

## נספח דרישות מחשוב והגנת הסייבר לחיבור מכשירים

### רפואיים לרשת שיבא ו/או לקבלת נתונים ממכשירים רפואיים

הנחיות למילוי הנספח :

1. לכל דגם מכשיר / מחשב / ציוד נלווה נדרש למלא נספח.
2. על כל ספק / יצרן למלא את הנספח במלואו.
3. לשאלות והסברים ניתן לפנות למנהל הפרוייקט בשיבא או למייל [IoMTCS@sheba.health.gov.il](mailto:IoMTCS@sheba.health.gov.il)
4. חיבור המכשיר יבוצע לאחר אישור צוות הגנת הסייבר ל-IOT בלבד.
5. נספח זה תקף גם להחלפת מכשיר תקול מדגם שונה.
6. המכשיר יחובר ל-VLAN ייעודי בהתאם לסוגו וייעודו.
7. גישה אל או מהאינטרנט תהיה חסומה באופן יזום.
8. ביקורות תקופתיות יבוצעו ע"י צוות הגנת הסייבר ל-IOT על מנת לוודא שלא השתנו הגדרות ו/או נוספו מכשירים חדשים או יכולות חדשות. מכשיר שלא יעמוד בתנאים שמולאו בנספח זה ינותק מהרשת.

### דרישות סף:

- סעיפים עם כוכבית (\*) – סעיף שלא יסומן כמקובל לא יעמוד בדרישות הסף.
- מערכות הפעלה ומערכות הגנה צריכות להיות **בתמיכת יצרן**.
- מערכות הפעלה יקבלו עדכוני אבטחה באופן שוטף בהתאם למדיניות הארגון.
- מכשיר/מחשב שיוגדר ע"י הספק כ Stand Alone מחויב לקבל אישור ע"י המחלקה/מכון/מרפאה והנדסה רפואית ויצורף לנספח מחשוב זה.
- מחשב/מכשיר שהוגדר כ Stand Alone אינו יורשה להעביר נתונים לרשת בית החולים, למערכות קליניות, אחסון וכדומה.

מספר מכרז: \_\_\_\_\_ תאריך: \_\_\_\_\_  
 מהות המכשיר: \_\_\_\_\_ שם היצרן: \_\_\_\_\_  
 דגם המכשיר: \_\_\_\_\_ שם הספק: \_\_\_\_\_  
 שם ממלא הטופס: \_\_\_\_\_ סולר: \_\_\_\_\_  
 מייל ממלא הטופס: \_\_\_\_\_ @ \_\_\_\_\_

**מנהל פרוייקט מטעם שיבא (מערכות מידע/הנדסה רפואית/מנהל מחלקה):**

### תקציר קישוריות:

1. על-מנת להבטיח את הקשר המיטבי בין המערכת המוצעת ובין מערכות המידע של שיבא, יבוא המציע בדברים עם בית התוכנה המתאים (ר' להלן), ויגיש כחלק מהמענה למכרז, אישור בחתימת בית התוכנה, המעיד על תאימות המוצר המוצע לתוכנה בשיבא שתקבל ממנו נתונים. האישור יבהיר אם מדובר בתאימות בעלת ניסיון מוכח או רק בעמידה בסטנדרטים שיאפשרו ליצור ממשק חדש. על ספק המערכת/המכשיר המוצע לפרט ממשקים רלוונטיים מול מנהל הפרוייקט בשיבא.
  - מכל מקום, הזכייה במכרז תותנה בהוכחה בפועל של תאימות זו.
  - מכל מקום, הממשקים האמורים במלואם יהיו כלולים בהצעת המחיר של הספק.
  
