THE STATE OF ISRAEL
MINISTRY OF HEALTH
THE CHAIM SHEBA MEDICAL CENTER
Affiliated to the Tel-Aviv University
Sackler School of Medicine
TEL-HASHOMER, zip 5265601, ISRAEL

מדינת ישראל
משרד הבריאות
המרכז הרפואי המשולב ע"ש חיים שיבא
מסונף לבית הספר לרפואה ע"ש סאקלר
באוניברסיטת תל-אביב
תל-השומר, מיקוד 5265601 , ישראל

PAPPENDIX: Cyber Security demands for software and applications intended to be installed or implemented in Sheba network

Tender no._____ Date: ___/___/____

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

Cyber Security Manager name: _____ Phone: _____

Cyber Security Manager email:_____@_____

Mandatory requirements:

1. Paragraphs appointed with an asterisk (*) that won't be marked as "Acceptable" in the Appendix, **will fail** to meet basic Cyber security standards.
2. The operating system and cyber security system provided by manufacturer (for example Anti-Virus) **must be in manufacturer support for acceptable period of time**.
3. Operating systems must receive security updates according to the organization policy.
4. Applications\software installed on Standalone Device\ Computer system will not be allowed to transfer data to Hospital network, Clinical systems, storage and so on.

As an addition to filling the appendix, strongly advised to attach following documents:

1. Application detailed architecture, including all the components (security, protocols, ports, infrastructure needed and\or used, input and output required and so on…)
2. Acquired Standards documents (ISO, HIPAA, SOC and so on…)
3. Manufacturer secure development policy (SSDLC)
4. Security assessment and penetration testing reports conducted in past 18 months, whether sharing this information is not possible due to security limitations, please allow Us blank report, that includes System risk level, Report conductor and his verification.
5. DR and backup policy

Name: _____ Signature: _____

THE STATE OF ISRAEL
MINISTRY OF HEALTH
THE CHAIM SHEBA MEDICAL CENTER
Affiliated to the Tel-Aviv University
Sackler School of Medicine
TEL-HASHOMER, zip 5265601, ISRAEL

מדינת ישראל
משרד הבריאות
המרכז הרפואי המשולב ע"ש חיים שיבא
מסונף לבית הספר לרפואה ע"ש סאקלר
באוניברסיטת תל-אביב
תל-השומר, מיקוד 5265601 , ישראל

1. Infrastructure and system architecture mandatories:

PC based system:

Connection to: Hospital network | standalone | to specific PC | Cloud | Sheba Cloud

- OS and it's version_____
- OS distribution (PRO\STD)_____
- Service PACK installed_____

Server based system:

Connection to: Hospital network | standalone | to specific PC | Cloud | Sheba Cloud

- OS and it's version_____
- OS distribution (PRO\STD)_____
- Service PACK installed_____
- Microsoft support_____
- please specify OPENSSL version: _____

Mark 'X' in each box, for example -

Non Acceptable	Acceptable
	X

nu		Acceptable	Unacceptable
1.1	System will be implemented with separation between layers of application and data (part of secure development procedures for secured systems)		
1.2	Application\WEB servers and DB servers will be installed in different network segments in SMC (Sheba Medical Center)		
1.3	Servers/PC will be joint to SMC domain		
1.4	In case the System will be installed in Cloud , which is not owned by Sheba, GEO ACL will be implemented according to Sheba demands		
1.5	OnPrem server installation will be on Sheba VMWARE ESX		
1.6*	PC\Server will be pre-installed with Sheba XDR client. Whether exclusions needed, the list should be provided in front. All unneeded services, network components and OS features will be hardened by supplier/manufacturer		
1.7*	In case paragraph 1.6 will be signed as "Not Acceptable", manufacturer will provide and implement Application control (WhiteList) software, that must be approved by SMC Cyber division. The system must be able to approve file and/or services engagement by HASH or certificate and full hard drive encryption. Please state following details: Protection system name_____ Version:_____ -Protection will be defined on all drives, including detachable (USB) -Protection system will be reviewed by SMC Cyber division representative Please provide credentials to Protection system from manufacturer and the list of excludes.		
1.8	Is there an active firewall on the system? Is it possible to disable?	YES	NO

