התכנית לתואר שני M.Sc. בניהול טכנולוגיה

הצעה למחקר בנושא:

"סיכוני סייבר במכשור רפואי"

מוגש ע"י

שם הסטודנט: פליקס קרסניצקי ת.ז.: 306012865

צבי ששון ת.ז.: 022114730

שם מנחה/ים : ד"ר הראל מנשרי ד"ר הדס לוי

[1. מבוא 4](#_Toc42335970)

[1.1. רציונל המחקר 4](#_Toc42335972)

[1.2. מטרת המחקר 5](#_Toc42335973)

[1.3. שאלות המחקר 5](#_Toc42335974)

[1.4. משתנים תלויים ובלתי תלויים 5](#_Toc42335975)

[1.5. חשיבות המחקר 5](#_Toc42335976)

[2. סקר ספרות ראשונית 6](#_Toc42335977)

[2.1. הקדמה 6](#_Toc42335978)

[2.2. סקר ספרות בנושא: אבטחת מידע והגנה על פרטיות 7](#_Toc42335979)

[2.3. סקר ספרות בנושא: איומים על מערכות מידע מגורמים זדוניים 9](#_Toc42335986)

[2.4. סקר ספרות בנושא: תשתיות, שיטות ודוגמאות לשירותים ומוצרים רפואיים 11](#_Toc42335989)

[2.5. מודל למיפוי סיכונים למכשור רפואי 14](#_Toc42335990)

[2.6. סיכום סקר הספרות 16](#_Toc42335991)

[3. מתודולוגיה ראשונית 17](#_Toc42335994)

[3.1. מערך המחקר, אוכלוסיית המחקר (אם רלבנטי – הארגונים שיכללו במחקר). 17](#_Toc42335996)

[3.2. הפרדיגמה המחקרית 17](#_Toc42335997)

[3.3. הנבדקים 17](#_Toc42335999)

[3.4. שיטת המחקר – במחקר כמותי, מה תהיה שיטת המחקר (ניסוי, סקר, מחקר קורלטיבי וכד')? 17](#_Toc42336001)

[3.5. כלי איסוף הנתונים – מדידות: היכן ואיך? שאלונים: כמה? איזה? מסמכים? סוג הראיונות (למשל, חצי מובנים) וסוג התצפיות (למשל, הצופה המשתתף) עם נימוקים להצדקתם. 17](#_Toc42336002)

[3.6. כלי מחקר נוספים (מה שרלבנטי) – סימולציות, מודלים, פיתוחים מתימטיים, תוכנות, כלי קבלת החלטות ובחירת חלופות, אלגוריתמים וכד'. 17](#_Toc42336003)

[3.7. בסקר – תכנון שלבי בניית השאלון (או השאלונים). 17](#_Toc42336004)

[3.8. ניתוח הנתונים - מה תהיה שיטת ניתוח ועיבוד הנתונים? בכמותי: כלים סטטיסטיים. באיכותי: ניתוח תוכן. 17](#_Toc42336006)

[3.9. אתיקה – דילמות אתיות ודרכי התמודדות. 17](#_Toc42336007)

[3.10. תכנון לוחות זמנים ושלבי העבודה – הסבר ותרשים גאנט 17](#_Toc42336009)

[4. רשימת מקורות References ראשונית 18](#_Toc42336010)

טבלה 1- קיצורים וראשי תיבות

|  |  |  |  |
| --- | --- | --- | --- |
| # | קיצור/ראשי תיבות | פירוש | הערות |
|  |  |  |  |
|  |  |  |  |
|  | CERT | Computer Emergency Response Team |  |
|  | CIA | Confidentiality, Integrity, Availability |  |
|  | ECG | Electrocardiogram |  |
|  | OSI | Open Systems Interconnection |  |
|  |  |  |  |

1. מבוא
   1. רציונל המחקר

מכשור רפואי ביתי דוגמת: קוצבי לב, משאבות אינסולין, מכשירי ECG ביתיים ומכשירים רפואיים אחרים, נעשים מתקדמים יותר ויותר. במקביל, שירותים רפואיים שונים עוברים טרנספורמציה דיגיטלית ולמעשה מאפשרים התגברות על פערי מרחק וזמן. מרבית המכשירים והשירותים הרפואיים מכילים תוכנה ומתבססים על חיבוריות לרשתות שונות, לרבות רשת האינטרנט. המידע הרפואי עובר על גבי רשתות בתי חולים, קופות חולים וטלפונים ניידים של המטופלים, על מנת להיות משולב בבסיסי הנתונים ולאפשר שיתוף מידע זה עם גורמי קצה (לדוג' רופאים מאבחנים).   
הטכנולוגיות החדשות עוזרות להגיע לאבחון מדויק יותר בזמן קצר, דרך איסוף כמות מידע גדולה (נתוני עתק), זיכוך וטיוב הנתונים בעזרת אלגוריתמים מתקדמים, ללא צורך בטיפול אמבולטורי. הטכנולוגיות נוחות למטופל עקב היותן משולבות בחיי היום יום שלו ומאפשרות למטפל לקבל מידע על המטופל שאין באפשרותו לקבל רק מביקור במרפאה וטיוב קבלת החלטות טיפוליות.  
לדוגמה מחשוב לביש (i.e. ECG Holter) מאפשר לחולי לב להיות מנוטרים 24/7, כאשר הם ממשיכים את אורח חייהם בצורה רגילה וללא צורך באשפוז ואף ביקור במרפאות. השתלת משאבות אינסולין זעירות המבוקרות ע"י מיקרו בקר מאפשרות לחולי סכרת לקבל מינון מדויק של אינסולין, כאשר תוצאות התהליך במלואו מנותרות מרחוק ע"י רופא. שרותי אבחון המתבססים על מצלמה או על מכשור דגימה מרוחק, מאפשרות קבלת אבחון בכל שעות היום והלילה ללא יציאה מהבית. טכנולוגיות לבישות אחרות מצילות חיים יום יום ע"י אוטומציה של קריאה לעזרה רפואית כאשר מערכת חכמה מזהה נפילה או במקרי חרום אחרים.

מכלול הטכנולוגיות הללו מביא לשינוי ברפואה ובמודל הטיפולי בהפיכתו לאינטגרטיבי, רציף, נגיש בבית או בכל מקום אחר ומציב את המטופל ואורח חייו במרכז.

הטכנולוגיות הנ"ל מסתמכות על חיישנים, מזעור המחשוב ועל קישוריות רציפה או מתוזמנת, הנעשית ברובה בתווך האינטרנט, אשר פתוח לכל. בכך, טכנולוגיות אלו חשופות לאיומי סייבר, החל מאיום על פרטיות המידע, אמינותו וכלה בהשתלטות על עזרים רפואיים מרחוק, העלול להביא לסיכון ושליטה על חייהם של המשתמשים.

