



Report of the State Comptroller of Israel | May 2022

The Ministry of Health

Cyber Protection of Medical Devices and the Security of the Information Stored Therein



Cyber Protection of Medical Devices and the Security of the Information Stored Therein

Background

Over the last decade, cyber-attacks on organizations and individuals worldwide have increased; in recent years, cyber threats to medical institutions have also increased. Medical centers have systems whose shutdown could affect the activity of the medical center and even risk patients' lives. Cyber-attacks on the health system may cause extensive damage, including damage to the provision of essential medical services in routine and emergency times; theft of personal medical information and its abuse, which has severe personal and trust effects on the country's medical institutions; intentional disruption of information following a change of personal clinical files information which may lead to making incorrect medical decisions; damage and destruction of expensive medical equipment.

Medical institutions use tens of thousands of medical devices for various medical procedures; among these are MRI¹ (Magnetic Resonance Imaging), CT (Computed Tomography), X-rays, and women's ultrasounds. Medical devices must be thoroughly and regularly available in light of the various procedures that must be performed, especially considering their necessity for life-saving procedures.

Cyber protection (information security) in medical devices, including imaging devices, is to prevent an unauthorized party from making changes to the information stored in them; unauthorized use or misuse of the medical information stored in them, which is processed in it or transferred from them to an external destination; and damage to their operation.

This report is based on the responses of the 25 medical institutions to a questionnaire on "Protection and security of information in medical devices" given by the State Comptroller's Office: the 11 general-government medical centers, the two public medical centers, the eight general medical centers of the Clalit HMO (Health Maintenance Organization) and the four HMOs. The Clalit HMO gave its response in some of the chapters in the questionnaire on behalf of all eight of its general medical centers and community clinics, therefore the number of institutions covered by these chapters is 17.

In mid-October 2021, during the audit period, hackers broke into the computers and servers at the Hillel Yaffe Medical Center in Hadera. The attack disrupted the medical center's activities. It caused patients to be diverted from the medical center to other centers, and a

1 Medical imaging is an advanced technology in which internal parts of a subject's body are demonstrated through photographs. This is a general name for a variety of basic tests carried out prior to a significant part of diagnoses and medical procedures, for the purpose of clinical diagnosis, treatment planning, patient follow-up and assistance in performing invasive procedures (surgeries).



switch to manual rather than computerized work to prevent access to the patient's medical information, and more. This attack highlights the importance of optimal preparation for cyber threats and information security.

Key figures

about 9.5 million

Cyber-attacks attempts around the world in 2020 aimed to disrupt computer systems²

about 2,700

the estimated number of MRI, CT, X-ray, and ultrasound imaging devices in the medical institutions that were examined

8%

the minimum budget rate that should be allocated, according to the government's resolution, to cyber protection, out of the information systems budget of the government medical centers

13 out of 17

medical institutions³ did not carry out a risk survey⁴ regarding medical devices

13 out of 17

medical institutions did not include in their plans the manner of handling and recovery of the medical devices in a disaster event

5 out of 17

medical institutions did not stipulate the purchase of medical devices on the information security officer examining their information security aspects

13 out of 17

medical institutions do not have logical privileges control (username and password) for access to a women's ultrasound machine

14 out of 17

medical institutions did not perform penetration tests⁵ for medical devices in 2018–2021

2 DDOS type attacks – Denial of Service Attack Distributed, denial of service attack.

3 The Clalit HMO was counted as one medical institution but the reference in this definition is to all eight of its general medical centers and clinics in the community.

4 A risk survey examines and locates threats and exposures of information security in the systems of the medical institutions and assesses the level of risk their activities face with respect to these threats.

5 A penetration test is a procedure during which a controlled and planned attack is carried out on the organization's computerized system in order to locate weaknesses therein.



Audit actions



From January to November 2021, the State Comptroller's Office examined the cyber protection of medical devices and the security of the information stored therein, focusing on imaging devices (CT, MRI, X-ray, and women's ultrasound). The audit included the examination of the administrative activity of information security in the medical institutions; the protection of the devices throughout their life cycle: their purchase, their use, and the end of their use; an examination of the devices protection on the network of the medical institution, the devices access privileges, the users management, the information security when deciphering the findings of the scans, the protection of the medical information stored on the devices and their maintenance methods. The audit was conducted in the Ministry of Health, in 25 medical institutions: in the HMOs, in all the general-government and municipal-government medical centers, in the general medical centers of the Clalit HMO, and two public medical centers⁶. Completion examinations were done at the National Cyber Directorate, the Privacy Protection Authority at the Ministry of Justice, and "Inbal Insurance Company Ltd.", a government insurance company.