2. המציע יפרט את הממשקים שיספק בין המוצר המוצע ובין מערכות המידע של שיבא, לרבות:
  - 2.1. קליטת נתוני מטופלים ממערכות שיבא
  - 2.2. העברת נתונים מן המערכת המוצעת אל מערכות שיבא.
  - 2.3. המציע יפרט:
    - סטנדרטים
    - פורמטים
    - פירוט המידע שעובר ואופן העברתו
    - הטריגר להעברת המידע
    - יכולת עצמית לזיהוי מטופל
    - יכולת התחברות ל-ACTIVE DIRECTORY
    - אגירת מידע מקומית והתנהלות ללא תקשורת
    - יכולת העברת נתונים למערכות BI ול-DATA LAKE (בנוסף להעברה לתוכנה הרלוונטית מסעיף 1)
    - תנאים ומגבלות
    - בתי חולים שבהם פועלים הממשקים המוצעים
    - כל מידע רלוונטי נוסף הנוגע לממשקים.

### נספח מכשיר רפואי:

נא להקיף בעיגול:

- מחובר - לרשת בית החולים | Stand Alone | למחשב ייעודי | ענן של שיבא | ענן חיצוני
- שומר נתוני מטופלים - מקומית בלבד | באחסון מרכזי | במערכת קלינית | אינו שומר
- בשימוש - משקי | מעבדתי | טיפולי/דיאגנוסטי | להתנסות זמנית
- גישה למכשיר לצורכי תחזוקה וטיפול - מהארץ | חו"ל | אין צורך

1. יש לציין את מערכת הפעלה: \_\_\_\_\_
- 1.1 גרסת מערכת הפעלה: \_\_\_\_\_
- 1.2 סוג מערכת הפעלה כגון (Pro/Embedded): \_\_\_\_\_
- 1.3 יש לציין איזה Service Pack/Patch/Build מותקן: \_\_\_\_\_
- 1.4 אם מדובר במערכת הפעלה 7/10 יש לספק תאריך סיום תמיכה ממיקרוסופט: \_\_\_\_\_
- 1.5 במידה ומוותקן נא לציין גרסת OPENSSL: \_\_\_\_\_

מקובל	לא מקובל
x	

ממ X בכל משבצת בטבלה, דוגמא -

מס"ד	מקובל	לא מקובל
2		שם משתמש וסיסמא בעלי הרשאת גישה של Administrator יועברו לנציגי אגף מערכות מידע ודיגיטל (לממשק, מערכת, אפליקציה או מחשב).
3		לא יותקן מודם/HUB או כל ציוד תקשורת צד ג' בתחנה. במידה ומוותקן מודם הוא יוסר לפני חיבור לרשת שיבא - באחריות הספק, במידה ויש צורך במודם לתפעול השוטף של המערכת יש לפנות למנהל אבטחת מידע הארגוני.
4		כל נושא חיבור מרחוק יבוצע דרך מערכת SSL VPN ארגוני מול אגף מערכות מידע ודיגיטל בלבד ללא תוכנות צד שלישי
5		מכשיר עם 2 כרטיסי רשת ומעלה יאושר רק לאחר בדיקה של צוות הגנת הסייבר IoT
*6		כל עדכון לחומרה, מערכת הפעלה, אפליקציה וכו' יש לבצע הלבנה לקבצי התקנה בתיאום מראש עם אגף מערכות מידע ודיגיטל. שדרוג המכשיר/המערכת יתבצע בתיאום מול המחלקה ומנהל הפרוייקט.
7		במידה ומכשיר יחובר לדומיין שיבא, יבוצע שינוי שם מחשב על פי כללי מרכז הרפואי שיבא
8		האם ניתן להוסיף משתמש מדומיין שיבא אשר יוקם לטובת המערכת ויבצע Login למחשב

**נספח מחשב המחובר למכשיר ו/או לרשת בית החולים (ימולא עבור מערכות שמחשב ומכשיר לא כחידה אחת):**

נא להקיף בעיגול:

- **מחובר** - לרשת בית החולים | Stand Alone | למכשיר ייעודי | ענן של שיבא | ענן חיצוני
- **שומר נתוני מטופלים** - מקומית בלבד | באחסון מרכזי | במערכת קלינית | אינו שומר
- **בשימוש** – משקי | מעבדתי | טיפולי/דיאגנוסטי | להתנסות זמנית
- **גישה למחשב לצורכי תחזוקה וטיפול** – מהארץ | חו"ל | אין צורך

1. יש לציין את מערכת ההפעלה: \_\_\_\_\_
- 1.1. גרסת מערכת הפעלה: \_\_\_\_\_
- 1.2. סוג מערכת הפעלה כגון (Pro/Embedded): \_\_\_\_\_
- 1.3. יש לציין איזה Service Pack/Patch/Build מותקן: \_\_\_\_\_
- 1.4. אם מדובר במערכת הפעלה 7/10 יש לספק תאריך סיום תמיכה ממיקרוסופט: \_\_\_\_\_
- 1.5. במידה ומותקן נא לציין גרסת OPENSLL: \_\_\_\_\_

מקובל	לא מקובל
x	

סמן X בכל משבצת בטבלה, דוגמא -

מס"ד	מקובל	לא מקובל
2		שם משתמש וסיסמא בעלי הרשאת גישה של Administrator יועברו לנציגי אגף מערכות מידע ודיגיטל (לממשק, מערכת, אפליקציה או מחשב).
3		לא יותקן מודם/HUB או כל ציוד תקשורת צד ג' בתחנה, במידה ומותקן מודם הוא יוסר לפני חיבור לרשת שיבא – באחריות הספק, במידה ויש צורך במודם לתפעול השוטף של המערכת יש לפנות למנהל אבטחת מידע הארגוני.
4		כל נושא חיבור מרחוק יבוצע דרך מערכת SSL VPN ארגוני בלבד ללא תוכנות צד שלישי
5		מכשיר עם 2 כרטיסי רשת ומעלה יאושר רק לאחר בדיקה של צוות הגנת הסייבר OT
*6		כל עדכון לחומרה, מערכת ההפעלה, אפליקציה וכו' יש לבצע הלבנה לקבצי התקנה בתיאום מראש עם אגף מערכות מידע ודיגיטל. שדרוג המכשיר/המערכת יתבצע בתיאום מול המחלקה ומנהל הפרוייקט.
7		במידה ומכשיר יחובר לדומיין שיבא, יבוצע שינוי שם מחשב על פי כללי מרכז הרפואי שיבא
8		האם ניתן להוסיף משתמש מדומיין שיבא אשר יוקם לטובת המערכת ויבצע Login למחשב

### נספח אחסון ושרתים:

#### במידה ונדרש שרת מערכת נא למלא טופס הקמת שרת בנוסף לנספח זה.

1. יש לציין את גרסת מערכת ההפעלה: \_\_\_\_\_
- 1.1. סוג מערכת הפעלה כגון: (Pro/STD): \_\_\_\_\_
- 1.2. יש לציין איזה Service Pack מותקן: \_\_\_\_\_
- 1.3. במידה ומוחקן נא לציין גרסת OPENSSL: \_\_\_\_\_
- 1.4. נא לציין גרסת IIS/Apache במידה ומוחקן: \_\_\_\_\_