Name: _____ Signature: _____

THE STATE OF ISRAEL
MINISTRY OF HEALTH
THE CHAIM SHEBA MEDICAL CENTER
Affiliated to the Tel-Aviv University
Sackler School of Medicine
TEL-HASHOMER, zip 5265601, ISRAEL

מדינת ישראל
משרד הבריאות
המרכז הרפואי המשולב ע"ש חיים שיבא
מסונף לבית הספר לרפואה ע"ש סאקלר
באוניברסיטת תל-אביב
תל-השומר, מיקוד 5265601 , ישראל

1.9	In case there is no possibility to disable the firewall, rules needs to be configured, according to Cyber division representative guidance		
1.10	If there is a DB needed, the system needs to support SQL 2022 and newer.		
1.11	Separation of environments: production will be separated from lower environments, such as test and staging, installed on different servers , components in lower environments will not hod sensitive information.		
1.12	Operating Systems will be installed in SMC, Supplier\manufacturer will be co-operating with SMC infrastructure representatives.		
1.13	OS security updates will be installed periodically on System servers, according to organizational policy and Cyber division instructions, taking in consideration manufacturer Best practice policy.		
1.14	Servers and application hardening will be applied according to Cyber division instructions and taking in consideration manufacturer Best practice policy.		
1.15	In case large storage space required for the System – it will be provided on NAS system by SMC. **CIFS protocol support is an obligation** Please provide following details: a. Weekly storage space _____GB b. Monthly storage space _____GB c. Annual storage space_____GB		
1.16	System will support MultiShare to the storage		

2. Application and Credentials mandatories:

Please circle the applicable:

Medical record storage: locally | central DB | medical record system | cloud
System definition: logistics | LAB | treatment\diagnostics |POC

Mark 'X' in each box, for example -

Non Acceptable	Acceptable
	X

nub		Acceptable	Unacceptable
2.1*	The development will be conducted according to Secure Development standards, such as OWASP, STAR(CSA), will be subjected to Penetration testing for code review and include Dynamic Code testing.		
2.2*	The System will include mechanisms for user authentication and authorization thru AD/EntraID (LDAPS).		
2.3*	Credentials management and permissions will be role-based according to user's role in Organization and Least Privilege policy, the System will ensure' that the user is not able to bypass permissions received.		
2.4*	The System will not allow generic and default credentials, applicative users will be managed in Organizational AD.		
2.5*	The System will include input/output authorization mechanism and file filtering. The System should include Tamper Resistance mechanism as well.		
2.6	Whether the System support file upload, the System should needs to have mechanism to recognize by MIME TYPE and filter file type.		

Name: _____ Signature: _____

THE STATE OF ISRAEL
MINISTRY OF HEALTH
THE CHAIM SHEBA MEDICAL CENTER
Affiliated to the Tel-Aviv University
Sackler School of Medicine
TEL-HASHOMER, zip 5265601, ISRAEL

מדינת ישראל
משרד הבריאות
המרכז הרפואי המשולב ע"ש חיים שיבא
מסונף לבית הספר לרפואה ע"ש סאקלר
באוניברסיטת תל-אביב
תל-השומר, מיקוד 5265601 , ישראל

