Cyber Directorate and the ICT Authority.

5. The Risk analysis

5.1. All possible risks that arise from using cloud computing and concerning the analysis of sections 1-4 of this addendum, should be mapped. To the extent relevant, individual risks arising from the use of medical information and/or from the application intended to move to cloud computing and/or the healthcare organization's characteristics, must be addressed.

5.2. For each of the risks, the probability of its occurrence, the severity of the damage, and the controls to be implemented to balance and reduce the chances of occurrence and the severity of the damage must be addressed.

5.3. The risks must be examined according to the values of confidentiality, availability, and integrity of the information and in accordance with the defined model of cloud computing usage, and the division of responsibilities between the cloud computing provider and the healthcare organization.

5.4. In general, the level of risk will be determined, among other things, by taking into account the following parameters: the type of information and its sensitivity; the scope of the data transmitted to cloud computing - both in terms of the number of records and in terms of the depth of information in each record; and the length of time the information will be in the cloud.

For each risk, the measures that will be implemented by the organization/provider to respond to such risk must be defined, as well as their chances of reducing the risk in question.

6. Proposed Architecture

The proposed architecture for the solution must be presented, including the solution components, the interfaces, the security mechanisms that will be activated, and the method of their implementation.

Addendum B - Guidelines of the Cyber Protection Unit for the Health Sector

Examples of threats while transitioning to a public cloud

Here are some examples of risks and threat scenarios, whose impact and their similarities should be considered when formulating a decision to move to any cloud environments, and assessing the control processes for risk mitigation (taken from the Government Cyber Security Guidance No. 5.5: "Securing information for moving to a public cloud"). It should be clarified that **these are only examples, and not an exhaustive list**, of the risks and threat scenarios, and additional risks and threats in using a public cloud should be examined, depending on the type of service and its characteristics, and the type of system and information transmitted to the cloud.

1. Disclosure or leakage of information

Several scenarios can cause threats of disclosure or leakage of information in cloud computing environments. The following are examples of common scenarios:

1.1. Disclosure of information resulting from an inefficient separation between cloud customers (Tenants) who share computing resources.

1.2. Information disclosure due to a court order of a foreign government. Retention of information in a jurisdiction other than the State of Israel, exposes the information to the laws and regulations of the governments in which the cloud provider operates and stores information.

1.3. Leakage of databases and sensitive information that have been transmitted or left in the cloud computing environment at the end of the engagement with a cloud computing service provider, without sufficient controls required to protect such information, and adapted to the profile of relevant threats and to the requirements of the Privacy Protection law in Israel.

1.4. Information disclosure by the employees of a cloud computing service provider or by a third party, who have the ability to access cloud computing information similar to outsourcing, which involves other entities that do not have direct contact with the cloud customer, and may not be bound by confidentiality of the information and to its owners.

1.5. Disclosure of information due to hacking into an end device - many end devices, usually mobile devices, use cloud computing services to store the data in a central and accessible location. Hacking into the device after its loss or theft, and in case the device is not protected by appropriate means, may result in information disclosure.

2. Loss or disruption of information

Cloud computing service providers are not immune to the loss or disruption of information due to a malfunction or intrusion into the system. In general, the threat of information loss or disruption, should be examined under the following scenarios:

2.1. Loss or disruption of information due to a malfunction at the cloud computing provider, including physical destruction of computing infrastructure.

2.2. Loss or disruption of information due to an attack that has penetrated the cloud computing environment. Keep in mind that in a cloud computing, the central management and the ability to control a variety of components from a single location, increase the ability to compromise all information and components.

2.3. The cloud computing provider ends its services.

2.4. Interception of the communication medium between the cloud computing provider and the health care organization.

3. Loss of information availability

In cloud computing, the availability of information depends on several factors, and several scenarios can cause the loss of service availability. The risk assessment should address these scenarios and their impact on the functional continuity of the healthcare organization:

3.1. The cloud computing provider cannot allow system availability due to a malfunction or denial-of-service attack (DDOS).

3.2. The customer loses the ability to connect to the system due to a network connection failure or a denial-of-service attack.

3.3. The customer's account is blocked due to a malfunction, attack, or violation of the terms of service.

3.4. The cloud computing provider does not meet the loads or SLA required to implement the customer's system.

3.5. The cloud computing provider was forced to discontinue the service due to a court order, violation of a law/regulations/business/financial decision.

3.6. The customer of the service loses availability to data in the cloud due to a failure of advance appropriate resources allocation by the cloud computing provider.