מקובל	לא מקובל
X	

סמן X בכל משבצת בטבלה; דוגמא -

מס"ד	מקובל	לא מקובל
2		השרת יותקן וירטואלית תחת VMWARE ESX .
3		מערכת הפעלה תותקן במרכז הרפואי ע"י הצוות של אגף מערכות מידע ודיגיטל ( ביחד עם הספק)
4		במידה ויידרש מערך אחסון גדול לארכיון השטח יסופק בתצורת NAS , חובה תמיכה בפרוטוקול CIFS <u>יש לציין את הפרטים הבאים:</u> 1. גודל השטח שבועי: _____ GB 2. גודל שטח חודשי: _____ GB 3. גודל שטח שנתי: _____ GB
5		תמיכה בעבודה מול האחסון ב Multi Share
6		תמיכה ברישיון תוכנתי דיגיטלי ולא דרך דונגל פיסי (אין אישור לחיבור התקן USB).
7		במידה והמערכת עובדת מול בסיס נתונים, על הספק לתמוך ב SQL 2019 ומעלה.
8		האפליקציה מחויבת לעבוד רק עם User Service ולא עם User Logon . כל השירותים הקשורים לאפליקציה יעבדו עם משתמש ייעודי אפליקטיבי.
*9		השרת יותקן עם מערכת הגנה XDR הקיים בשיבא ויתעדכן אוטומטית באופן שוטף.
10		כל עדכון לחומרה, מערכת ההפעלה, אפליקציה וכו' יש לבצע הלבנה לקובצי התקנה בתיאום מראש עם אגף מערכות מידע ודיגיטל. שדרוג המכשיר/המערכת יתבצע בתיאום מול המחלקה ומנהל הפרוייקט.
11		המערכת תתחבר לדומיין ארגוני מול Active Directory בפרוטוקול LDAPS ו- Kerberos

**נספח קישוריות:**

מס"ד	מקובל	לא מקובל
1		המערכת חייבת לספק ולתמוך באפשרויות הקישור הבאות (עלויות החיבור תהיינה על הספק): (a) העברת נתונים למערכות קיימות (לדוגמא - תיקים רפואיים, אוטולימס) בהתאם לסטנדרטים מקובלים (FHIR, txt, PDF, Dicom בצילומים ועוד) (b) קבלת נתונים ממערכות קיימות וטעינתם (לדוגמא - נתוני דמוגרפיה) בשתי צורות אפשריות: i קבלת קובץ מהמערכת התפעולית לדוגמא קובץ נתוני דמוגרפיה ii שימוש ב ווב סרוויס לצורך קבלת נתוני דמוגרפיה מהמערכת התפעולית
2		העברת נתונים חייבת לתמוך בהעברה מלאה ותכופה (בקצב של נתון בדקה לפחות) של הפרמטרים המוגדרים כחובה על פי הצוות הרפואי.
3		הקישוריות אמורה להיות ניתנת לשינוי ולהתאמה בהתאם לדרישות המרכז הרפואי ולממשקים הקיימים
4		המכשיר הרפואי יחובר ישירות לרשת שיבא באמצעות כרטיס רשת (העדפה ל- POE)
5		כל המשתמע מביצוע הממשקים למערכות שיבא הינו באחריות החברה ובטיפול הבלעדי מול ספקיות התוכנה לרבות אפיון הממשקים, פיתוחים הנדרשים מכל הצדדים (כולל ספקי התיק הרפואי, כגון: iMDsoft ואלעד מערכות, סופטוב) וההוצאות הכספיות בגין העבודה הנדרשת משני הצדדים. במסגרת אפיון הממשקים החברה תתחייב לחשוף את הפרוטוקול איתו היא עובדת.
6		במידה והפתרון יושם ע"י החברה באתר אחר, על הספק לפרט לגבי ההטמעה של המערכת וכן על אופן הקישוריות כפי שבוצע.
7		על הספק לספק מחשב/שרת Gateway על מנת לחבר את המכשיר לרשת בית החולים. <b>רכיבים כגון: קפסולות, DIGI, לנטרוניקס לא מאושרים בבית חולים.</b>
8	כן	לא האם מידע מועבר למערכת קלינית? כל העברת מידע למערכת קלינית דורשת את אישור מנהל הפרוייקט.
9	***	*** במידה ומידע מועבר למערכת קלינית יש לציין לאיזו מערכת (כגון: קמיליון, פאקס וכו')