	As an addition – hook up to SMC file sanitization system should be considered. The Supplier should configure file limitation by file type and size. SMC file sanitization system includes file rewriting.		
2.7	In case system obliged to operate with service account, it is mandatory that the password will be at least 25 characters including complex, capital letters and numbers and service account will not have permissions to login to Operating System. The account will be set to 180 days expiration.		
2.8*	Runtime errors will be handled and not be visible to user. In case of malfunction – error messages, that will be presented to user will include required minimum level on information, in order to handle the malfunction, for example Error number. Error message will **never** include sensitive or confidential information, for example: patient\user information and\or sensitive information of configuration or System internal processes or System servers. In case applicative error has been identified and there is security error in application' the session must be **terminated** immediately and documented in logs.		
2.9*	Session idle timeout must be set to maximum of 15 minutes. There is a mandatory for configuring session idle time out on server side and the session must be terminated from the server.		
2.10*	Control and Log Management (Audit Trail). The System will implement mechanism' that will write logs into table and log user and process activities' made applicative users. The Audit Trail mechanism will be protected from change or cancellation and will alert administrators of any anomaly. Th Audit Trail will include the following details: user identity, date and time of login attempt (timestamp), System component being accessed, type of access (Read-Write-Execute) and access success or failure. The logs will be saved for 24 at least 24 months. Log table will be saved in designated instance from System DB and protected against change or deletion, segmented by credentials and for authorized personnel only.		
2.11	Monitoring: The System will support log forwarding to SIEM's, for example QRADAR.		
2.12	Whether the System\application will require external management – MFA will be mandatory. 2FA will be limited to number of tries (10 times in 5 minutes), after this kind of abuse – user will be blocked for at least 15 minutes, this can be replaced by verification mechanism applied (such as Google Captcha).		
2.13	Whether the application is internal – access attempts should be limited to 3 retries, while after unsuccessful attempts, the user will be blocked for 15 minutes.		
2.14	Installation or update/upgrade will require Cyber Division approval. Unsupervised installations are prohibited.		
2.15	System must support in software license and not dongle based.		
2.16	Files needed for update/upgrade, will be uploaded to Organization with SMC sanitization system **in front and not on installation window**, co-operating with SMC NOC team to deliver the files.		
2.17*	Administrative System credentials will be handled to Information and Digital department representative.		
2.18	Administrative interface will be secured with complex password. According to Organizational policy: password length should be at least 12 characters long' including small letters, capital letters, digits and special characters, such as #,$,* and so on. Audit Trail of activities will be saved in Log table.		

Name: _____ Signature: _____

THE STATE OF ISRAEL
MINISTRY OF HEALTH
THE CHAIM SHEBA MEDICAL CENTER
Affiliated to the Tel-Aviv University
Sackler School of Medicine
TEL-HASHOMER, zip 5265601, ISRAEL

מדינת ישראל
משרד הבריאות
המרכז הרפואי המשולב ע"ש חיים שיבא
מסונף לבית הספר לרפואה ע"ש סאקלר
באוניברסיטת תל-אביב
תל-השומר, מיקוד 5265601 , ישראל

	Administrative interface will be available **only** in SMC internal network and not in public networks and access will be limited to allowed IP's. Cloud administrative interface will be limited to Organizational IP's and Supplier\Manufacturer IP's only. MFA will be applied. Administrative login will be with designated employee user and not with login account.		
2.19	There is a mandatory to alter default credentials of Supplier and Manufacturer on the System.		
2.20*	Local Admin accounts will be disabled or they permissions will be minimized to servers and/or endpoints, on which the System will be installed.		
2.21	Credentials\Security keys will **not** be stored in clear text but secured and encrypted in designated storage or vault.		
2.22*	In case update\upgrade of admin interface exists, login to it will be to authorized personnel and according to pre-set permissions.		
2.23	Disclosure of sensitive information in Headers should be disabled and secured Headers needs to be added. Following links can be used for assistance: Removing Headers: https://owasp.org/www-project-secure-headers/ci/headers_remove.json Adding Headers: https://owasp.org/www-project-secure-headers/ci/headers_add.json		
2.24*	Following methods should be blocked, such as: OPTIONS TRACE HEAD PROPFIND COPY LOCK UNLOCK PROPPATCH MKCOL MOVE DELETE		
2.25	Following options should be revoked: Null ciphers, anonymous ciphers and disable RC4 encryption suite.		
2.26	Print spooler service should be disabled		
2.27	IPv6 disabled		
2.28	Disabled and revoked protocols engagement will be possible according to SMC Cyber Division approval.		
2.29	Open SSH will be uninstalled		
2.30	Please state JQUERY updated version_____		
2.31	On LINUX machines BOOT folder will be limited to READ ONLY		
2.32	Tokens will be at least 20 characters long, must be encrypted with appropriate and up-to-date encryption mechanism. The token on server side should be verified.		
2.33	Directory Listing – verification must be conducted, that support of Directory Listing by the Web Server is disabled for all the libraries under the root library.		
2.34	Mandatory to block access to all 'git' folders and files in those folders (relevant to sites managed by Open GIT).		
2.35	Cross Site Scripting protection mechanism must be implemented: • Modern framework that includes defense against XSS vulnerabilities must be used. • Please apply verification that input in designated fields are being examined, substantial risk characters are neutralized or dropped. • Strongly advised to execute Output Encoding, while data of one of the user presented to another user.		

