APPENDIX: Demands for computer and Cyber Security to connect medical devices into the Sheba network and/or to receive data from medical devices

Tender no._____ Date: ___/___/____

Device Name: _____ Manufacturer name: _____
Device model: _____ Supplier Representative name: _____
Supplier Name: _____ Cellphone number: _____
Supplier Email: _____@_____

Mandatory requirements:

1. Paragraphs appointed with an asterisk (*) must be Marked as "Acceptable" in the Appendix.
2. The operating system and cyber security system (for example Anti-Virus) **manufacturer supports**.
3. Operating systems receive security updates following the organization policy.
4. Device\ Computer system, which declared by Supplier as **standalone**, obliged to be approved by the Department\Institute\Clinic acquiring the Device\ Computer system and Medical Engineering department. The approval will be attached to this document.
5. Standalone Device\ Computer system will not be allowed to transfer data to Hospital network, Clinical systems, storage and so on.

Name: _____ Signature: _____

Connectivity summary

1. To ensure effective and functional connectivity between Proposed System and information systems in Sheba network, it's crucial that a Supplier of Proposed System will contact and cooperate with that Sheba information systems leaders, prior to attending the Tender and naturally, include the projection in Tender proposition. Validation and signed positive answer from the Sheba information systems leaders will clarify whether it is full and proved compliance or accepted standard, that will require a development of a new interface for information exchange.
   1.1. For Medical Imaging devices – ALGOTEC company
   1.2. Laboratory devices – SOFTOV
   1.3. Monitoring and measuring devices on patient body (monitors, respiratory, anesthesia, vital sign and etc.) – IMDSOFT software
   - Receiving a contract for a Tender will depend on physical proof of the compliance.
   - Whether a development of a new interface needed, this development will be evaluated and included in bid proposition.

2. The Supplier of Proposed System will elaborate on interfaces, that will be provided, including:
   2.1. Patient data input from Sheba information systems interface 2.2. Transfer of data from Proposed system to Sheba information systems 2.3. Supplier of Proposed System will also elaborate on:
      a. Standards
      b. Formats
      c. Details about information passing through the device and a manner of transition
      d. How transition of information is triggered
      e. Self-ability of recognizing patient identity
      f. Ability to connect to AD
      g. Local accumulation of produced data and general behavior due to lack of network communication
      h. Ability to transfer data to Data Lake and BI systems (as an addition to transition in section 1)
      i. Terms and limitations
      j. Medical centers with operational interfaces in question
      k. Any relevant information, regarding interfaces in question

Name: _____ Signature: _____

Medical Device:

Please circle the applicable:

* **Connection**: to Hospital network | standalone | to specific PC *
  Medical record storage: locally | central DB | medical record system | not recording
* **System definition:** logistics | LAB | treatment\diagnostics |POC
* **Maintenance access:** Israel | abroad | not applicable

1. Name and type of the Operating System: _____

   (a) Operating system version: _____
   (b) Type of the OS (Pro\Embedded or other): _____
   (c) Service Pack/Patch/Build: _____
   (d) Whether system is WIN 7/10 please provide date of expiration for Microsoft support___/_____/____
   (e) please specify OPENSSL version: _____

Mark 'X' in each box, for example -

Non Acceptable	Acceptable
	X

nub		Acceptable	Unacceptable
2.	Username and password for OS with Administrative rights access will be handed to the Computer Unit.		
3	The device won't be connected through independent modem, if a modem is installed it will be removed before joining Medical device to the Sheba network – this is a responsibility of the supplier. Whether an maintenance of the system won't be possible, without modem installed, the organizational CISO must be contacted for approval.		
4	Each issue regarding remote connection will be executed only by the Computer Unit without third-party software. The supplier have to sign a non-disclosure agreement provided by the Information Security staff.		
5	Medical Device with more than one network card won't be allowed into Sheba network.		
6*	All installations \ upgrades of the OS, application or other software will be admitted to Sanitization system, software will be provided upfront in cooperation with Sheba Computer Unit staff.		
7	Device network name must be altered in accordance to organizational convention		
8	For security reasons – login to the device should be with domain and not local user, please mention , whether it can be implemented.		