**נספח אבטחת מידע, הגנת הסייבר ופרטיות:**

מס"ד	מקובל	לא מקובל
*1		התווך לממשק הניהול של המכשיר הרפואי יהיה מוצפן (על פי תקן מקובל)
2		כל סיסמאות ברירת המחדל ( של היצרן ) ישונו בתשתיות ובאפליקציות
*3		הסיסמאות הנמצאות במכשיר לא יהיו ב- Clear Text רק בצורה מוצפנת
4		ממשק הניהול יהיה מאובטח עם סיסמא מורכבת
5	כן	לא
5		אם מופעל Firewall מקומי? (הקיפו בעיגול <input type="radio"/> את התשובה )
6	כן	לא
6		האם ניתן לבטלו? (הקיפו בעיגול <input type="radio"/> את התשובה )
7		במידה ולא ניתן לבטל Firewall מקומי. יש לבצע כללים (Rules) ב Firewall על פי הנחיית גורם אבטחת מידע בשיבא בזמן הטמעת המוצר.
*8		המכשיר יוגדר עם כתובות IP בוילן (VLAN) ייעודי ברשת בית החולים ( מאחורי Firewall ארגוני) שצוות הגנת הסייבר יספק.
9		באילו Ports (TCP/UDP) המערכת משתמשת: _____
10		מכשיר/מחשב/שרת שיוספק, יותקן עליו XDR הקיים בשיבא ע"י נציגי בית החולים ויתעדכן אוטומטית באופן שוטף. א. יש לציין החרגות במידת הצורך _____
11		במידה וסעיף 9 סומן כ "לא מקובל" על היצרן להתקין תוכנת Application Control (White List) המאשרת הפעלת קבצים לפי HASH או לפי Certificate והגנה מלאה על כל הכוננים במכשיר. <b><u>יש לציין את הפרטים הבאים:</u></b> שם המערכת: _____ גרסה: _____ • ההגנה תוגדר על כל הכוננים הקיימים הכולל חסימה על Disk on key • המוצר ייבדק ע"י נציגי צוות הגנת הסייבר (שיבא) ונציגי הספק/יצרן. יש לספק מהיצרן סיסמה למערכת ורשימת הקבצים המוחרגת.
12		המכשיר יותקן עם הגבלת רכיבים נתיקים (כגון יציאת USB   CD ). שדרוגים למערכת/תוכנה ו/או למכשיר יתואמו מראש עם אגף מערכות מידע ודיגיטל לצורכי הלבנת מדיה נתיקה (כגון: Disk on key , דיסק נייד, CD וכו'...).
13		כל פורט נוסף אשר אינו משמש לתקשורת והפעלת המכשיר באופן קבוע ייחסם ע"י הספק ברמת מערכת הפעלה או ברמה פיזית.
*14		התחברות למרכז הרפואי שיבא תל השומר תבצע ע"י מערכת SSL VPN עם אימות ID שלבי ואישור רפרנט מטעם שיבא.