Name: _____ Signature: _____

THE STATE OF ISRAEL
MINISTRY OF HEALTH
THE CHAIM SHEBA MEDICAL CENTER
Affiliated to the Tel-Aviv University
Sackler School of Medicine
TEL-HASHOMER, zip 5265601, ISRAEL

מדינת ישראל
משרד הבריאות
המרכז הרפואי המשולב ע"ש חיים שיבא
מסונף לבית הספר לרפואה ע"ש סאקלר
באוניברסיטת תל-אביב
תל-השומר, מיקוד 5265601 , ישראל

	• In case the user obliged to ability to insert HTML code, it is strongly advised to use HTML sanitization.		
2.36	SQL Injection protection mechanism must be implemented: • Strongly advised not to allow dynamic SQL query build • Please implement "Protected Statements" mechanism • Please implement "Properly Constructed Stored Procedures" mechanism • Please implement "AllowList Input Validation" mechanism • Strongly advised to use Escaping for every input received from User • Permissions should be implemented and enforced by Least Privilege method		
2.37*	It is **not** allowed to use GET method for transferring sensitive information. POST method must be applied with encryption (standard SHA256 can be put to use)		

3. Communications Mandatory

Mark 'X' in each box, for example -

Non Acceptable	Acceptable
	X

number		Acceptable	Unacceptable
3.1	List of Ports (TCP\UDP) used by System_____ Please state every port usage purpose.		
3.2*	Allowed protocol usage is for secured protocols only, for example HTTPS and not HTTP.		
3.3	Organizational certificates from CA will be implemented SHA2 4096bit for System use.		
3.4*	The System will be configured without connection to destinations external to Organization, unless it was specifically approved by SMC.		

4. Connectivity Mandatory

Name: _____ Signature: _____

THE STATE OF ISRAEL
MINISTRY OF HEALTH
THE CHAIM SHEBA MEDICAL CENTER
Affiliated to the Tel-Aviv University
Sackler School of Medicine
TEL-HASHOMER, zip 5265601, ISRAEL

מדינת ישראל
משרד הבריאות
המרכז הרפואי המשולב ע"ש חיים שיבא
מסונף לבית הספר לרפואה ע"ש סאקלר
באוניברסיטת תל-אביב
תל-השומר, מיקוד 5265601 , ישראל

number		Acceptable	Unacceptable
4.1	In case the System was implemented by the Supplier in another organization, please elaborate on implementation method and connectivity assimilation.		
4.2	I n case the data transferred to a clinic system, please state to which system (PACS, EMR and so on)_____		
4.3	Interfaces will support secure and encrypted connection, using such protocols as: KERBEROS, LDAPS, TLS 1.2 and above…		
4.4	The system will connect to AD using Kerberos or LDAPS		
4.5	Organizational certificates will be implemented on the System SHA2 4096bit		
4.6*	Cooperation between various system components will be protected by authentication with organizational AD applicative user account.		
4.7	The System must provide and support following options (all costs for implementation and development will be applied on Supplier): 1. Data transition to existing systems (EMR, PACS …) will be according to industry acceptable standards (DICOM, TXT, PDF, FHIR). 2. System will support receiving data from existing systems, for example demographic information, in one of 2 options: 2.1 Reception as a file from designated system. 2.2 Reception of data using WebService from designated system.		
4.8	Data transition must support full and frequent (at least once a minute) transition of parameters, defined by medical staff as mandatory.		
4.9	Connectivity must be subjected to alteration and adjustment, according to SMC organizational demands and existing interfaces.		
4.10	All configurations of interfaces to SMC systems will be Supplier's responsibility and handled exclusively by software suppliers, including interfaces characterization, development (systems by Elad software, IMDSoft, Softov and so on..) and financial matters for all of the above. Protocol used for interfaces will be disclosed to SMC representatives.		
4.11*	Sensitive data encryption will be implemented, using **strong** encryption protocol.		
4.12	API security is an mandatory and Supplier's responsibility for implementation. Designated third party product must be used to secure API requests.		