This report was presented to the Prime Minister and the Knesset State Audit Committee on February 15, 2022, and was classified as confidential until the State Audit Committee's subcommittee hearing.





By the authority under Section 17(c) of the State Comptroller Law, 1958 [Consolidated Version], and after considering the government's arguments, consulting with the bodies responsible for the protection of national security information and in coordination with the Chairman of the Knesset, since the subcommittee above did not convene, it was decided to publish this report while imposing confidentiality on sections of it.

These sections shall not be submitted to the Knesset, nor shall they be published. The findings of the audit report and its recommendations are valid as of the date of its presentation.

⁶ In most chapters of the report, the Clalit HMO was counted as one entity, including both community clinics as well as its hospitals, and therefore the number of institutions covered by these chapters is 17.



Key findings

-  **The responsibility for cyber security** – about six years after the adoption of Government Resolutions 2443 and 2444 on national preparedness and the advancing of national regulation for cyber security (in 2015)⁷, and despite the national importance of regulating cyber defense, the powers of the National Cyber Directorate regarding the units for professional guidance in the government ministries (sectorial units) were not regulated, including in the health sector.
-  **The Ministry of Health activity in the cyber security** – the Ministry of Health has not completed the formulation of cyber security guidelines, including basic principles for managing cyber security and tools to cope with a cyber-event, and these have not been published. As part of the licensing inspections that the Ministry conducted in the medical centers in 2019 and 2020, it did not examine the medical devices protection; and does not regularly follow-up on the rectifying of deficiencies that arose in the inspection reports it carried out on information security, and thus does not verify their non-recurrence. The Ministry of Health's SOC (Center for Monitoring, Command and Control of Cyber Events) is partially staffed – during certain hours on weekdays, and certain deficiencies have arisen in its operation. The guidelines of the Medical Devices Department in the Ministry of Health, which handles the registration of medical devices and the granting of import and marketing permits for them to Israel, do not pertain to the need for their compliance with information security standards.
-  **The Government Medical Centers Division's responsibility for information and cyber security** – the Medical Centers Division at the Ministry of Health does not have an optimal situation report of the information security quality in each of the medical centers under its responsibility. Although the government's resolution states that the Division will serve as a head office regarding information systems, and even though the Ministry of Health Director General circular states that the Division's responsibility of operation the medical centers includes information systems aspects, in practice – the Division operates an information systems division, but the sectorial cyber unit in the Ministry of Health deals with information security without the Division's involvement.
-  **Information security policy in the medical institutions – steering committee and officials** – in 19 out of the 25 medical institutions that answered the information security questionnaire, the institution's CEO did not head the steering committee on

⁷ Government Resolution 2444, "Advancing the National Preparedness for Cyber Security" (February 15th, 2015); and Government Resolution 2443, "Advancing National Regulation and Government Leadership in Cyber Defense" (February 15th, 2015). Resolution update date – July 28th, 2015.



information protection; eight of the 25 medical institutions did not appoint a privacy protection officer.

The following findings were raised from the above mentioned information security questionnaire where the Clalit HMO answered on behalf of all eight of its medical centers and community clinics and was therefore counted as one medical institution. The findings, therefore, concern 17 medical institutions:



Information security policy in the medical institutions and their compliance with the information security procedures – the medical institutions significantly differ in the ratio between their number of employees in the information security or cyber protection and the number of their total employees: Five institutions have an information security staff member for every 1,000 employees or less and three have one staff member for every 3,000 employees; six out of 11 general-government medical centers allocated to cyber protection, on average, in the years 2015–2020 a rate lower than the one set in the government resolution – 8% of the budgetary allocation for information security⁸; at the time of the audit, all government medical centers did not have cyber insurance. Regarding the other medical institutions, some had cyber insurance, and others did not. Five medical institutions did not address in their work plan for the years 2020 and 2021 the improvement of the medical devices protection and the security of the information stored therein; Eight out of 17 of the medical institutions did not carry out an internal audit in the field of information security; 13 out of 17 medical institutions did not conduct a risk survey regarding medical devices; 11 of the 17 medical institutions did not define risk groups for the medical device according to risk classifications.