**המשך נספח אבטחת מידע, הגנת הסייבר ופרטיות:**

מס"ד	מקובל	לא מקובל
*15	כן	לא
		חיבור לרשת ביה"ח דרך תוכנה צד ג' של שליטה מרחוק (לדוגמא: VNC , TeamViewer וכו'...) לא מאושר.
*16		
		המכשיר הרפואי ו/או המחשב ייסרקו במערכת ייעודית לזיהוי נזקות, פוגענים וחולשות. במידה ותמצא ע"י אגף מערכות מידע ודיגיטל חשיפה/חולשה קריטית במכשיר, מחשב ו/או בשרת המחובר אליו, על הספק/יצרן לדאוג לחסום זאת במייד.
17		
		הכנסת המכשיר/מחשב לדומיין ארגוני (כולל משתמש דומיין במצב לוגין)
*18		
		מיפוי כונן רשת לאחסון ארגוני (Storage) מחייב את הכנסת המכשיר/מחשב לדומיין הארגוני.
*19		
		על הספק לחתום על טופס סודיות בנספח "סודיות"
20		
		המכשיר יקבל עדכוני אבטחה של מיקרוסופט באופן שוטף.
21		
		האם בוצע למכשיר מבדק חדירה ו/או סקר סיכונים ב 18 חודשים האחרונים?
22		
		במידה ובוצע מבדק חדירה ו/או סקר סיכונים, האם ניתן לספק סיכום ממצאים לגורמי הסייבר במרכז הרפואי שיבא
23		
		תמיכה מול שרתי NTP הארגוני – יתרון
24		
		מסמך הגדרות של היצרן הכולל התקנה מפורטת של ה – Certificates יתרון
25	כן	לא
		האם יש מערכת שמאפסת הגדרות לאחר אתחול?
26	כן	לא
		האם המכשיר עומד בתקינה כגון: HIPAA / ISO 27799 ? נא לפרט: _____
*27		
		מכשיר רפואי יהיה ללא גישה לרשת האינטרנט
28	כן	לא
		האם יש רישום לוגים במכשיר. נא לציין היכן נרשמים הלוגים ומה סוגי הלוגים: _____ _____
29	כן	לא
		האם ליצרן יש הרשאת אדמין על המכשיר על מנת לבצע שינויים במכשיר הרפואי
30	כן	לא
		האם לספק יש הרשאת אדמין על המכשיר על מנת לבצע שינויים במכשיר הרפואי
31	כן	לא
		בחתימה על הסכם זה, הספק מתחייב לעמוד בכל דרישות אבטחת מידע וסייבר על פי המדיניות שתקבע ע"י מרכז הרפואי שיבא והממונה על אבטחת המידע תתעדכן מעת לעת

**נספח תקשורת ורשת אלחוטית:**

לא מקובל	מקובל	מס"ד
		*1 חיבור לרשתות אלחוטיות על פי תקן (הקיפו בעיגול) <input type="radio"/> את התקן הקיים אצלכם) א. 802.11ac (wave2) ב. 802.11n
		*2 יכולת התקנת תעודת אבטחה ( User Certificate/Computer Certificate ) בעדיפות ל- 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) <b>SHA2</b> .
		3 ניהול מרחוק (הטמעה ועדכון תעודות הצפנה ושינוי הגדרות)
		4 חסימת גישה בBluetooth
		5 תמיכה בשרתי NTP הארגוני – יתרון
		6 עדכון/חידוש תעודות Certificate באופן אוטומטי – יתרון
לא	כן	7 האם מופעל שידור במולטיקאסט (רב-נתיב)
		*8 אישור כרטיס ה-WIFI מותנה בבדיקה פיזית במרכז הרפואי שיבא

**נספח סודיות:**

**התחייבות לשמירת סודיות ולמניעת ניגוד עניינים-ספק**

תאריך: \_\_\_\_/\_\_\_\_/\_\_\_\_

לכבוד

המרכז הרפואי ע"ש שיבא, תל השומר

=====

א.ג.נ

**הנדון: התחייבות לשמירת סודיות ולמניעת ניגוד עניינים**

- והואיל המרכז הרפואי ע"ש שיבא, תל השומר (להלן "שיבא") מעוניין לקבל שירותים בנושא \_\_\_\_\_ עבור אגף מערכות מידע ודיגיטל בשיבא (להלן: "השירותים");
- והואיל והמציע \_\_\_\_\_ (להלן: "המציע") מעוניין להעניק שירותים אלו.
- והואיל ושיבא התנה את התקשרות שני הצדדים בתנאי שהמציע והבאים מטעמו ישמרו על סודיות כל המידע שהגדרתו להלן, וכן על סמך התחייבות המציע לעשות את כל הדרוש לשמירת סודיות המידע;
- והואיל והוסבר לי כי במהלך עיסוקי במתן השירותים לשיבא ו/או בקשר אליהם יתכן כי אעסוק ו/או אקבל לחזקתי ו/או יבוא לידיעתי מידע מסוגים שונים, שאינו מצוי בידיעת כלל הציבור, בין בעל פה ובין בכתב, בין ישיר ובין עקיף, השייך למזמין ו/או הנודע למזמין ו/או לפעילויותיו בכל צורה ואופן, לרבות אך מבלי לגרוע מכלליות האמור, נתונים, מסמכים ודו"חות (להלן: "המידע");
- והואיל והוסבר לי וידוע לי כי גילוי המידע בכל צורה שהיא לכל אדם או גוף מלבדכם, עלול לגרום לכם ו/או לצדדים שלישיים נזק, והוא עלול להוות עבירה פלילית;

