6 ביוני 2022
ז׳ בתמוז, התשפ״ב

הגנה על פרטיות מטופלים במתן שירותי רפואה מרחוק

נוסח מעודכן בעקבות תיקון 13

מבוא

1. אחת התופעות המרכזיות המתפתחות בשנים האחרונות היא מתן שירותי רפואה מרחוק, קרי באופן מקוון (Telemedicine ,Telehealth).[1] תופעה זו היא חלק מתופעה רחבה יותר במסגרתה שירותים שעד לאחרונה ניתנו רק באופן פיזי ו״מקרוב״, כגון שירותי חינוך או שירותים בנקאיים, הופכים להיות כאלו הניתנים גם באופן מקוון. תופעה זו הינה מאפיין מובהק של חיים בעידן הדיגיטלי, והפכה נפוצה פי כמה בעקבות פרוץ משבר הקורונה והצורך לשמור על ריחוק חברתי.

2. שירותי רפואה מרחוק מוגדרים, בין היתר, כ״אבחון וטיפול רפואי באמצעים דיגיטליים״,[2] וכ״מפגש המתבצע באמצעים טכנולוגיים ובאמצעות תקשורת אלקטרונית לצורך מתן שירותי בריאות בין מטופל למטפל מזוהים, לא בהכרח בחפיפת זמן ומקום״.[3]

3. מטבע הדברים, לשירותי רפואה מרחוק יתרונות רבים. עם זאת, השימוש בהם טומן בחובו גם אתגרים שונים מבחינת הגנה על פרטיותם של מטופלים ועל מידע הנוגע אליהם.

4. מטרת המסמך היא להציב זרקור על התופעה ועל אתגרי הפרטיות הכרוכים בה. המסמך ממפה את סוגי שירותי הרפואה מרחוק העיקריים המסופקים כיום בישראל, סוקר את הוראות הדין הרלוונטיות למתן שירותים אלו, ומציג מספר המלצות מרכזיות ביחס אליהם. המסמך מחדד גם את החובות המוטלות על **ארגוני הבריאות** שהם **ספקי השירות** (מרפאות, קופות חולים ובתי חולים, פרטיים וציבוריים), **ספקים חיצוניים** (חברות מסחריות המספקות את התשתית הטכנולוגית, הפלטפורמה והמכשירים הרפואיים המקוונים בהם נעשה שימוש במסגרת השירות), ועל **מטפלים**.[4]

5. יובהר כי מטרת המסמך אינה להגביל את השימוש בשירותי הרפואה מרחוק אלא להבטיח כי שימוש זה ייעשה תוך מתן התייחסות הולמת לסוגיית ההגנה על פרטיותם של מטופלים.

---

[1] סוגיה זו מוגדרת גם כמתן טיפול רפואי מרחוק, טלה-בריאות וטלה-רפואה. על היקף השימוש בשירותי רפואה מרחוק בארץ ובעולם ובדגש על תקופת ההתמודדות עם משבר הקורונה, ראו קובי גלזר ״השלכת מגפת הקורונה על רפואה מרחוק – אתגרים והזדמנויות״ **חידושים בניהול** 8, 78 (2021).

[2] תמר תבורי ״היבטים משפטיים בטלה-רפואה״ **הרפואה** 159, 898, 898 (2020).

[3] ראו סע׳ 3 לחוזר מנכ״ל ״אמות מידה להפעלת שירות בריאות מרחוק (טלה-בריאות/טלה-רפואה/Telemedicine)״ (26.5.2019), (להלן: ׳חוזר מנכ״ל אמות מידה להפעלת שירות בריאות מרחוק׳).

[4] יובהר כי ההגדרות שבסעיף זה מבוססות ככלל על ההגדרות בחוזר מנכ״ל משרד הבריאות 2/2001 ״שימוש במחשוב ענן במערכת הבריאות״. עוד יובהר כי במסמך זה, רופא עצמאי המעניק שירות של רפואה מרחוק נחשב הן מטפל והן ספק השירות.

PPA@justice.gov.il | 02-6467064 | 073-3928555
WWW.PPA.JUSTICE.GOV.IL | 6107202 קרית הממשלה, ת.ד. 7360, תל אביב

רפואה מרחוק – מיפוי סוגי השירותים

6. ככלל, שירותי רפואה מרחוק המסופקים כיום בישראל ניתנים לחלוקה למספר סוגי שירותים:[5]

א. הצגת מידע רפואי וביצוע פעולות מרחוק – שירות זה כולל אפליקציות ואתרי אינטרנט להצגת מידע רפואי על אודות מטופל (כגון מרשמים ותוצאות בדיקות), המאפשרים גם ביצוע פעולות שונות מצד המטופל, כגון קביעת תורים והזמנת תרופות "עד הבית". כך לדוגמה, תחת שירות זה יכול מטופל להיכנס לאתר האינטרנט של קופת החולים בה הוא חבר, לצפות בתוצאות בדיקות הדם שהוא ערך לאחרונה ולקבוע תור לרופא מומחה.