Name: _____ Signature: _____

THE STATE OF ISRAEL
MINISTRY OF HEALTH
THE CHAIM SHEBA MEDICAL CENTER
Affiliated to the Tel-Aviv University
Sackler School of Medicine
TEL-HASHOMER, zip 5265601, ISRAEL

מדינת ישראל
משרד הבריאות
המרכז הרפואי המשולב ע"ש חיים שיבא
מסונף לבית הספר לרפואה ע"ש סאקלר
באוניברסיטת תל-אביב
תל-השומר, מיקוד 5265601 , ישראל

5. Cyber Security demands and instructions

Mark 'X' in each box, for example -

Non Acceptable	Acceptable
	X

number		Acceptable	Unacceptable
5.1	Connection of a router, hub or any other network component to device/PC/server is forbidden.		
5.2*	All third party remote management software will be disabled\uninstalled.		
5.3*	Connection to SMC for support purposes will be through an organizational VPN-SSL system with 2FA and "supplier approval" mechanism. The Supplier must sign NDA and the connection will be from Israel or designated static IP address abroad, provided to Cyber Division for firewall configuration.		
5.4*	Whether the system will possess personal protected information (as defined in Private Information Protection Law), the System will comply to every Standard in this Law and will be subjected to Privacy Officer approval.		
5.5*	Security assessments and Penetration testing will be conducted. System "kick-off" will be subjected to Cyber Division approval and correction of risks found in assessments and PT.		
5.6	If the Supplier/Manufacturer conducted Security assessments and/or Penetration tests, please allow SMC Cyber Division review of those if possible. In case there is no such possibility, please disclose whether medium or higher risks were found and fixed or planned to be fixed before implementation in SMC and commitment for lower risks to be fixed at maximum period of 3 months.		
5.7*	In case a certain vulnerability/threat will be categorized by Cyber Division as critical – it will oblige the Supplier/Manufacturer to eliminate immediately. *Categorization of vulnerability/threat will be conducted according to Security Threat assessment of SMC.		
5.8*	Once the PT or Security assessment will be completed and vulnerabilities/threats will be found – it is Supplier responsibility to fix those, both technical and financial. This will be as a part of commitment to supply secured solution, according to principals of SDLC (secure development cycle), which **are undivided part of agreement mandatories.**		
5.9*	Sensitive technical data will be stored in private secured safe and not in public/supplier accessible storage. *Sensitive technical data, such as architecture documentation protocols, credentials, configuration files and hardening data and so on…		

Name: _____ Signature: _____

THE STATE OF ISRAEL
MINISTRY OF HEALTH
THE CHAIM SHEBA MEDICAL CENTER
Affiliated to the Tel-Aviv University
Sackler School of Medicine
TEL-HASHOMER, zip 5265601, ISRAEL

מדינת ישראל
משרד הבריאות
המרכז הרפואי המשולב ע"ש חיים שיבא
מסונף לבית הספר לרפואה ע"ש סאקלר
באוניברסיטת תל-אביב
תל-השומר, מיקוד 5265601 , ישראל

6. Mandatories for connecting additional components/IOT/controllers – Fill only if this section relevant to the System

number		Acceptable	Unacceptable
6.1	All connectivity issues will be made through technologies allowed and used by Digital Department, without using third party software.		
6.2	Connecting external is not allowed, in case there is a connection, it will be disconnected before connecting the System/PC to SMC network.		
6.3	If more than one network card exists on the system, please state the usage of every card.		
6.4	All hardware, OS, application upgrades/updates – files will be presented to SMC upfront for sanitization purposes. Installation will be scheduled and in present of SMC representative.		
6.5	A Gateway to connect supplied controller to SMC network will also be supplied by Supplier.		
6.6	Please state a system to which data will be transferred (A\C control, Electric, Lights and so on…)		
6.7	Connection to the management interface of all connected equipment will be encrypted (complying to the industry standards).		
6.8	All default credentials on hardware and in applications must be altered.		
6.9	All the credentials on equipment components **will not** be stored in clear text and stored encrypted.		
6.10	Management interface will be protected by complex password, according to Organizational policy.		
6.11	Hardware components will be connected to SMC network to designated VLAN and configured with organizational IP's, behind a firewall.		
6.12	Please state ports System uses TCP/UDP_____		
6.13	Supplied Controleer/PC/Server will be preinstalled with Organizational XDR by SMC representatives. OS support will be responsibility of System Manufacturer, XDR updates will be according to Organizational policy. Please attach list of needed exclusions.		
6.14	In case paragraph 6.13 is marked as "Unacceptable", The manufacturer will provide third party Application Control, allowing files and processes by HASH or certificates. Please state following details: Apllication Control system_____ version____		