### אי לזאת, אני הח"מ מתחייב כלפיכם כדלקמן:

1. לשמור על סודיות גמורה ומוחלטת של המידע ו/או כל הקשור והנובע מן השירותים או ביצועם ובפרט מידע הרפואי.
2. ומבלי לפגוע בכלליות האמור בסעיף 1 לעיל, הנני מתחייב כי במשך תקופת מתן השירותים לשיבא או לאחר מכן ללא הגבלת זמן לא אגלה לכל אדם או גוף, לא אפרסם וכן לא אוציא מחזקתי את המידע ו/או כל חומר כתוב אחר ו/או כל חפץ או דבר, בין ישיר ובין עקיף, לצד כלשהוא.
3. מבלי לפגוע בכלליות האמור לעיל, מידע סודי לא יכלול מידע שהינו נחלת הכלל או שהפך להיות נחלת הכלל ללא הפרת חובת הסודיות ו/או מידע שחובה לגלותו על פי כל דין או צו של רשות מוסמכת ו/או מידע שפותח באופן עצמאי ללא תלות במידע הסודי ו/או מידע שהתקבל בידי המציע מצד ג' כדין ללא הפרת חובת סודיות.
4. לנקוט אמצעי זהירות קפדניים ולעשות את כל הדרוש מבחינה בטיחותית, ביטחונית, נוהלית או אחרת כדי לקיים את התחייבויותי על פי התחייבות זו.
5. להביא לידיעת עובדי ו/או מי מטעמי חובה זו של שמירת סודיות ואת העונש על אי מילוי החובה.
6. להיות אחראי כלפיכם על פי כל דין לכל נזק או פגיעה או הוצאה או תוצאה מכל סוג, אשר יגרמו לכם או לצד שלישי כל שהוא כתוצאה מהפרת התחייבותי זו, וזאת בין אם אהיה אחראי לבדי בגין כל האמור ובין אם אהיה אחראי ביחד עם אחרים.
7. להחזיר לידיכם ולחזקתכם מיד כשאתבקש לכך כל חומר כתוב או אחר או חפץ שקיבלתי מכם או השייך לכם שהגיע לחזקתי או לידי עקב מתן השירותים או שקיבלתי מכל אדם או גוף עקב מתן השירותים או חומר שהכנתי עבורכם. כמו כן, הנני מתחייב לא לשמור אצלי עותק כל שהוא של חומר כאמור או של מידע.
8. שלא לעסוק בכל דרך שהיא בעיסוק שיגרום לי להיות במצב של ניגוד עניינים עם עיסוקי במתן השירותים כאמור לעיל.

9. בכל מקרה שאגלה מידע כאמור השייך לכם ו/או הנמצא ברשותכם ו/או הקשור לפעילויותיכם, תהיה לכם זכות תביעה נפרדת ועצמאית כלפי בגין הפרת חובת הסודיות שלעיל.
- הנני מצהיר כי ידוע לי ששימוש במידע שיגיע לידי במהלך ביצוע העבודה ומסירתו לאחר מהווים עבירה על פי חוק עונשין, התשל"ז - 1997 וחוק הגנת הפרטיות התשמ"א - 1981 וכן חוקים אחרים לפי סוג המידע, לרבות חוק זכויות החולה, התשנ"ו - 1996.
10. התחייבותי זו לא תפורש כיוצרת קשר אישי מכל סוג שהוא ביני לבניכם.
11. יש למלא פרטי נציג אבטחת מידע של החברה:
- 11.1 שם מלא נציג אבטחת מידע מהחברה: \_\_\_\_\_
- 11.2 מייל הנציג: \_\_\_\_\_
- 11.3 מספר סלולרי הנציג: \_\_\_\_\_