Disaster recovery and business continuity of medical devices – out of the 17 institutions, two do not have a disaster recovery plan (for example, a cyber attack on the medical institution's information systems infrastructure) or business continuity plan (an organization's ability to continue its normal operations); six do not have an alternative site (DR) available to continue the information systems operation in the event of a disaster; 13 did not include in their disaster recovery or business continuity plans, the handling manner and recovery of the medical devices.

8 The government resolution on the subject did not pertain to public medical centers or the HMOs, therefore the medical institutions examined in this chapter were 11 general-government medical centers.



Information security policy																	
Inst. B	Inst. O	Inst. E	Inst. H	Inst. M	Inst. L	Inst. K	Inst. J	Inst. I	Inst. Q	Inst. G	Inst. F	Inst. N	Inst. D	Inst. C	Inst. P	Inst. A	
●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	The institution's CEO heads the steering committee
●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	Appointment of an Information Security Officer
●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	Appointment of a Privacy Protection Officer
●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	Work plan concerning information security
●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	Work plan addressing the protection of medical devices
●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	Risk survey concerning information security
●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	Updating of the risk survey
●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	Risk survey concerning medical devices
●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	Defining risk group classifications for medical devices
●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	Business continuity or disaster recovery plan
●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	Available alternative site (DR)
●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	The disaster recovery plan addresses medical devices
●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	Procedure for coping with an information security event
●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	Internal audit concerning information security

● Yes ● No ● Partial ● In process/ Being written

Information security when purchasing a new medical device – out of the 17 institutions examined, five did not refer in their procurement procedures to medical devices information security, and one had no procurement procedure; five did not stipulate the medical devices purchase on the information security officer approval, and sometimes medical institutions that required in their procedures the approval of the information security officer for the purchase purchased the devices without receiving approval; there are also discrepancies between the types of information security tests performed by the medical institutions when purchasing medical devices and before starting to use it and their number, including removing from the device applications that are not required and scanning the device using a tool for identifying malware, malicious software, and unusual activities.

Information security when purchasing a new medical device																	
Inst. B	Inst. O	Inst. E	Inst. H	Inst. M	Inst. L	Inst. K	Inst. J	Inst. I	Inst. Q	Inst. G	Inst. F	Inst. N	Inst. D	Inst. C	Inst. P	Inst. A	
●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	Addressing information security of medical devices in the procurement procedures
●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	Stipulating the purchase of medical devices on the approval of the Information Security Officer
●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	Submitting a form with technical indices to the Information Security Officer

● Yes ● No



Protection of the medical devices while they are being used in the medical institution – of the 17 medical institutions examined, six did not map all their medical devices; not all institutions included in their mappings the devices critical information security characteristics; there are substantial deficiencies in the protection system that the medical institutions implemented in the network for protecting medical devices, including MRI and CT imaging devices, and in some institutions there is a combination of deficiencies that increase the devices' exposure to information security risks; 11 of the 17 institutions did not regulate software procedure updates, which is required to ensure continuous and safe operation of the medical devices, and ten institutions did not document the software version updates they performed on medical devices; 14 institutions did not perform penetration tests including an attack on medical equipment in the years 2018–2021, as stipulated by the procedure of the Ministry of Health.

Protection of the medical devices during use thereof in the medical institution																	
Inst. B	Inst. O	Inst. E	Inst. H	Inst. M	Inst. L	Inst. K	Inst. J	Inst. I	Inst. Q	Inst. G	Inst. F	Inst. N	Inst. D	Inst. C	Inst. P	Inst. A	
●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	Mapping of the medical devices' array
●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	Mapping was updated
●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	Privileges were updated in 2019 and 2020
●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	Proactive deletion of the remaining information
●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	Procedure for regulating software updates
●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	Documentation of the software updates
●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	●	Performance of penetration tests to the medical device

● Yes ● No ● Pilot stage/ Process of being executed/ Not relevant



Physical and logical privilege controls for imaging devices – access privileges, user list management, and password policies – are central tools in implementing information security policies in any organization. Seven institutions did not update at least once the list of users with logical privileges (username and password) for the medical equipment system in 2019–2020; two institutions have x-ray devices without physical privileges control (locked room) and logical privileges control. There are no physical and logical privileges controls in two medical institutions on some of the women's ultrasound devices. There is no logical privilege control for any imaging devices examined in four medical institutions.