ב. מפגש וירטואלי בין מטופל למטפל בזמן אמת (סינכרוני) – שירות המאפשר מפגש מקוון (On-line) בזמן אמת בין מטופל למטפל הנמצאים במקומות גיאוגרפיים שונים. ככלל, המפגש מתקיים באמצעות שיחות וידאו ולרבות באמצעות אפליקציה ייעודית המותקנת במחשב או בנייד, כגון האפליקציות הייעודיות של קופות החולים. במסגרת זו המטפל יכול לראות ולשמוע את המטופל, להציע אבחנה רפואית ביחס למצבו, ולתת הנחיות ביחס להמשך הטיפול בו.

שירות זה יכול להינתן גם באמצעות מכשירי בדיקה רפואיים מקוונים (Connected Medical Devices), המיועדים לשימוש ביתי (להלן: 'מכשירים רפואיים מקוונים'). מכשירים אלו, המחוברים לרשת באמצעות אפליקציה ייעודית, מאפשרים למטפל לבדוק את המטופל בזמן המפגש המקוון ולקבל חיווי ביחס למצבו, וזאת בדומה לנעשה בפגישה פיזית.[6] מכשירים אלו מאפשרים צפייה, מדידה, עיבוד והצגה של נתונים פיזיולוגיים של המטופל. המכשירים מאפשרים, בין היתר, בדיקה של קצב לב (דופק), של טמפרטורת גוף, של מצב הריאות וקצב הנשימה, וכן של מצב הגרון, האוזניים והעור. המידע הנקלט והנאסף על-ידי המכשיר (לרבות צילומי סטילס וצילומי דימות) מועבר מידית ובאופן מקוון למטפל, אשר נעזר בו על מנת לאבחן בזמן אמת את מצבו הרפואי של המטופל.

ג. בדיקה עצמית לשם התייעצות, אבחון או טיפול במועד מאוחר יותר (א-סינכרוני) – שירות זה מתייחס לשימוש עצמאי של מטופל באפליקציות או מכשירי בדיקה רפואיים מקוונים לניטור מצבו הרפואי, שלא בזמן מפגש מקוון עם מטפל. במסגרת זו המטופל משתמש במכשירים שונים - כדוגמת ערכות ביתיות לבדיקת שתן ומערכות של אולטרסאונד ביתי למעקב אחר התפתחות היריון - על-פי הצורך ומצבו הרפואי. המידע הרפואי שנקלט ונאסף על-ידי המכשירים מועבר באופן מקוון למטפל, אשר בתורו (ובמועד שונה ממועד השימוש

[5] הסיווג נועד לשם הבהרה וחידוד בנוגע לסוגי שירותי הרפואה מרחוק המסופקים כיום בישראל ובעולם. הסיווג אינו מחייב וניתן כמובן לסווג את השירותים גם באופנים אחרים.

[6] על-פי רוב, תפעול המכשיר נעשה על-ידי המטופל ובהנחיית המטפל.

PPA@justice.gov.il | 02-6467064 | 073-3928555
WWW.PPA.JUSTICE.GOV.IL | 6107202 קרית הממשלה, ת.ד. 7360, תל אביב

של המטופל במכשיר הבדיקה), משתמש במידע למעקב אחר מצבו של המטופל ולמתן אבחנה רפואית ביחס אליו.[7]

ד. מעקב וניטור רפואי מתמשך באמצעות מכשירים לבישים או מושתלים – שירות זה מאפשר ניטור מתמשך של מצב בריאותו של מטופל כאשר הוא נמצא מחוץ למוסד רפואי, וזאת באמצעות מכשירי בדיקה רפואיים מקוונים לבישים (Wearables) או כאלו המושתלים בגופו. מכשירים אלו אוספים מידע על אודות מצב המטופל באופן תדיר ושולחים את המידע באופן מקוון לגורם המטפל, לעיתים על ידי שליחת המידע תחילה לטלפון הנייד של המטופל (ולאפליקציה ייעודית בו) ומשם למטפל. בין מכשירים אלו ניתן למצוא קוצבי לב מקוונים ומוניטורים של רמות גלוקוז בדם. יצוין כי מכשירים רפואיים מסוימים פועלים על בסיס ניטור המידע המתמשך גם לשם מתן טיפול רפואי, כגון מכשיר המזריק אינסולין לגופו של מטופל באופן אוטומטי כאשר הוא מזהה צורך רפואי בכך על בסיס המידע המנוטר על ידו, או על-ידי מכשיר אחר. גם המידע הנאסף על ידי מכשירים אלו מתועד וסביר כי מועבר לגורם המטפל.[8]