* 1. מטרת המחקר

עבודת מחקר זו נועדה לסייע לפיתוח הטכנולוגיות הרפואיות המרוחקות באמצעות בחינת "מודל יהלום למיפוי סיכוני סייבר במכשור רפואי מחובר". המודל מציג 4 תהליכים פונקציונליים עיקריים, המורכבים מנקודות השפעה שונות, התהליכים מתקיימים במקביל זה לזה ואינם בהכרח תלויים זה בזה. המודל מראה תלות בין נקודות ההשפעה השונות וממפה את סיכוני הסייבר העולים מתלות זו.

סיכון סייבר, על פי מודל CIA כולל: פגיעה בסודיות, אמינות ושלמות מידע, ותפקוד המכשיר. מודל זה פותח ע"י מערך הסייבר הלאומי, ולכך נוסיף גם את רכיבי הזמינות והשרידות

* 1. שאלות המחקר
     1. שאלות המחקר שננסה לענות עליהם הן:  
        1. האם קיימים סיכוני סייבר שלא מופו ע"י "מודל היהלום"?  
        2. מה רמת החשיפה של מכשור הרפואי ביתי והמטופל לסיכון שלא מופה ע"י מודל היהלום?  
        3. לאילו שירותים ומכשירים המודל נותן מענה מלא ולאילו פחות? והאם ניתן לזהות נקודות קריטיות שמחייבות מענה נוסף?
  2. משתנים תלויים ובלתי תלויים

היות ואופי המחקר הנו יותר איכותי (התאמת מודל למגוון שירותים ומוצרים) קשה לנסח מדד כמותי אמין לעבודת חקר זו.

* + 1. השערת המחקר: מודל היהלום מתאים לשימוש ככלי לזיהוי נקודות כשל אפשריות במובן של אבטחת מידע והגנה על פרטיות בפיתוח כלים ושירותים רפואיים.
    2. השערת מחקר 2: במידה ותמצא אי התאמה בין מודל היהלום ומושא הבדיקה, ניתן יהיה להתאימו בקלות יחסית באופן שייתן מענה גם מקרה זה.
  1. חשיבות המחקר

עולם הרפואה עובר במהלך השנים האחרונות למערך של רפואה ביתית, במטרה להקל על הפעילות המתבצעת בבתי החולים ובמרכזים הרפואיים, ובעיקר על המטופלים עצמם, ולפיכך, המחקר הנו בעל חשיבות גבוהה. אירועי התקופה האחרונה ובעיקר הבידוד החברתי, בעקבות התפשטות מחלת ה COVID-19, מגביר את חשיבותו של המחקר. העולם עבר לקבלת שירותים מרוחקים, וקיימת האצה גם במתן שירותי רפואה מרחוק. עקב חוסר רגולציה ברורה לגבי שימוש במכשירים שאינם ייעודיים לעולם הרפואה ( אינטרנט, טלפון חכם) ו/או חוסר הבנה מצד חברות המפתחות מכשור לטיפול רפואי מרחוק , את נהלי הפיתוח המאובטח הרשמיים, קיים קושי בפיתוח והטמעה של מוצרים מאובטחים לשוק הרפואי.

מודל היהלום עשוי לתת מענה להנגשת תהליכי פיתוח מאובטח ו/או אישור למוצרים רפואיים מרוחקים. המודל פשוט להבנה ויישומו יפשט תהליכי פיתוח וקיצור זמנים עד לקבלת מוצרים ושירותים לשוק. זאת, בהיבט אבטחת המידע ומהימנות השירותים.

1. סקר ספרות ראשונית
   1. הקדמה

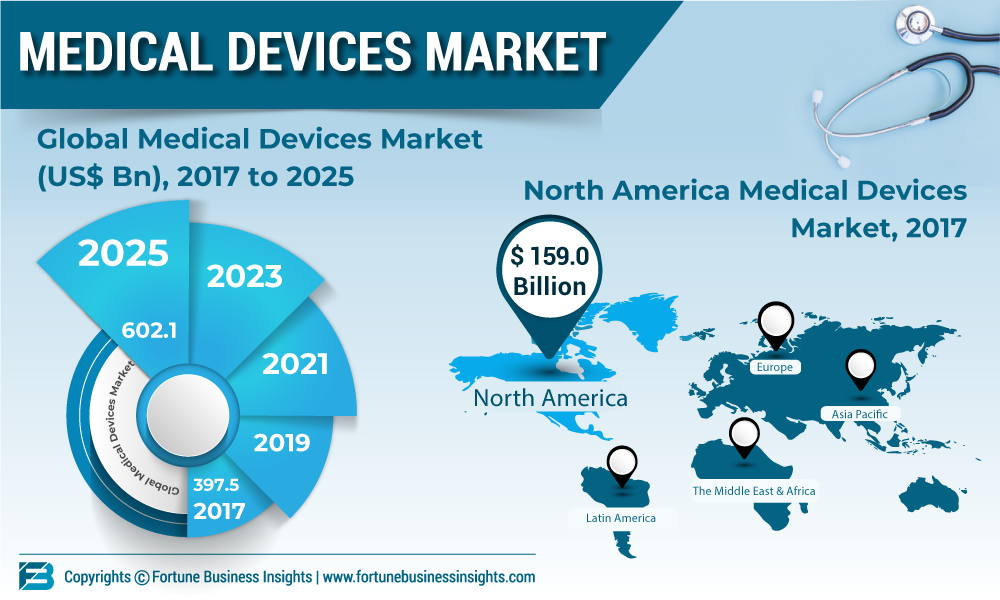
בפרק זה נסקור את המידע הזמין במקורות מקצועיים ואקדמיים בנושא:

* + 1. אבטחת מידע והגנה על פרטיות
    2. איומים על המידע מצד גורמים זדוניים
    3. טכנולוגיות רפואיות מרוחקות.
    4. מודל מיפוי סיכונים במכשור רפואי

מקורות המידע הינם מקורות דיגיטליים פתוחים (מאמרים, אתרי CERT לאומיים – בין היתר של מדינות OECD , ספרות מקוונת) וכן מקורות פרסונליים: מנהלי פרויקטי סייבר, יזמים בתחום הגנת מידע, מפתחים בחברות בעלות זיקה לאבטחת מידע ורפואה.

מיקוד הלמידה של התחום דואלי - מצד אחד, איומים ונהלים קיימים ומאידך פיתוח טכנולוגי רפואי.