**ולראיה באתי על החתום - התחייבות לשמירת סודיות ולמניעת ניגוד עניינים**

			היום:
שנת	בחודש	יום	
			המציע:
ת"ז	שם פרטי ומשפחה		
חתימה			כתובת

### טופס הצהרה על שמירת סודיות - עובד של ספק

אני החתום מטה: (שם פרטי ומשפחה) \_\_\_\_\_ ת.ז: \_\_\_\_\_

העובד ומועסק אצל \_\_\_\_\_ (שם המעסיק), מתחייב בזאת:

1. לשמור בסוד ולא להעביר, לא להודיע, לא למסור ו/או לא להביא לידיעת כל אדם, כל ידיעה וכל מידע רגיש ו/או אישי ו/או חסוי לרבות תכנים וחומר בכתב ובעל פה, אשר יגיעו לידיעתי בתקופת עבודתי מטעם \_\_\_\_\_ (שם המעסיק) הנותן שירותים למרכז הרפואי שיבא תל השומר, בתקופת עבודתי כאמור, או לאחר מכן.
2. התחייבותי זו חלה לגבי כל סוגי המידע, בין אם יגיעו לידיעתי בתוקף עבודתי כאמור ובין אם יגיעו לידיעתי בכל דרך אחרת.
3. ומבלי לפגוע בכלליות האמור בסעיף 1 לעיל, הנני מתחייב כי במשך תקופת מתן השירותים לשיבא או לאחר מכן ללא הגבלת זמן לא אגלה לכל אדם או גוף, לא אפרסם וכן לא אוציא מחזקתי את המידע ו/או כל חומר כתוב אחר ו/או כל חפץ או דבר, בין ישיר ובין עקיף, לצד כל שהוא, לרבות מידע אודות הנבדקים.
4. כמו כן, אני מתחייב כי אם אקבל רשות להשתמש במאגרי המידע של שיבא, אעשה זאת אך ורק לצורך מתן השירותים לשיבא, ובהסכמה מפורשת בכתב מטעם שיבא. אני מתחייב לפעול בהתאם להוראות חוק הגנת הפרטיות והוראות כל חוק הנוגע לעניין.
5. אני מתחייב להתחבר ממחשב השייך לחברה שבה אני עובד ומוגן עם אנטי וירוס מעודכן, לא להוריד מידע ששייך לשיבא למחשבי החברה, אמצעים נתיקים ו/או מחשבים ניידים אלא בכפוף לאישור בכתב מאת ממונה אבטחת המידע של שיבא,
6. אין להעביר את אמצעי הזיהוי החכם שקבלתי משיבא לכל אדם אחר ולא לגלות לאף גורם את הקוד האישי (PIN) המשויך לאמצעי הזיהוי, יש להודיע מידית על אובדן אמצעי הזיהוי או חשיפת הקוד למנהל אבטחת המידע של שיבא.



7. עם סיום עבודתי אצל הספק או עם סיום הצורך בגישה מרחוק מתוקף תפקידי אני מתחייב להודיע על כך למנהל אבטחת המידע של שיבא

8. אני מצהיר בזה שידוע לי, כי אי מילוי התחייבויותי הנ"ל מהווה עבירה פלילית מכוח חוק העונשין, התשל"ז - 1977 וחוק הגנת הפרטיות התשמ"א-1981 וכן חוקים אחרים לפי סוג המידע, לרבות חוק זכויות החולה, התשנ"ו-1996 וכי אהיה צפוי לעונשים הקבועים בחוק בגין אי מילוי התחייבויותי.

9. מספר הסולרי שאליו אקבל את הקוד: \_\_\_\_\_

10. דוא"ל ארגוני של העובד: \_\_\_\_\_

\_\_\_\_\_  
חתימת המצהיר

\_\_\_\_\_  
תאריך