Choosing a Cloud Computing Provider

Characteristics for the selection of cloud computing provider and entry into contract with him

1. Preference should be given to selecting cloud computing provider who implements a recognized and accepted international standards, such as ISO 27001, ISO 27017, ISO 27018, SOC 2, CSA, AICPA as well as those that are compatible with the GDPR.
2. For the sake of availability and the durability of the service, preference should be given to a cloud computing provider that allows multiple availability sites in each geographical site.
3. The commitment of the cloud computing provider for the availability of the geographical sites should be examined, as well as determining the provision of an appropriate SLA at the time of signing the contract with the provider based on the RPO and RTO values of the organization's information systems, and in accordance with the organizational cloud policy.
4. Preference should be given to choosing a cloud computing provider that commits to allowing the organization to have a unilateral option to stop using the provider's services or to switch to another provider while transferring its relevant data from the provider's systems within a short period of time, deleting them from the provider's systems, and have the provider's commitment to a complete and comprehensive deletion of the data in compliance with accepted international standards.

Designing Secure Architecture for Cloud Computing Services

1. Following the selection of a cloud computing provider, the architecture solution for the cloud computing transition should be built by the organization or by an external provider who specializes in cloud computing, and along with a professional who has appropriate training in cloud computing, and experience and expertise in cloud infrastructure protection.
2. The solution architecture should address at its outset, the aspects of information security and Cyber security and on ways to prevent the realization of the threat scenarios defined in the risk assessment.
3. The organization must ensure that for the solution architecture which includes channels from/to the cloud computing provider, there are measures for cyber security and information security, which will enable to minimize, as much as possible, the use of these channels to attack the organization.
4. The organization's information must be encrypted (by at least 256AES protocol) during network transmission, and when stored in a system which is not for the organization's sole use (Multi-Tenancy). In cases where it is difficult to encrypt all said information, at least the data classified by the organization as sensitive, whose disclosure may harm the organization and its patients, must be encrypted. An application that enables, as much as possible, to store the encryption keys at the organization must be examined.
5. In addition, the ability to maintain a separation between the domains outside of the healthcare organization and those linked to the organization must be ensured; Ensure the availability of the service and the information and alternatives (BCP) during a communication crisis; Maintain relevant user and key management, as well as define the operational function and its various permissions.
6. The architecture must be approved by the Chief Information Security Officer and the Chief Information Officer.

Transition of the system to a production environment

1. Examination of the security of the proposed solution

Prior to the implementation of the architecture to the production environment, a comprehensive information security check must be performed, to examine the proposed solution. During the process, a durability and resilience test must also be performed to the proposed solution and to the components on which the system/application is installed.

2. Transition of the system to a production environment

    2.1. Before approving the system in the production environment, the system must be tested in the testing environment in order to check for failures. Make sure that changes made to the system at all stages of testing and Acceptance Test Procedures (ATP) are documented.

    2.2. A soundness testing, penetration testing, and targeted weaknesses testing of cloud application must be done according to the complexity of the system and its features.

    2.3. Once all failures (if any) have been fixed and with the Chief Information Security Officer approval, the system can be uploaded to the production environment.

    2.4. As needed, training shall be provided to all the employees in the healthcare organization who use the service/system located in the cloud computing services, which will include aspects of secure usage.

3. Monitoring information security incidents and failures

3.1. The organization must ensure that it can monitor information security events that are related to the cloud computing application and its use in cloud computing systems throughout the period of the cloud computing services usage.

3.2. The organization must define monitoring objectives, including the types of information and activities to be monitored, the type of required monitoring, how monitored information is to be saved, who will be authorized to access this information, and how the data will be accessed.

3.3. Monitoring can be done using tools provided by the cloud computing provider, however it must be verfied that the tools meet acceptable standards and allow integration with the organization's existing monitoring systems.

4. Responsibility and control

4.1. The Chief Information Security Officer and the Chief Information Officer and the Infrastructure Operations Administrator will be responsible for the control of the proposed solution, the examination of its integrity, and monitoring failures.

4.2. The Chief Information Security Officer will be responsible for conducting cyber surveys and penetration tests at the commencement of the cloud computing service, in accordance with the frequency set forth in the Privacy Protection Regulations (Data Security), (Hebrew Year 5777)-2017.

5. Tracking and reporting

5.1. It is the responsibility of the Chief Information Security Officer and the Chief Information Officer to continuously monitor the implementation of the solution in the organization.

5.2. The Chief Information Security Officer and the Chief Information Officer will report to the Organizational of Cloud Committee regarding planning versus execution of the chosen solution and on the monitor improvement of deficiencies, if required.

6. General

Reports in accordance with this circular shall be submitted to the following e-mail address: infosec@moh.gov.il.