כאמור, פיתוח טכנולוגי רפואי הנו תחום בעל קצב גדילה הולך וגובר [‏1]. זאת, במקביל להתפתחות טכנולוגיית המידע, והשימוש בה, אשר נהיה נפוץ ונגיש לרמת משתמש קצה ממוצע. כמות המידע העובר ברשתות גלויות ובין היתר מידע רפואי פרטי מהווה יעד אטרקטיבי לגורמים זדוניים על מנת ליירט ולעשות שימוש במידע כמו גם לפגוע באמינות וזמינות המידע. אבטחת המידע והגנה על הפרטיות לא הייתה נדרשת לולא האיומים על המידע מגורמים זדוניים.



איור 1 - צפי גידול שוק מדיקל [באדיבות FortuneBuisness]

* 1. סקר ספרות בנושא: אבטחת מידע והגנה על פרטיות

במשך העשור האחרון גרמה ההתפתחות הטכנולוגית המהירה קונפליקט וחוסר הלימה בין הזכות לפרטיות לבין הרגלי איסוף, שמירה ועיבוד של מידע אישי, שהכלכלה המודרנית, המבוססת על הטכנולוגיה הדיגיטלית, דוגלת בהם. השינוי בולט ב:

* + 1. טכניקות חדשות וזולות לאחסון כמויות עצומות של מידע אישי
    2. מהפכת הקישוריות (אינטרנט) , לא רק במה שקשור לתקשורת תוכן אלא במישורים נוספים (החל במכשירים וכלה בבוטים). מהפכת הקישוריות מאפשרת העברת נתוני עתק (Big Data) בלתי פוסקת מחיישנים בעמדות קצה וממכשירים אוגרי מידע אישי ל"מוחות" מרכזיים המסייעים בעיבוד הנתונים ומתן המלצות רפואיות.
    3. מהפכת הבינה המלאכותית – המאפשרת ניתוח כמות גדולה של הנתונים, לרבות המידע האישי שנאגר. גופי ענק מסחריים ומדינות הפכו להיות "כּוֹרֵי מידע אישי". למעשה ההתייחסות לאדם הנה כ- "נושא מידע" (Data Subject). ליבת הכלכלה הדיגיטלית והמודל העסקי של חברות ענק כגון גוגל, ואמזון פייסבוק הנה צבירת מידע אישי וניתוח שלו לצורך הפקת תובנות חדשות, כגון שיווק ממומן ממוקד ושרות תוכן אישי יותר. יתר על כן, מיליוני עסקים קטנים ובינוניים אוגרים מידע אישי כל העת. ערכם של מאגרי המידע הפרטי גבוהה מאוד - ממידע על הרגלי גלישה ועד למידע על היסטוריה רפואית. המדינות לא נותרו מאחור, וגם הן מפתחות מערכות לאיסוף מידע אישי מסוגים שונים - החל במידע אישי הנאסף בפעילות ממשלתית שגרתית (כדוגמת בטחון, חינוך, שרותי רווחה ובריאות), דרך מצלמות רחוב ומערכות פיקוח עירוניות וחיישני חום וקול לזיהוי אזרחים ולניטור פעולותיהם, וכלה במאגרים למידע ביומטרי או איסוף יזום של מידע מרשתות חברתיות.

איסוף המידע האישי האינטנסיבי והיתרונות הגלומים בטכנולוגיה מחייבים מודעות ואמצעי הגנה על מנת למנוע שימושים פסולים במידע ובגישה אליה, (כגון פרשת קיימברידג' אנליטיקה [‏7]).

כיום נהוג ליישם אבטחת מידע על בסיס שני מודלים עיקריים. האחד: “מודל שבע השכבות” של ארגון ה-OSI [‏5] והשני: “מודל המעגלים” - CIA. בשני המודלים שכבות ההגנה החיצוניות הן: שכבת מדיניות, שכבת הגנה פיזית, שכבת הגנה על התקשורת הפנימית, שכבת הגנה על התקשורת החיצונית, שכבת הגנה על בסיס הנתונים ותחנת המשתמש, שכבת אבטחת האפליקציה, ושכבת אבטחת הנתונים. במודל המעגלים מקובל להתייחס לשלושה נכסים מרכזיים שעליהם נדרש להגן במערכות מידע:

* + 1. חסיון המידע (**[C**]onfidentiality) – מידע יהיה נגיש לגורם שהורשה לו בלבד.
    2. שלמות ואמינות המידע ([**I**]ntegrity)– הגנה על כך שהמידע במערכת יכיל את כל שהוגדר מלכתחילה וכי הנתונים עצמם לא עברו שינוי על ידי גורם שאינו מורשה.
    3. זמינות המידע והמערכת ([**A**]vailability) – מערכת המידע והמידע האגור בה יהיו זמינים בהתאם לרמת הזמינות שהוגדרה על ידי לקוחות המערכת.

מאידך, יש להתייחס לשלושה מרכיבים שונים הגורמים לסיכון:

* + 1. טכנולוגיות – מערכות החומרה, התוכנה והתקשורת המהוות “מערכות”
    2. אנשים – המשתמשים בטכנולוגיות, ולכן מהווים חוליה חלשה במיוחד, מכיוון שהם מפעילים או משתמשים בטכנולוגיות, ונוטים לעשות שגיאות המייצרות פרצות במערך ההגנה אשר מאפשרות לתוקף לנצלן.
    3. תהליכים – מידת הנזק משגיאת אנוש או נקודת תורפה טכנולוגית עשויה לִהצטמצם מאוד אם מבוצע תכנון נכון של התהליכים בארגון. הגדרת תהליכים בסדר נכון ובדוק מראש מאפשרת זיהוי מוקדם של פגיעה או ניסיון פגיעה במערכות.
  1. סקר ספרות בנושא: איומים על מערכות מידע מגורמים זדוניים

סיכון סייבר הינו מתקפה אשר מבוצעת על ידי או בעזרת מערכות ממוחשבות על הארגון. מתקפות אלו מתוחכמות יותר (מאשר התקפה פיזית) ועל כן על הארגון להקים מערך הגנה בהתאם לטכנולוגיות ומערכות אלו. ניתן לומר כי איום סייבר איננו גורם לסוג חדש של נזק אלא שיטה חדשה לתקוף את הארגון, סיכונים כגון דליפת מידע והונאות הינם סיכונים אשר היו קיימים קודם לכן. למשל, דלף מידע הוא אינו איום חדש [‏16]. הונאה, גם היא אינה איום חדש. אלו הם איומים קיימים אשר ארגונים מטפלים בהם מזו תקופה ארוכה. האבחנה בין איום סייבר לבין איום שאינו סייבר, נעוצה בתרחיש אשר מממש את הסיכון. אם הדרך למימוש האיום בוצעה על ידי תקיפה של מערכות מחשב או מערכות ותשתיות משובצות מחשב, אזי מדובר באיום סייבר.