Name: _____ Signature: _____

THE STATE OF ISRAEL
MINISTRY OF HEALTH
THE CHAIM SHEBA MEDICAL CENTER
Affiliated to the Tel-Aviv University
Sackler School of Medicine
TEL-HASHOMER, zip 5265601, ISRAEL

מדינת ישראל
משרד הבריאות
המרכז הרפואי המשולב ע"ש חיים שיבא
מסונף לבית הספר לרפואה ע"ש סאקלר
באוניברסיטת תל-אביב
תל-השומר, מיקוד 5265601 , ישראל

	• Protection will be applied on all existing drives and include block of external drives attachment • The Protection will be reviewed and approved by SMC Cyber Division and Supplier . • Supplier/Manufacturer **must** provide to SMC credentials for the protection.		
6.15	Hardware components will be provided with external drive connection disabled, such as USB, CD drive and so on. Updates/Upgrades must be scheduled with Digital Department representatives.		
6.16	In case a vulnerability/threat will be announced by SMC Digital Department on Controller/Device/PC or on connected server – responsibility of Supplier/ Manufacturer to address to it immediately.		
6.17	Please state whether Penetration testing and/or Risk assessment has been conducted at past 18 months.		
6.18	If possible provide SMC with results of Penetration testing and/or Risk assessment that has been conducted.		
6.19	NTP-System will be synchronized by SMC NTP.		
6.20	Does the System possesses mechanism of reset to default configuration after restart?		
6.21	Does the hardware component comply to HIPAA/ISO 27799		
6.22	Does the controller have Logging mechanism? Please provide path to logs_____		
6.23	Does the Manufacturer have admin access to make changes to the controller?		
6.24	Does the Supplier have admin access to make changes to the controller?		
6.25	By signing the Agreement, the Supplier obliged to comply to all Cyber security demands, according to SMC policy and all changes and\or additions to it, which will occur from time to time.		

Name: _____ Signature: _____

THE STATE OF ISRAEL
MINISTRY OF HEALTH
THE CHAIM SHEBA MEDICAL CENTER
Affiliated to the Tel-Aviv University
Sackler School of Medicine
TEL-HASHOMER, zip 5265601, ISRAEL

מדינת ישראל
משרד הבריאות
המרכז הרפואי המשולב ע"ש חיים שיבא
מסונף לבית הספר לרפואה ע"ש סאקלר
באוניברסיטת תל-אביב
תל-השומר, מיקוד 5265601 , ישראל

7. Characterization of mandatory Cyber demands for AI components- fill if relevant

number	Query	Response
7.1	Please state model type: LLM\ML\NLP	
7.2	Does the model engaged locally or on Cloud?	
7.3	Is there a need to open from the organization to external addresses?	
7.4	What data is used to train the model?	
7.5	Is there access control implemented for model files?	
7.6	Does the model trained or will be trained with SMC data?	
7.7	Is a model based on "Mass Sharing"?	
7.8	Does the processing of data requires sensitive information (PII\PHI)?	
7.9	While working with the model, is there anonymization mechanism being used?	
7.10	Is there a mechanism protecting against Prompt Injection? Please elaborate affirmative answer.	
7.11	Is there a mechanism for data filtration? Please elaborate affirmative answer.	
7.12	Is there periodical integrity review of Model results?	
7.13	Is there a proper versions registration procedure?	
7.14	Is there a possibility for Logs upload to Centralized SIEM?	
7.15	All sensitive data transfer, storage or processing will be accompanied with latest encryption technologies.	
7.16	Unauthorized access prevention: access with a use of AI technologies will require limitation to authorized personnel with carefully managed permissions.	