Name: _____ Signature: _____

Computer connected to Medical Device (fill according to relevance):

Please circle the applicable:

* **Connection**: to Hospital network | standalone | to specific PC
* **Medical record storage**: locally | central DB | medical record system
* **System definition:** logistics | LAB | treatment\diagnostics |POC
* **Maintenance access:** Israel | abroad | not applicable

1. Name of the Operating System: _____

   (a) Type of Operating system version: _____
   (b) Type of the OS (Pro\Embedded or other): _____
   (c) Service Pack/Patch/Build: _____
   (d) Whether system is WIN 7/10 please provide date of expiration for Microsoft support___/_____/____
   (e) please specify OPENSSL version: _____

Mark 'X' in each box, for example -

Non Acceptable	Acceptable
	X

nub		Acceptable	Unacceptable
2.	Username and password for OS with Administrative rights access will be handed to the Computer Unit.		
3	The computer won't be connected through independent modem, if a modem is installed it will be removed before joining Medical device to the Sheba network – this is a responsibility of the supplier. Whether an maintenance of the system won't be possible, without modem installed, the organizational CISO must be contacted for approval.		
4	Each issue regarding remote connection will be executed only by the Computer Unit without third-party software. The supplier have to sign a non-disclosure agreement provided by the Information Security staff.		
5	Medical Device with more than one network card won't be allowed into Sheba network.		
6	All installations \ upgrades of the OS, application or other software will be admitted to Sanitization system, software will be provided upfront in cooperation with Sheba Computer Unit staff.		
7	Computer network name must be altered in accordance to organizational convention		
8	For security reasons – login to the computer should be with domain and not local user, please mention , whether it can be implemented.		

SERVER:

Name: _____ Signature: _____

1. Name and type of the Operating System: _____

a) Version: _____

b) Service Pack: _____

c) OPENSSL version: _____

d) IIS/Apache version: _____

Mark 'X' in each box, for example -

Non Acceptable	Acceptable
	X

nub		Acceptable	Unacceptable
2	The server will be virtually installed under VMWARE ESX.		
3	An operating system will be installed in the medical center by the Computer Unit staff (accompanied by the supplier).		
4	If a large storage arrangement required for the archives, the area will be provided by NAS configuration, and CIFS protocol must be supported on the system. **Please provide following details:** a. Required daily size: _____GB b. Required monthly size: _____GB c. Required annual size: _____GB		
5	Multi Share must be supported connecting to Storage		
6	Software license support and not through Dongle PC.		
7	In case that the system works with DATABASE, the supplier has to support SQL 2016 as basic criteria.		
8	The application is obligated to work only with Service and not with User Logon.		
9	The server will be preinstalled with Sheba XDR (Sentinel One) and will be daily updated from Medical Center XDR servers		
10	All installations \ upgrades of the OS, application or other software will be admitted to Sanitization system, software will be provided upfront in cooperation with Sheba Computer Unit staff		

CONNECTIVITY:

Name: _____ Signature: _____

nub		Acceptable	Unacceptable
1	The system has to supply and support the following link options (supplier will bare the cost of the connection): a. The transfer of data to an existing system (for example – medical files) in accordance with the required standards (Dicom, PDF, txt, HL7, XML in X-rays etc) b. b. Receiving data from existing systems and loading it (for example – demographic data) in two possible ways: i. Receiving a file from an operative system for example a demographic data file. ii. ii. Using Web Service for the purpose of receiving demographic data from the operative system.		
2	The transfer of data must support a full and frequent transfer (at a rate of at least an item of data for a minute) of the parameters defined as obligatory, according to the medical staff.		
3	The connectivity should be modifiable and adjustable according to demands of the Medical Center and suitable to existing interfaces.		
4	The Medical Device will be connected to Medical Center network using standard RJ-45 network connection (preference to Device that has POE ability)		
5	All the connections and execution of scripts and commands, that interacts with interfaces to the Sheba network is the responsibility of the company and its exclusive handling with the software providers including the specification of the interfaces, development required from all sides (including the medical file suppliers, such as iMDsoft and ELAD Systems) and the financial costs for development required from both sides. While conducting characterization of interfaces, the company is obligated to expose the protocol which used for operation.		
6	In case that the solution is implemented by the company on another site, the supplier have to elaborate regarding the implementation of the system and about the manner in which the connectivity was executed.		
7	Supplier must provide PC\Server "Gateway" to withheld proper connection to Hospital network and its systems. **Components, like: capsules, DIGI or Lantronix are not allowed!**		
8	Information transferred to MRS (medical record system)		
9	Elaboration to which MRS the Medical device will upload data (PACS, RIS, EMR, etc.): _____	***	***