מאפיין נוסף של איומי הסייבר הוא מורכבות ורמת התחכום של תרחיש התקיפה, אשר עלול לנצל חולשות קיימות במוקדי סיכון שונים. לדוגמה, התרחיש יכול להתחיל בניצול חולשה אנושית כאשר תוקף מתחזה לאיש תמיכה ומבקש מעובד את שם המשתמש והסיסמא שלו למערכת הכספים, בשיטת ה"הנדסה החברתית" [‏8] . התרחיש ימשיך בניצול חולשה טכנולוגית שבאמצעותה התוקף פורץ למערכת, מזדהה בשם העובד ומבצע העברת כספים לחשבון היעד.

איומי סייבר מתחלקים לפי מספר קריטריונים:

* + 1. גורמי האיום - מיהם התוקפים המאיימים על הארגון, מהם יעדי התקיפה שמעניינים אותם, מהי המוטיבציה שלהם לתקוף את הארגון, ומהן היכולות של התוקפים כדי להוציא לפועל את ההתקפה ולהשיג את היעד.
    2. נכסים מאוימים – מכלול האמצעים שעלולים להוות מטרה לתקיפות סייבר: כסף, מוניטין, מערכות, שירותים, מידע, אנשים ומשאבים פיזיים.
    3. השלכות של פגיעה במערכות (בכל אחד מגורמי ה CIA [‏6]) ועלות השיקום של מערכת המידע של הארגון ונכסיו

נושא אבטחת המידע הרפואי הינו בעל חשיבות גבוהה, ומחייב את מערכת הבריאות הישראלית ( וכך גם עבור כל מדינה) להבטיח עמידה בסטנדרטים הגבוהים ביותר. עם התגברות האיומים על מערכות מבוססות מחשוב, ובכלל זה הטרור הקיברנטי, המערך הרפואי נדרש להגן על מערכות המחשוב הקריטיות של מערכת הבריאות בכל  
הרמות, על מנת להבטיח רצף טיפולי וניהולי כנדרש. למערכת הבריאות קיימים איומים ייחודיים בתחום ההגנה על המידע הכוללים, בין השאר:

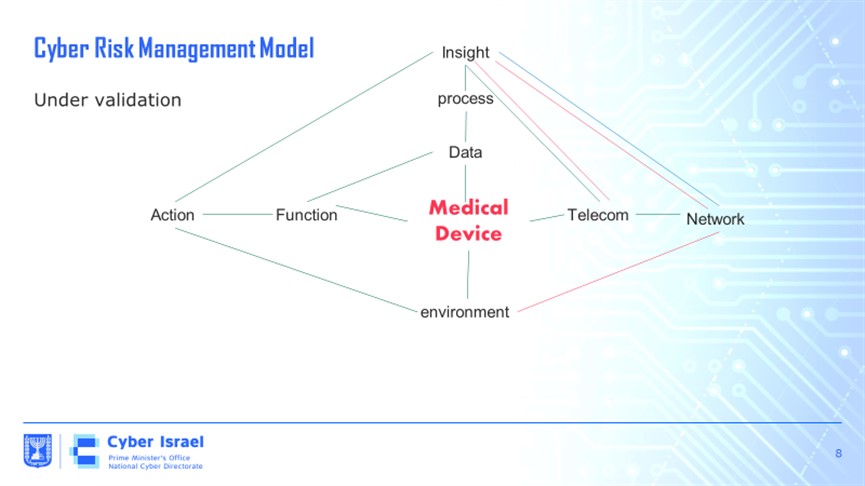
* + 1. מניעת שירות Denial of Serviceדבר אשר עשוי לפגוע במתן שירות  
       רפואי חיוני בשגרה ובמיוחד בחירום. התלות הקיימת כיום במערכות מידע  
       לצורך אספקת חלק משירותי הרפואה, הופכת איום זה למוחשי במיוחד.
    2. גניבת מידע – מידע רפואי הינו מידע אישי רגיש ולגניבתו עשויות להיות  
       השלכות קשות ברמה האישית וברמת האמון במוסדות הבריאות במדינה.
    3. שיבוש מידע – הנזק אשר יכול להיגרם משינוי מידע בתיקו הקליני של  
       מטופל עולה לעיתים על הנזק מגניבתו, היות ויכול להוות בסיס להחלטות  
       רפואיות שגויות

* 1. סקר ספרות בנושא: תשתיות, שיטות ודוגמאות לשירותים ומוצרים רפואיים
     1. רקע: המהפכה הדיגיטלית שינתה את אורח החיים בצורה משמעותית [‏17]. גם בעולם מערכות הבריאות ושירותי הבריאות [‏9], הרשומה הרפואית הממוחשבת הפכה למשתתף השלישי במפגש מטופל–רופא ומשנה באופן מהותי את אופן המפגש. מחוץ למתקני הרפואה, רשת האינטרנט, משמשת לחיפוש מידע בנושאי בריאות, ומטופלים קוראים את המאמר המעודכן בעניינם, פעמים לא מעטות לפני שרופאם מוצא לכך זמן. בנוסף להיותם מעודכנים יש למטופלים היום גם נגישות למידע באיכות משתנה על תפקוד רופאים, הרקע שלהם ונתונים על תפקודם. לבסוף, השימוש של רופאים ברשתות חברתיות כפייסבוק וטוויטר לתקשורת עם מטופליהם בוחנת את הגבולות ביחסי חולה–רופא.
     2. העידן הדיגיטלי בבריאות: טכנולוגיית המידע מעמידה לרשות המטופלים והמטפלים כאחד מגוון רחב של אמצעים חדשים בתחום הרפואה והבריאות. בעוד שבעבר היה הידע הרפואי נחלת המקצוע ונגישותו הוגבלה לספריות ולספרים, הרופא נתפס כבעל סמכות שאינה ניתנת לערעור והמלצותיו היו בגדר הוראות, הרי שנגישות המידע הרפואי לכל והשקיפות היחסית של הרופא וארגוני הבריאות שינו באופן מהותי את מבנה מערכת היחסים בין מטפל למטופל. הבסיס לשינוי היה גם פרי תהליכים חברתיים מודרניים. בעת הזאת, המידע הרפואי נגיש לכל, המטופל פעמים רבות בוחר את המטפל (ולעיתים קרובות על בסיס המידע הדיגיטלי שהוא אוסף אודותיו). בעידן הדיגיטלי ניתן להתייעץ וירטואלית ללא מגבלות גיאוגרפיות. יש הסרת חסמים רבים למפגש מטופל–מטפל (פריצת מרחק וזמן במונחי טרנספורמציה דיגיטלית), וגובר והולך מספר ההתייעצויות הווירטואליות והציפייה, כך נראה, של הדור הצעיר (Digital Natives [‏10]) לנקודת מפגש קלינית שאיננה במתקן רפואי בהכרח, אלא מתקיימת בטלפון הסלולרי. בעידן הדיגיטלי שבו לכל אחד יש טלפון חכם, גם במדינות עולם שלישי שאין נגישות לעובדי בריאות, לדוגמה, המטופל לובש לעיתים זהות חדשה ושונה מקודמתה, אשר יש המכנים אותה e-patient ,והוא מאתגר את המטפל בו בדרכים שלא נודעו בעבר. במקביל, מתפתח העידן של האבחון העצמי. המטופל "מתייעץ" בתחילה עם המאגרים הדיגיטליים, ועם "חבריו" ברשתות החברתיות, ורק בשלב שני הוא מחליט אם הוא זקוק למפגש וירטואלי או פיזי עם שירות בריאות כלשהו. גם בהמשך התמודדותו עם נושאי בריאות וחולי, נדרש המטופל לאינטרנט כדי ללמוד ולהבין את מצבו, והוא יכול להצטרף לקהילות מטופלים וירטואליות של בעלי מצב רפואי דומה, המעניקות תמיכה וייעוץ לחבריהן וגם מזמינות רופאים לעיתים לתרום לקהילה, אך בעמדה של יועץ אחד מני רבים - מקצועיים ושאינם מקצועיים