Protection of the devices and the information therein during their maintenance and when deciphering results – in one institution, external technicians perform maintenance activities without the medical institution's accompaniment, and two medical institutions did not sign a confidentiality agreement with companies that provide maintenance services for the medical devices, or with their technicians; Out of 14 institutions that allow the manufacturers of the devices to connect to the MRI and CT devices remotely, one institution did not regulate the method of remote connection through a procedure, and two did not monitor the remote connection, for example by recording the actions or the connection; Seven out of 12 of the institutions that took medical devices for maintenance outside the medical institution did not have accurate information regarding the number of devices taken out for maintenance in 2020 and their identification.





Establishment of a monitoring, command, and control center (SOC - Security Operating Center) of the health sector – in 2016, even before the issue of the National Cyber Directorate directive, the Ministry of Health decided to establish a sectorial SOC that will provide service to medical institutions – act as a center serving to monitor cyber incidents as well as for the command and control thereof. The SOC began operating at the end of that year.

Compliance with the ISO standard and the existence of a work plan – at the end of the audit (November 2021), all the medical institutions included in this report complied with the international standard ISO 27799 for the information systems security in the health sector. In addition, all 17 medical institutions that answered the information security questionnaire had an annual or multi-year work plan in information security.




Key recommendations

 The State Comptroller reiterates his recommendation from a previous report to advance the powers regulations of the National Cyber Directorate concerning the sectorial units in the government ministries, including the health sector and the disparities between the powers of the regulators.

 It is recommended that the Ministry of Health:

- Complete the formulation of cyber security guidelines and their publication, so it will regularly integrate into the control it conducts in the medical centers and HMOs an examination of both information security matters and medical devices, and follow the rectifying of the deficiencies that arose in them. It is also recommended that the Ministry formulate a multi-year plan for cyber security in medical institutions that include a definition of goals, priorities, indicators, and an assessment of the required budget and the possible funding sources. It is also recommended that the Ministry consider obligation to appoint a privacy protection officer similar to the requirement in many Western countries.
- Examine the interfaces between the Government Medical Centers Division and the sectorial cyber unit and consider which to entrust the responsibility for handling the information security in all government medical centers (general, geriatric, and mental health), also in light of the government's resolution on the matter.
- Take steps so that the SOC of the sectorial unit will operate regularly, respond to the inadequacies that have arisen, and complete the connection of all medical institutions to the SOC. It is further recommended that the Ministry consider incorporating information security standards into the approval process of the Medical Devices Department for the import and marketing of medical devices to Israel. This step will allow for a centralized inspection of the information security measures required for new medical devices. It will improve the security of medical devices used by hospitals, HMOs, and other medical institutions. It is also recommended that the Ministry examine the necessity to define at the national level, which medical devices should be included in the highest risk group and should be given the maximum protective response.

 It is recommended that the medical institutions:

- Ensure that the CEO heads the data protection steering committee as required in the 2015 circular of the Ministry of Health's Director General; follow the government resolution instructions and allocate a dedicated budget for cyber security at the rate determined by it; survey the risks posed to the medical devices they use and define risk groups for them. The internal auditors of medical institutions should prepare an internal audit plan to examine information security issues.