ה. שירות אבחון ראשוני מבוסס בינה מלאכותית – שירות זה מתייחס לשימוש מטופלים באלגוריתם "לומד" מסוג בינה מלאכותית, המנתח מידע רפואי ממקורות שונים במטרה לזהות דפוסים חוזרים, ועל-פיהם להציע אבחנה רפואית וטיפול אפשרי.[9] מערכות אלו משתמשות בנתונים אגרגטיביים,[10] על אודות כמות גדולה של מטופלים השמורים במאגרי המידע שברשותן לניתוח תסמינים של מטופל ספציפי, ועל יסוד כך להציע לו אבחנה רפואית בדבר מצבו.[11] מטופל המשתמש במערכת שכזו "מכניס" למערכת, באמצעות המכשיר החכם שברשותו, מידע (לרבות תמונות) בדבר התסמינים אותם הוא חווה, כגון כאבי ראש תכופים או היווצרותה של פריחה בגוף. המערכת מנתחת את המידע על יסוד נתונים נוספים הנוגעים למטופל (ההיסטוריה הרפואית שלו וכדומה), ועל יסוד נתונים וממצאים של מטופלים אחרים בעלי תסמינים ונתונים דומים. על יסוד ניתוח זה מציעה המערכת למטופל אפשרויות שונות בנוגע למצבו הרפואי ובנוגע להמשך הטיפול (כגון, המלצה לפנות לרופא מומחה בתחום ספציפי).

---

[7] הליך ההתייעצות ומתן האבחנה על בסיס המידע שהועבר יכולים להיערך גם בשיחה טלפונית בין המטפל למטופל.

[8] יצוין כי סיכוני אבטחת המידע בשירותים אלו עשויים להיות גבוהים ביותר, שכן חדירה למכשירים אלו והשתלטות עליהם מרחוק, עלולות להביא לפגיעה בבריאות המטופל, ואף למותו.

[9] נושא זה מוגדר לעיתים כהחלטות אלגוריתמיות, קרי, החלטות בעניינו של אדם המתקבלות על סמך ניבוי סטטיסטי המבוצע בידי אלגוריתם, בעקבות ניתוח מידע בעניינו של אותו אדם. להרחבה בעניין זה ראו: מעיין פרל "פרטיות, שליטה ופיקוח בעידן של נתוני עתק: חובת הנמקה על החלטות אלגוריתמיות" **משפט, חברה ותרבות** ב 167 (2019). לעניין זה ראו גם הוראות סעיף 22 ל- GDPR, המתייחסות לזכויות נושא מידע במסגרת הלכי קבלת החלטות אוטומטיות.

[10] נתונים אגרגטיביים הם מידע מצרפי (או מקובץ) שאינו אישי על אודות אדם, כגון גילו, ארץ מוצאו, אזור מגוריו.

[11] יובהר שפסקה זו אינה עוסקת בשימוש במערכות של בינה מלאכותית לצרכי מחקר, אלא בבינה מלאכותית המשמשת לשם קביעת אבחנה או המלצה לטיפול במטופל קונקרטי.

רפואה מרחוק – סיכונים מרכזיים לפרטיות

7. מידע רפואי על אודות אדם הוא מידע אישי רגיש ביותר. זליגתו וחשיפתו של מידע זה – כגון מידע על מחלותיו של אדם, אופי הטיפול הרפואי אותו הוא מקבל, או מידע בדבר ההיסטוריה הרפואית שלו – עלולים לפגוע במטופל ולהשפיע על מישורים רבים של חייו.[12]

בהתאם לכך, אף נקבע בחוק הגנת הפרטיות כי "**מידע אישי המתייחס למצב בריאותו של אדם, ובכלל זה מידע רפואי כהגדרתו בחוק זכויות החולה, התשנ"ו-1996**" הוא בגדר "**מידע בעל רגישות מיוחדת**", על כל המשתמע מכך לעניין חוק זה.

8. מתן שירותי רפואה מרחוק ובאופן מקוון כרוך באיסוף, תיעוד, שמירה ועיבוד של מידע רפואי על אודות מטופלים. ככלל, מידע זה נאסף ונשמר הן על-ידי הגורם המספק את השירות (כגון ארגוני בריאות) והן על ידי ספקים חיצוניים כגון החברות המספקות והמפעילות את הפלטפורמות והמכשירים הרפואיים המקוונים בהם נעשה שימוש במסגרת השירות. המידע נשמר במאגרי מידע ובמקרים מסוימים מאוחסן בשירותי ענן שונים.