* + 1. האמצעים שמעמיד לרשותנו העידן הדיגיטלי על פי קטגוריות
       1. Big Data, רפואה מותאמת אישית, רפואה חישובית
       2. מידע רפואי באינטרנט
       3. הרשומה הממוחשבת
       4. יישומונים
       5. תקשורת דיגיטלית
       6. המטופל והרופא הדיגיטלי, בריאות ניידת
       7. רשתות חברתיות, העצמת בריאות מטופלים באמצעות הרשת.
       8. מערכות תומכות החלטה ושימושים קליניים של טכנולוגיית המידע בנקודת המפגש הקליני
       9. מערכות מנהליות דיגיטליות (זימון תורים, פורטלים למטופלים, אתרים)
       10. טלה–רפואה
    2. אמצעים אלה מייצרים שורה של דילמות חדשות כמו: חיסיון רפואי בעולם הדיגיטלי, הפער הדיגיטלי וגבולות בעולם הווירטואלי. הם מרחיבים את מנעד האוריינות הנחוצה למטפלים ומטופלים כאחד. הם מחייבים רכישת כישורים רבים חדשים הנובעים מהאתגרים שהם מציבים למטפל. רק בתחום התקשורת בין מטופל למטפל בנוכחות מחשב אותרו עשרות כישורי תקשורת חדשים ]9 .]בעת שעולם האבחון הרפואי עבר ועובר טרנספורמציה דיגיטלית, ועולם המידע וההכשרה הרפואיים מסגלים כלים דיגיטליים מגוונים, דומה שדווקא המטופלים )לפחות בעלי האוריינות הדיגיטלית( כבר סיגלו לעצמם מרכיבים רבים של השינוי, בעוד שהרופאים נמצאים בפיגור משמעותי בהתאמת התנהלותם למציאות החדשה.
       1. Big Data רפואה מותאמת אישית, רפואה חישובית:  
          באמצעות ביו-אינפורמטיקה ורפואה חישובית התאפשרו פריצות הדרך בתחום ונכנסו לשיח המקצועי חקר החלבונים, חקר הדנ"א והדם בכלים חישוביים. תחום זה זוכה להכרה גוברת במערכת ההכשרה של רופאי העתיד באמצעות קורסים, שיעורים ואף מסלולים ייעודיים (לדוגמה, בפקולטה לרפואה של הדסה והאוניברסיטה העברית והתכנית החדשה של HIT- טכנולוגיות דיגיטליות ברפואה [‏11] ).
       2. מידע רפואי ברשת האינטרנט:  
          כשם שכמעט כל צורך במידע נענה היום באמצעות גלישה בנייד, כך גם הפך המידע הרפואי לנגיש ביותר. הקלדת מושג רפואי כלשהו מקפיצה תשובות רבות, חלקן מעולמות תוכן שאינם מבוססי מידע מהימן )רפואה משלימה, פרסומת אישית, אנקדוטות וכדומה). לכן נזקקים המטופל והמטפל גם יחד לאוריינות מידע דיגיטלית שבאמצעותה נלמדת הדרך המיטבית לחפש מידע רפואי מהיימן באינטרנט אך עדיין לוקה בבעיה של אינפורמציה לא אמינה במקרים רבים.
       3. הרשומה הממוחשבת: כיוון שכל מערכת הבריאות הישראלית מקוונת ברשומה רפואית ממוחשבת (רר״מ) ומרושתת גם במערכת אינטגרטיבית הנמצאת בהליכי הטמעה ("אופק") [‏12], זהו כנראה התחום שבו יש לרופא הישראלי את המגע היום-יומי והמוחשי ביותר עם העידן הדיגיטלי. ההכשרה לשימוש הטכני בו היא לרוב אינטואיטיבית או קצרה והידע באבטחת מידע לעובדי מקצועות הבריות מוגבלת להכשרות קצרות דרך לומדות ארגוניות.
       4. יישומונים (אפליקציות):  
          בעוד שבשוק יש עשרות ואולי מאות אלפי יישומונים בתחום הבריאות והרפואה, דומה שבתחום זה מתקיים הפער המרבי בין מטופלים למטפלים. בעוד שהציבור הרחב מוריד ומשתמש בשקיקה במספר משמעותי של יישומונים לפי צרכיו, דומה שרופאים כמעט שאינם יכולים להשתמש בתוצרי התחום, גם כאשר יש מספר ניכר של יישומונים בעלי ערך מוסף ליעילות ולתוצאי הטיפול הרפואי שמעניק הרופא. בין החסמים לשימוש נרחב יותר ניתן למנות את מיעוט החקירה המהימנה של ביצועי היישומונים והיעדר אינדקס סדור שמאפשר לחפש יישומון מתאים בהתאם לצורך וחוסר הטמעה בארגוני בריאות עקב בעיית אבטחת מידע באינטגרציה לתיק הרפואי.
       5. תקשורת דיגיטלית:  
          הטלפון הנייד החכם ויישומיו התקשורתיים מייצרים טרנספורמציה בתקשורת בבריאות - דואר האלקטרוני, מסרונים, וואטסאפ (WhatsApp), סקייפ (Skype) ודומיו, ומערכות רבות נוספות - כל אלה יוצרים חלופה ראויה למפגש פנים אל פנים אשר מצמצמת משמעותית מגעים פנים אל פנים לצרכים שהמפגש הפיזי אינו מספק להם ערך מוסף. מרבית הצרכים המנהליים מקבלים מענה משופר וירטואלי וחוסכים זמן, כסף וחיים )שכן נסיעה ברכב היא אולי מסכן החיים המרכזי בחיינו(, ולא מעט צרכים קליניים בדיפרנציאציה נמוכה וגבוהה מקבלים מענה משפר בריאות בדרך וירטואלית [‏13]
       6. בריאות דיגיטלית, המטופל הדיגיטלי, הרופא הדיגיטלי, רפואה ניידת:  
          מומחי עתידנות מנבאים שחלקים הולכים וגוברים של תשתית הרפואה יועתקו לתשתית במרשתת, כך שמגעים בנושאי בריאות יתרחשו וירטואלית [‏14] ויחייבו אותנו לתפקוד מוגבר כרופאים דיגיטליים. במערך כזה וגם במציאות היום, המטופל הופך למטופל וירטואלי, כמו ePatient Dave [‏15] מטופל שמספר כיצד באמצעות הכלים הדיגיטליים הפך לגורם העיקרי לריפוי מוצלח מסרטן שמטפליו לא מצאו לו פתרון. כדי לאמץ פרסונה של רופא דיגיטלי, עלינו לפתח מידה משמעותית של מיומנות דיגיטלית ותפקוד מיטבי בסביבה עתירת טכנולוגיה. מכיוון שתחום זה נמצא בגאות בלתי פוסקת, חוסר המעורבות והמיומנות של רופאי ישראל בו, מביא להגדלה קבועה ומדאיגה של הפער בין הציבור לרופאיו בתחום זה.
       7. רשתות חברתיות: הרשתות החברתיות והטלפוניה/ מחשוב הניידים חוברים לנוכחות מוגברת של רבים בעולם הווירטואלי. האם עבור הרפואה והרופאים הם אויב או ידיד? יש ברשתות יתרונות (לדוגמה, קידום בריאות, ניטור מחלות כרוניות והעצמת מטופלים), ולא מעט חסרונות (לדוגמה, גבולות, סודיות). רשימת הסוגיות שהרשתות החברתיות מציבה בפנינו היא ארוכה ביותר.
  1. מודל למיפוי סיכונים למכשור רפואי
     1. רקע:

המודל מציג 4 תהליכים פונקציונליים עיקריים, המורכבים מנקודות השפעה שונות, התהליכים מתקיימים במקביל זה לזה ואינם בהכרח תלויים זה בזה.

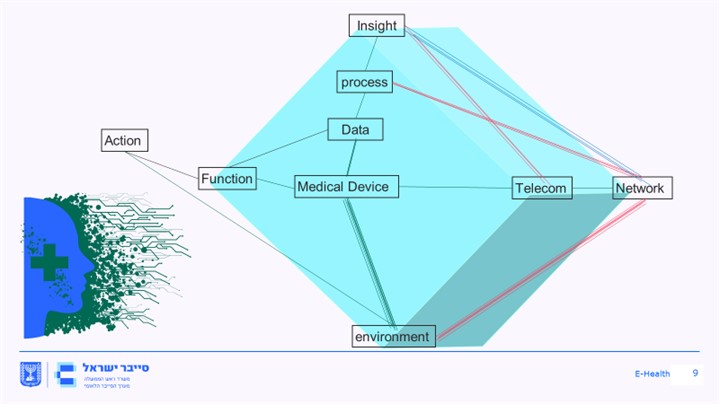
מטרת המודל להראות תלות בין נקודות ההשפעה השונות המוצגות בו ולמפות את סיכוני הסייבר העולים מתלות זו.



איור 2 - מודל למיפוי סיכונים

סיכון סייבר הוא על פי מודל CIA – פגיעה בסודיות, אמינות ושלמות המידע ותפקוד המכשיר, בתוספת רכיב שימוש שלא בהתאם לייעוד.

* + 1. המשימה:
       1. המודל נבחן מנקודת מבטם של שלושה גורמים המושפעים מפעילות המכשיר ויש להציג את מפת הסיכונים מנקודת מבטו של כל אחד מהגורמים.
       2. יש למתוח קו בין נקודות ההשפעה שיש ביניהן תלות רק כאשר תלות זו עשויה להצביע על סיכון סייבר מתוך נקודות מבט שונות.
       3. נקודות המבט של: מספק המכשיר (חברה/בית חולים/ארגון בריאות) – קו בצבע **אדום**, המטופל – קו בצבע **כחול**, המטפל – קו בצבע **ירוק** (בתנאי שאורן רואה את ההבדל).

לגבי כל וקטור יש לשאול - האם ישנו סיכון לשיבוש המידע או פעילות המכשיר בקשר שבין הרכיבים. אם התשובה היא כן – יש למתוח קו בצבע המשקף את נקודת המבט. 

איור 3 - נקודות ההשקה במודל

* + 1. תיאור נקודות ההשפעה:
       1. **תיאור הסביבה**המתקן בו מופעל המכשיר  
          הארגון מוסר המכשיר  
          דוגמא: מפעיל, בית החולים, רופא, מטפל, מטופל, מחזיק המידע (ענן)
       2. **יעד תקשורת**לרבות אחסון ענן  
          רכיבי תקשורת שונים  
          יעד חיבור סופי (מיקום אחסון פיזי / ענן)  
          החברה בעלת האחסון
       3. **תקשורת מקומית**פירוט הרכיבים שדרכם עוברת התקשורת בין המכשיר לארגון
       4. **תקשורת חיצונית**פירוט הרכיבים שדרכם עוברת התקשורת מהארגון לאינטרנט או לספק (אם הספק איננו הארגון בו פועל המכשיר).
       5. **מידע**איזה מידע יוצא מהמכשיר  
          איזה מידע נכנס למכשיר
       6. **שרשרת רפואית**  
          תיאור התפקוד הרפואי של המכשיר – כיצד המכשיר מפעיל את מתן הטיפול הרפואי
       7. **מתפעל מקומי**   
          האם נדרש  
          מי מפעיל את המכשיר באופן שוטף  
          מי מוסר את המכשיר  
          מי הגורמים המעורבים בתפעול השוטף – עדכוני גרסאות, עדכוני טיפול וכו'
       8. **מטופל**מהו הידע המקדים הנדרש למטופל?  
          מה הן הפעולות התלויות במטופל?  
          מה המידע עליו יכול לשלוט המטופל?
       9. **ידע**  
          הנתונים הנאספים על ידי המכשיר.  
          מה מקורם?  
          באילו סנסורים נעשה שימוש?  
          האם נעשה שימוש בפרוטוקולים מסוימים, תדרים?  
          באיזה פורמט ובאיזה היקף הידע נשמר?
       10. **עיבוד**  
           היכן העיבוד מתבצע ? האם על המכשיר או בענן  
           מהיכן המידע המעובד על ידי המכשיר  
           לאן המידע המעובד עובר
       11. מידע
       12. תוצר העיבוד של הידע  
           האם משפיע על פעילות המכשיר
  1. סיכום סקר הספרות