- Please mention, whether use of Sheba Medical Center Storage needed:
  _____

APPENDIX OF CYBER SECURITY FOR MEDICAL DEVICES

Name: _____ Signature: _____

Mark 'X' in each box, for example -

Non Acceptable	Acceptable
	X

nub		Acceptable	Unacceptable
1*	The mediation of the management interface to, or from the medical device will be encoded (according to the acceptable standard).		
2	All the default credentials (manufacturer based) existing upon access to infrastructure and to software, must be altered .		
3*	Passwords stored on Medical Device must be encrypted (not in clear text)		
4	The management interface will be secured with a complex password (Cap. Letter, symbol, number- must have two factors out of three).		
5	Is there a local firewall on Medical Device? (Choose the right answer)	**Yes**	**No**
6	If Question number five was answered "Yes", Is it possible to cancel the firewall? (Choose the right answer)	**Yes**	**No**
7*	As a default the system will be installed in Hospital secured environment protected (Dedicated VLAN) by Hospital firewall and IP will be provided by Hospital Cyber Team.		
8	List of ports (TCP/UDP) the Medical Device is using**:** _____	**********	
9*	On the device\PC\server must be installed a Sentinel One XDR existing in the organization, supports Windows, Linux, MAC OS XDR will receive regular updates, as per Sheba Medical Center policy. If the device\PC\server demands an exclusions, a document or a list of such need to be provided by the Integrator\Manufacturer.		
10*	In case paragraph 9 is not acceptable, manufacturer obliged to provide installation of third party White Listing\Application Control software, which filter allowed software by **HASH** or **Certificate**. Application control software manufacturer: _____ Application control system version: _____ • The software will be tested on site by Cyber team member, accompanied by Supplier\Manufacturer representative • Password for the software will be provided upfront, so the whitelisted software will be approved and recorded.		
11	The Medical Device will be configured with all external sockets and ports disabled as a default (such as USB and CD\DVD drive), Hospital Device Controller system will limit the connection.		
12	Each port, which is not regularly used for communication and activating the device, will be blocked by the supplier on OS or physically.		
13	Connection of layer 2 or 3 network devices (router, switch, etc.) explicitly prohibited		
14*	Third party remote connections such as TeamViewer, VNC and so on, will not be allowed and uninstalled, as per Hospital Information Security Policy, internal remote assistance can be achieved by Hospital SSL VPN system connecting to Vendors server and then to Medical device.		

Name: _____ Signature: _____

15*	It is responsibility of manufacturer/supplier to fix or migrate critical vulnerabilities announced or discovered on equipment provided.		
16	Joining the device/computer/system into a Hospital domain will provide a stronger level of security, this will be considered by the Supplier		
17*	A standard NDA conducted by Sheba Medical center will be signed by the Supplier		
18	Assuming, that the decision was to join the device/computer/system into a Hospital domain regular security updates of Microsoft from Hospital MS servers will be considered as an advantage		
19	Has a Penetration test or Risk Analysis review been conducted in last 18 months?		
20	If one of the above in paragraph 19 occurred, please provide necessary documentation that includes summary.		
21	NTP services from Hospital NTP servers will be considered as an advantage		
22	Specification document from the device/computer/system manufacturer including detailed installation of the Certificates and Anti-Virus exclusions, will be prepared by the Supplier, assuming that Manufacturer prepared those documents		
23	The Medical Device system have physical or software setting that wipes out changes, made to the system, after it restarts.	YES	NO
24	Please mention whether Medical device is in compliance with HIPAA /ISO 27799 standard or any other regulation_____	YES	NO
25	Medical Device will not be allowed to access World Wide Web	YES	NO
26	Logs collection executes on the Medical Device. If so, please provide path to logs_____	YES	NO
27	Manufacturer have elevated credentials of Admin to perform changes on MD	YES	NO
	Supplier have elevated credentials of Admin to perform changes on MD	YES	NO

Name: _____ Signature: _____

WIRELESS APPENDIX FOR MEDICAL DEVICES

Mark 'X' in each box, for example -

Non Acceptable	Acceptable
	X

nub		Acceptable	Unacceptable
1*	Connection to the wireless networks according to standard: (Choose the right answer) a) 802.11 ac (wave2) b) 802.11n		
2*	The capability of installing a Security certificate (User Certificate/Computer Certificate) Preference to – Computer Certificate. As per hospital policy we allow wireless access to internal network with 802.1x (Based on certificates only). Encryption – WPA2-AES (WPA2 with AES encryption and dynamic keys using 802.1x via Transport Layer Security (**TLS**)). Support cryptographic hash function (Secure Hash Algorithm 2) **SHA2**.		
3	Remote management (implementation and updating certificates and settings)		
4	Disabling Bluetooth		
5	Support of organizational NTP servers – an advantage		
6	Update/renewal of the Certificates automatically – An advantage.		
7	IP Multicast enabled	Yes	No
8	Approval of WIFI network card will be upon physical assessment on site		

Name: _____ Signature: _____

CONFIDENTIALITY APPENDIX

CONFIDENTIALITY AND NON-DISCLOSURE UNDERTAKING

We acknowledge that as part of our engagement with Sheba Medical Center, we will be given access to information that is of a personal, confidential and/ or proprietary nature, for example: (1) patient information, (2) personnel information, or (3) confidential business information of Sheba Medical Center and/or third parties, including third-party software and other licensed products or processes, and/or (4) trade secrets, research data ("**Confidential Information**"), for the purpose of fulfilling engagement obligations.