- To ensure the ability of the medical institutions to return, as soon as possible, to regular and reasonable operation in the event of a disaster, it is required that they establish an alternative site (DR)⁹. It is further recommended that they refer in their plans for business continuity and disaster recovery to the handling manner and recovery of the medical devices under the prioritization of the devices according to their degree of importance within the medical institution's activity.
- It is recommended that they ensure the procurement procedure of medical devices information security aspects, including the involvement of officers in the information security, compliance of the medical devices with the threshold conditions established by the medical institution, and the checks that must be carried out with the supplier. The medical institutions that have not yet done so should integrate the information security officer into the chain of approvals for new medical devices, and incorporate this procedure into their current procurement activities; it is also recommended that they integrate comprehensive tests of the medical devices they purchase prior to using them and that they designate a person within the institution to be in charge of performing the tests and documenting their performance.
- It is recommended that they reconcile the deficiencies found therein in the components of the protection of medical devices; complete regulations of the software updates process in the medical institution, which will document the software version updates they have done in the computer systems, including in the medical equipment system. The medical institutions should incorporate in their work plans periodic penetration tests for medical devices both at the infrastructure and at the application level; It is recommended that the tests be performed on the basis of a risk survey allowing to identify the medical devices exposed to the highest security risk; It is further recommended that all medical institutions improve the logical control system in their imaging devices, and if there is a limit to the definition of such control, it is recommended that they implement compensatory controls in this work environment, to minimize the risks associated with the use of these devices.
- It is recommended that they Ensure that external technicians performing maintenance work at the medical institution will arrive only after coordination with the relevant authorities and will be accompanied at all times by an employee of the institution; that they regulate in the procedure the remote connection method of the suppliers and implement control processes for the remote maintenance activity. They should also keep a complete record of all the information necessary before taking the medical devices for maintenance outside the institution, including indicating in

9 DR – Disaster Recovery – an alternative site available for the continued operation of the information systems in the event of a disaster – damage or shutdown of the main site. Such a site will allow, in the event of a disaster, the medical institution's information systems to be put to use quickly, to recover patient information and to continue providing medical services.

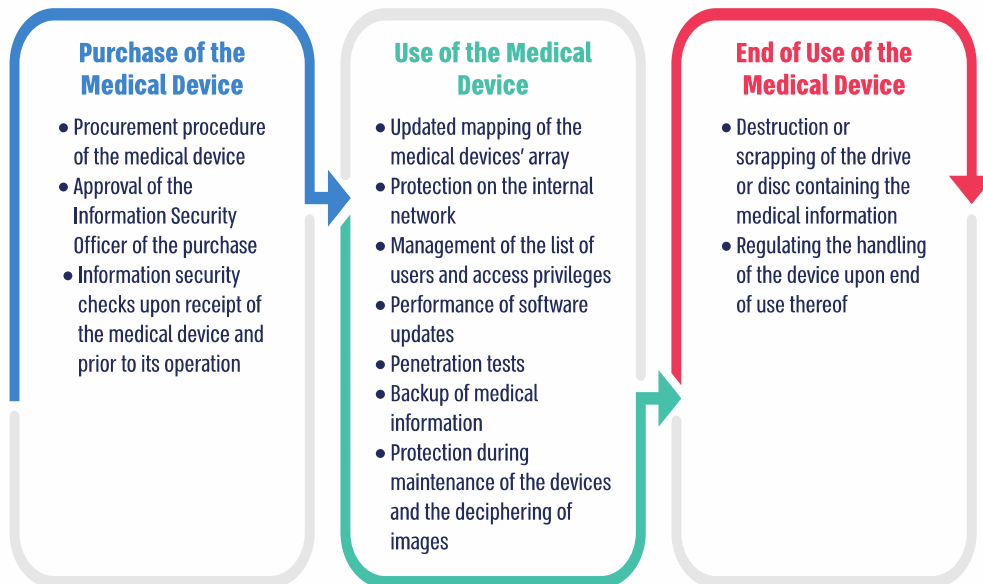


the records if the medical information stored in the devices is deleted before they are taken out for maintenance and upon the end of their use.



It is recommended that the Ministry of Health and the National Cyber Directorate consider establishing a minimum standard and requirements regarding the size of the desired information security team in a medical institution according to its characteristics.

The Medical Devices' Process of Protection During Their "Life Cycle"





Summary

The cyber threats to the health system are increasing. They are real and not just a threat; attack attempts by hackers are carried out all the time. Such attacks may disrupt the medical institutions' regular operations, leak patients' medical information, and damage essential medical devices. However, this does not merely pertain to attack attempts by hackers but also to attempts by interested parties who have access to systems and equipment and wish to damage or disrupt their activities. Moreover, even routine and innocuous activity may damage information systems, databases, and medical devices. These threats oblige the Ministry of Health and the management of medical institutions to emphasize the information security risks involved in using medical devices and the proper way to cope with them.