Name: _____ Signature: _____

THE STATE OF ISRAEL
MINISTRY OF HEALTH
THE CHAIM SHEBA MEDICAL CENTER
Affiliated to the Tel-Aviv University
Sackler School of Medicine
TEL-HASHOMER, zip 5265601, ISRAEL

מדינת ישראל
משרד הבריאות
המרכז הרפואי המשולב ע"ש חיים שיבא
מסונף לבית הספר לרפואה ע"ש סאקלר
באוניברסיטת תל-אביב
תל-השומר, מיקוד 5265601 , ישראל

8. Characterization of mandatory Cyber demands for Cloud - fill if relevant

number	Query	Response
8.1	Architecture of implementation Sheba Cloud\ External Cloud\ Hybrid	
8.1.1	External Cloud – Single Tenant\ Multi Tenant	
8.1.2	External Cloud – Sheba data stored in secluded location?	
8.1.3	External Cloud – List of protection mechanisms WAF\DDOS\API security and so on…	
8.1.4	Authentication – external or connected to Sheba authentication mechanisms	
8.1.5	Active MFA mechanism (APP\SMS\Mail\Voice)	
8.2	User community (Infra \ Med staff \ patients)	
8.3	Classification of Data processed\ stored	
8.4	Data transfer mechanism and channel (APN\VPN\Other)	
8.5	Data security mechanisms in transit \ at rest	

For every question or clarification Cyber Division contact details are:
CSTP@sheba.gov.il

Please note that without written approval from Cyber Division – this appendix is not authorized and the System\ Software\ Application is not authorized for use Sheba Medical Center (SMC). Without verified written approval, the system will be treated as NON APPROVED.

Name: _____ Signature: _____

THE STATE OF ISRAEL
MINISTRY OF HEALTH
THE CHAIM SHEBA MEDICAL CENTER
Affiliated to the Tel-Aviv University
Sackler School of Medicine
TEL-HASHOMER, zip 5265601, ISRAEL

מדינת ישראל
משרד הבריאות
המרכז הרפואי המשולב ע"ש חיים שיבא
מסונף לבית הספר לרפואה ע"ש סאקלר
באוניברסיטת תל-אביב
תל-השומר, מיקוד 5265601 , ישראל

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.

Name: _____ Signature: _____

THE STATE OF ISRAEL
MINISTRY OF HEALTH
THE CHAIM SHEBA MEDICAL CENTER
Affiliated to the Tel-Aviv University
Sackler School of Medicine
TEL-HASHOMER, zip 5265601, ISRAEL

מדינת ישראל
משרד הבריאות
המרכז הרפואי המשולב ע"ש חיים שיבא
מסונף לבית הספר לרפואה ע"ש סאקלר
באוניברסיטת תל-אביב
תל-השומר, מיקוד 5265601 , ישראל

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.

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 case needed, please fill Information Security representative, should be contacted:

Surname_____ First Name_____

Email_____@_____ Cell Number_____

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

By: _____ By: _____

Date: _____ Date: _____

Position: _____Position: _____

Name: _____ Signature: _____

THE STATE OF ISRAEL
MINISTRY OF HEALTH
THE CHAIM SHEBA MEDICAL CENTER
Affiliated to the Tel-Aviv University
Sackler School of Medicine
TEL-HASHOMER, zip 5265601, ISRAEL

מדינת ישראל
משרד הבריאות
המרכז הרפואי המשולב ע"ש חיים שיבא
מסונף לבית הספר לרפואה ע"ש סאקלר
באוניברסיטת תל-אביב
תל-השומר, מיקוד 5265601 , ישראל

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. This obligation is to take all precautions and to apply all needed from safety, procedural, security or any other aspect.
4. Without detracting from what is stated in Paragraph 1 as above, I hereby undertake 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.
5. 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

Name: _____ Signature: _____

THE STATE OF ISRAEL
MINISTRY OF HEALTH
THE CHAIM SHEBA MEDICAL CENTER
Affiliated to the Tel-Aviv University
Sackler School of Medicine
TEL-HASHOMER, zip 5265601, ISRAEL

מדינת ישראל
משרד הבריאות
המרכז הרפואי המשולב ע"ש חיים שיבא
מסונף לבית הספר לרפואה ע"ש סאקלר
באוניברסיטת תל-אביב
תל-השומר, מיקוד 5265601 , ישראל

after receiving express, written consent from Sheba to access the databases. I pledge to act in accordance with the Privacy Act and any other provisions made by the law relating to this matter.

6. 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 non-compliance, as they are designated by law.
7. The mobile phone number on which I will receive the code: _____.
8. Organizational Email of the employee: _____.

_____ _____

Date Signature of Declarant

For every question or clarification Cyber Division contact details are:
CSTP@sheba.gov.il

Name: _____ Signature: _____