We, therefore agree:

- To hold all confidential information in trust and strict confidence and agree that it shall be used only for the purposes required to fulfill engagement obligations, and shall not be used for any other purpose, or disclosed to any third party.
- To keep any Confidential Information in my control or possession in a physically secure location to which only I and other persons who have signed a confidentiality agreement with Sheba Medical Center have access.
- Not to remove any Confidential Information from Sheba Medical Center unless, and to the extent that, I obtain Sheba's written pre-authorization. Whenever I am so pre-authorized, I agree to take all necessary steps to keep such Confidential Information secure and to protect such Confidential Information from unauthorized use, reproduction or disclosure.
- To maintain the absolute confidentiality of personal, confidential and proprietary information in recognition of the privacy and proprietary rights of others at all times, and in both professional and social situations.
- To comply with all privacy laws and regulations, which apply to the collection, use and disclosure of personal information.
- At the conclusion of any discussions, or upon demand by Sheba, to return all confidential information, including prototypes, code, written notes, photographs, sketches, models, memoranda or notes taken, to Sheba's possession and the responsible manager/director.
- Not to disclose confidential, personal and/or proprietary information to any employee, consultant or third party unless they agree to execute and be bound by the terms of this agreement and have been approved by Sheba Medical Center in an official, legal capacity.

We understand that a breach of confidentiality or misuse of information could result in disciplinary action up to and including immediate termination of the agreement.

Name: _____ Signature: _____

We understand that this undertaking survives the termination of the agreement relationship with Sheba Medical Center.

The laws of Israel shall govern this Undertaking and its validity, construction and effect.

We fully understand and accept responsibilities set above relating to personal, confidential and/or proprietary Information.

IN WITNESS whereof this UNDERTAKING has been executed on the date shown hereunder:

By: _____ By: _____

Date: _____ Date: _____

Position: _____ Position: _____

Name: _____ Signature: _____

CONFIDENTIALITY AND NON DISCLOSURE AGREEMENT

TO BE SIGNED BY ALL THE SUPPLIERS' EMPLOYEES

Declaration of confidentiality

Date: _____

I, the undersigned (First name and last name of the Employee): _____, I.D.Number: _____, am employed by (Name of employer): _____, and am hereby committed to undertaking the following:

1. To keep secret and not pass on, not inform, not hand over and / or bring to any person's attention, any detail and any information which shall come to my attention during my work on behalf of _____ (Name of employer) who provides services to _____, throughout said working period, or thereafter.
2. This obligation applies to all types of information, whether they are brought to my attention as part of my job/work or whether they are brought to my attention in any other way.
3. Without detracting from what is stated in Paragraph 1 as above, I hereby underdertake that for the duration of my provision of services to Sheba and also afterwards, indefinitely, I will not tell any person or entity, I will not publish and will not relinquish from my possession the information and / or all written information and / or any object or thing whether directly or indirectly to any party, including information about patients.
4. Likewise, I pledge that if I receive permission to use any of Sheba's databases I will do so solely for the purpose of providing my services to Sheba and only after receiving express, written consent from Sheba to access the databases.

Name: _____ Signature: _____

I pledge to act in accordance with the Privacy Act and any other provisions made by the law relating to this matter.

5. I hereby declare that I am fully aware that any failure on my part to fulfill my obligations, as they are stated above, is considered a criminal offense under the Penal Code (1977) and the Protection of Privacy Act (1981) and any other laws in keeping with the types of information, including the Patients' Rights Act (1996), and that I will be liable to receiving all punishments for my noncompliance, as they are designated by law.
6. The mobile phone number on which I will receive the code:

   _____.
7. Organizational Email of the employee:

   _____.

_____ _____

Date Signature of Declarant

Authorization and approval of people responsible for allowing the System (listed below) – essential. Without verified written approval, the system will be treated as NON APPROVED.

For clarifications or questions please contact: infosec@sheba.health.gov.il

Roman Korobitsyn: 054-3358913 Roy Faigel: 052-5222899 Roman Ratman: 054-6975739

Itamar Adut: 050-3562572

Name: _____ Signature: _____

Name: _____ Signature: _____