לאור הטרנספורמציה הדיגיטלית שעבר עולם הרפואה והתפתחות ה-טלה-רפואה בצירוף להתרחבות האמצעים, שיטות ותגמול בפגיעה בתשתיות רפואה ו/או גניבת מידע רפואי, נדרשת תפיסה חדשה להתמודדות עם איומים אלה במיוחד בעולם הרפואה. בנוסף למודלים הקיימים למיפוי ונטרול איומים קיים גם מודל "היהלום" שמפשט ומנגיש את המתודולוגיה להגנה על מוצרים רפואיים.

1. מתודולוגיה ראשונית
   1. המחקר יתבסס על שירותים ומוצרים הניתנים ע"י מערך קופות החולים בישראל וכן שירותים פרטיים משלימים. במהלך המחקר ייבחן מוצר/שירות של הקופה ויופעל עליו מודל היהלום למיפוי סיכונים. כל מוצר/שירות ינותח לפי נקודות ההשקה הרלבנטיות לו ותוצאות המיפוי יסוכמו.
      1. להלן תכנון ראשוני של הקופות ושירותים
         1. אפליקציות גישה בקופות חולים (כללית, מכבי וכו')
         2. שח"ל/נטל"י
            1. ניטור קצב לב מרחוק
      2. אפליקציה ומכשור IOT למדידה, ניטור והמלצת טיפול בסוכרת
      3. התכנון לעיל הנו ראשוני ובהחלט ייתכן מצב שאחד השרותים/מכשורים אינו זמין והבחינה שלו קשה. במקרה זה יתבצע תשאול של מספר משתמשים וננסה לתת הערכה גסה לנקודות ההשקה אל מול המודל
      4. בנוסף, במידה ויתאפשר יבוצע סקר של מכשיר לא רפואי בכדי לקבל הערכה לגנריות המודל. במקרה זה יבוצע ראיון עם אחד מראשי פרויקט של מכשור לא רפואי.
   2. הפרדיגמה המחקרית
      1. המחקר, ביסודו מחקר איכותי. מטרת המחקר בחינת התאמה של מודל סיכונים ומיפוי נקודות חוסר התאמה הדורשות התייחסות מיוחדת שלא נכללה במודל ונמצאה במחקר פתרונות קיימים.
      2. התשובה לשאלות המחקר אינה ניתנת לניסוח במספרים, המטרה הנוספת של המחקר זה חשיפת נקודות תורפה\אי התאמה והצעת עדכונים למודל האמפירי על מנת לגבש מדיניות המלצות למשתמשים השונים במערכת הבריאות.
   3. המחקר תוכנן על סמך ידע הקיים בספרות, מודל היהלום שפותח ב HIT ביחד עם מערך הסייבר הלאומי ומחקר צרכי מערכת הבריאות בראיית פני עתיד. אין משמעות למחקר גישוש במקרה זה. עם זאת בהנחיה משתתפים מומחים מתחומי הרפואה הדיגיטלית ואבטחת מידע שיאפשרו הבנה של מידת יכולת היישום של תוצרי המחקר והנבדקים
      1. נבדקי המחקר הנם מכשירים ושירותים רפואיים שמספקים טלה-רפואה. קריטריוני בחירה הנם:
         1. זמינות המכשור (בהשאלה ממשתמשים, ברכישה זמנית למשך המחקר וכו')
         2. התאמת המכשיר/שירות למודל (למשל שירות טלפוני אינו מתאים לטעמנו שכן הוא תלוי רבות בגורם אנושי ועל כן קשה לבחון את נקודות הממשק של המודל)
   4. שיטת המחקר – במחקר כמותי, מה תהיה שיטת המחקר (ניסוי, סקר, מחקר קורלטיבי וכד')?
   5. כלי איסוף הנתונים – מדידות: היכן ואיך? שאלונים: כמה? איזה? מסמכים? סוג הראיונות (למשל, חצי מובנים) וסוג התצפיות (למשל, הצופה המשתתף) עם נימוקים להצדקתם.
   6. כלי מחקר נוספים (מה שרלבנטי) – סימולציות, מודלים, פיתוחים מתמטיים, תוכנות, כלי קבלת החלטות ובחירת חלופות, אלגוריתמים וכד'.
   7. בסקר – תכנון שלבי בניית השאלון (או השאלונים).

שיטת המחקר תהיה ניתוח תהליכי של מודל היהלום בהתאמה לניתוח תהליכי העבודה והעברת המידע בשירותים הנבחרים.

כל אחד מהשירותים ימופה בהתאם לקריטריונים הבאים:

1. התהליך של העברת המידע- ארגון בריאות ( לדוגמא, תיק רפואי או מידע שמגיע מתוך המערכת ומועבר דרך שכבת מידע חיצונית) מערכת תקשורת כללית או רפואית, אופן איסוף המידע מהמטופל, עיבוד המידע ( לדוגמא- העברה, עיבוד נתונים\ המלצות רפואיות),
2. מידת הביקורת הרפואית הניתנת במהלך התהליך ( דורש אישור רופא? מייעץ לרופא? מנגיש מידע והרופא מחליט?)
3. מידת הסיכון למטופל ( ייעוץ בוידאו לעומת הנחיות ללקיחת מינון תרופה)

תהליך זה ייבחן על פי מודל היהלום לבחינת יכולת המודל לזהות סיכונים וההמלצות לאבטחת המידע לבחינת איכות ההמלצות ומידת ההתאמה.

מודל זה ייבחן בראיית המשתמשים השונים: ארגון נותן שירות, מטופל וחברת מפתחת מכשיר\שירות.

לסיכום ייבחנו כלל התוצאות המתקבלות מהניתוחים השונים המתוארים מעלה לקבלת מסקנות להנחיות לבחינת שירות\מיכשור לצורך פתוח הנחיות לפתוח, שמוש והכנסת דירות חדש לארגון בריאות.

* 1. ניתוח הנתונים
     1. היות ומדובר על מחקר איכותי, יבוצע ניתוח תוכן על הנתונים שיאספו במהלך המחקר.
     2. כפי שצוין בסעיף ‏3.1 כל שרות יבחן מול "מודל היהלום" שתואר בסעיף ‏2.5 "מודל למיפוי סיכונים למכשור רפואי".
     3. התוצאות של מבחן אל מול המודל ירשמו ויסוכמו בטבלה בה יצוינו נקודות ההשקה שעברו ונקודות שאינן רלבנטיות.
     4. נקודות הסיכון ידורגו על פי מידת החשיבות והסיכון ישמשו כבסיס לפתוח הנחיות להכנסת שירות חדש לארגון בריאות, לפתוח מכשור\שירות רפואי באופן שיאפשר הטמעה ונחיות לקהל המטופלים על שימוש נכון בשירות\מכשור רפואי דיגיטלי בחיי היומיום
  2. אתיקה – דילמות אתיות ודרכי התמודדות.
     1. כמו בכל עבודה הקשורה לדיון בפגיעויות ואפשרויות דלף של מידע אישי, עלול החוקר לגלות פרצה שמאפשרת פגיעה/שליפה של מידע אישי. במצבים אלו בעולם חקר אבטחת המידע, נהוג לדווח לחברה האחראית בדיסקרטיות, לאפשר פרק זמן לתיקון ורק אז לפרסם כי נמצאה הבעיה. הליך זה אינו אחיד ולכל חברה מדיניות משלה (Disclosure Policy). אם במהלך עבודה זו תתגלה פגיעות קריטית, נאמץ במסגרת עבודה זו את המדיניות של גוגל ונחכה במשך 90 [‏4] יום מדיווח הבעיה לחברה האחראית.

יש לציין כי אין בעייה אתית בעבודת מחקר זו כיוון שאין שמוש בנתוני מטופלים ו\או תיאור מקרים אמיתיים. נושא האתיקה ישולב בעבודה בראיית סיכונים אתיים באבטחת מידע ויוגש כחלק מהמלצות העבודה

* + 1. דילמה נוספת הנה חשיפה לנתונים אישיים שלא במכוון. במסגרת עבודה זו יהיה שימוש אך ורק בנתונים ושירותים של כותבי עבודה זו.
  1. תכנון לוחות זמנים ושלבי העבודה – הסבר ותרשים גאנט

1. רשימת מקורות References ראשונית

1. [סקר חיזוי גודל שוק מכשור רפואי](E:\\Download\\1.https:\\www.medgadget.com\\2020\\01\\medical-devices-market-regional-analysis-2020-2025-global-market-size-research-report-trends-growth.html)
2. [הרשות להגנת הפרטיות – מדריך לתקנות להגנה על פרטיות](https://foi.gov.il/sites/default/files/%D7%94%D7%9E%D7%93%D7%A8%D7%99%D7%9A%20%D7%94%D7%9E%D7%9C%D7%90%20%D7%9C%D7%99%D7%99%D7%A9%D7%95%D7%9D%20%D7%AA%D7%A7%D7%A0%D7%95%D7%AA%20%D7%90%D7%91%D7%98%D7%97%D7%AA%20%D7%9E%D7%99%D7%93%D7%A2%20-%20PDF%20%D7%9C%D7%94%D7%93%D7%A4%D7%A1%D7%94.pdf)
3. [מדריך תורת הגנה ארגונית](https://www.gov.il/he/departments/topics/11)
4. [Google project zero Disclosure Policy](https://googleprojectzero.blogspot.com/)
5. [מודל שכבות תקשורת ה- OSI](https://www.cloudflare.com/learning/ddos/glossary/open-systems-interconnection-model-osi/)
6. [מודל ה CIA לאבטחת מידע](https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html)
7. [פרשת Cambridge-Analytics](https://www.businessinsider.com/cambridge-analytica-a-guide-to-the-trump-linked-data-firm-that-harvested-50-million-facebook-profiles-2018-3)
8. קווין מיטניק, The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders and Deceivers, 2005, ISBN: 0471782661
9. Reis S, A Visser & Frankel R, Health information and communication technology in healthcare communication the: the bad, the good and the transformative. Patient. Educ Couns 2013. Couns Educ :doi. 62-359):3(93;Dec

1. [Marc Prensky](https://www.marcprensky.com/writing/Prensky%20-%20Digital%20Natives,%20Digital%20Immigrants%20-%20Part1.pdf), “Digital Natives, Digital Immigrants” On the Horizon, vol. 9, no. 6 (December 2001), pp. 15–24;
2. https://alumni.huji.ac.il/news/mediaaccess 18-Aug-2019
3. [מרכז סמוקלר לחקר מדיניות הבריאות. מערכת אופק - התיק הרפואי הווירטואלי](https://brookdale.jdc.org.il/wp-content/uploads/2018/01/556-10-Ofek-ES-HEB-1.pdf)
4. Peleg R & Nazarenko E, Providing cell phone numbers and e-mail addresses to patients: The patient’s perspective, a cross sectional study. Isr J Health Policy Res. 2012 Aug 28
5. Dorsey ER & Topol EJ, State of Telehealth. N Engl J Med. 2016 2016 Jul154-61
6. <https://www.epatientdave.com/about-dave/>
7. [הערכת סיכוני סייבר, 08 אוקטובר 2018, אורן מזרחי](https://www.bdo.co.il/he-il/%D7%9B%D7%AA%D7%91%D7%95%D7%AA-%D7%95%D7%9E%D7%90%D7%9E%D7%A8%D7%99%D7%9D/%D7%99%D7%A2%D7%95%D7%A5-%D7%A2%D7%A1%D7%A7%D7%99/%D7%99%D7%A2%D7%95%D7%A5-%D7%95%D7%91%D7%99%D7%A7%D7%95%D7%A8%D7%AA-%D7%9E%D7%A2%D7%A8%D7%9B%D7%95%D7%AA-%D7%9E%D7%99%D7%93%D7%A2-it/%D7%94%D7%A2%D7%A8%D7%9B%D7%AA-%D7%A1%D7%99%D7%9B%D7%95%D7%A0%D7%99-%D7%A1%D7%99%D7%99%D7%91%D7%A8-%D7%91%D7%90%D7%A8%D7%92%D7%95%D7%A0%D7%99%D7%9D-%E2%80%93-%D7%AA%D7%A4%D7%99%D7%A1%D7%AA-%D7%A0%D7%99%D7%94%D7%95%D7%9C-%D7%94%D7%A1%D7%99%D7%9B%D7%95%D7%9F-%D7%97)
8. ירחון "רפואה", כרך 158, אוקטובר 2019

את רשימת המקורות References יש לערוך לפי תקן APA. ראו למשל:

[http://owl.english.purdue.edu/owl/resource/560/01](http://owl.english.purdue.edu/owl/resource/560/01/)