9. מצב זה מציב מספר סיכונים לפרטיות המטופלים:

א. <u>זליגת מידע</u> – **שירותי רפואה מרחוק, המסופקים באופן שאינו מאובטח דיו, עלולים להביא לזליגתו ולחשיפתו של מידע רפואי רגיש, וזאת כתוצאה מכשלי אבטחת מידע**.

מצב שכזה עלול להתרחש, לדוגמה, כתוצאה מפריצה לרשת האינטרנט הביתית של המטופל (במיוחד אם מדובר ברשת אלחוטית, Wi-Fi, שאינה מאובטחת דיה), מפריצה למכשירים החכמים של המטופלים או למכשירים הרפואיים ולאפליקציות הייעודיות בהם נעשה שימוש במסגרת השירות, וכתוצאה מפריצה לשירותי הענן ולמאגרים בהם שמור המידע.

זליגת מידע עלולה להתרחש גם כתוצאה מהתנהלות המטפל או המטופל. לדוגמה, זליגת מידע עלולה להיגרם כתוצאה מאי-יציאה מסודרת של הגורם המטפל מהמערכת בתום השימוש, או כתוצאה משימושו במערכות לא מאובטחות. גם התנהלות לא בטוחה מצד המטופל (כגון העדר הגנה על סיסמת חשבון המשתמש שלו לאתר קופת החולים באופן שהביא לחשיפתה, או הימנעות מהתנתקות מהאתר/אפליקציה בסיום השימוש), עלולה להביא לזליגת מידע רגיש על אודותיו ועל אודות אחרים שפרטיהם שמורים בחשבונו, כגון ילדיו הקטינים.

ב. <u>ערכו הכלכלי של מידע רפואי</u> – בעידן המידע, מידע אישי הוא בעל ערך רב לגורמים שונים ומגוונים. הדבר נכון ביתר שאת ביחס למידע רפואי. מידע זה עשוי להיות בעל ערך כלכלי רב לגורמים שונים כגון חוקרים וחברות מסחריות (לרבות חברות טכנולוגיה וחברות תרופות), המבקשים להשתמש במידע לפיתוחים רפואיים וטכנולוגיים חדשניים. כמו כן,

[12] על רגישותו של מידע רפואי ועל הצורך להגן עליו ניתן ללמוד, בין היתר, מפסיקת בית המשפט העליון, אשר קבע כי "פרטים רפואיים מצויים בליבת הפרטיות, ועל כן יש לצמצם במידת האפשר את חשיפתם". ראו רע"א 8019/06 **ידיעות אחרונות בעמ' נ' לוין**, פסקה ב' לפסק דינו של השופט (כתוארו אז) א' רובינשטיין, (פורסם בנבו, 13.10.2009).

בשל רגישותו של המידע, מאגרי מידע רפואי הם יעד מבוקש לגורמים עבריינים, העלולים לחדור למידע ולאיים בחשיפתו, תוך דרישת כופר בסכום כספי משמעותי.

משמעות הדבר היא שלגורמים רבים יש אינטרסים, לגיטימיים ופסולים, באיסוף מידע רפואי בהיקף רב ככל האפשר, ולשימוש בו למטרות מגוונות. מצב זה מגביר את הסיכון להתרחשות אירועי אבטחת מידע במאגרי מידע רפואי, ולשימוש במידע שכזה בניגוד להוראות הדין ותוך פגיעה בפרטיות מטופלים.

ג. <u>העדר מודעות מטופלים לאיסוף מידע ולמטרות השימוש בו</u> – כאמור, מידע אישי ורפואי על אודות מטופלים - שנוצר ונחשף בעת מתן הטיפול מרחוק – נשמר לא רק במאגרי מידע של ארגוני הבריאות אלא גם במאגרים של ספקים חיצוניים המספקים בפועל את שירותי הרפואה מרחוק.[13] כך לדוגמה, השימוש שעושה מטופלת במכשיר רפואי מקוון מסוג בדיקת אולטרסאונד ביתית, כחלק ממעקב ההיריון שלה ולשם שליחתו לבחינת הגורם המטפל, יביא לאיסוף ולשמירת מידע על אודותיה גם במאגרי המידע של החברה המספקת את השירות לקופת החולים. הסכמת מטופלים לאיסוף המידע ניתנת לרוב במסגרת הליכי הרישום לשירות, הורדת האפליקציה הייעודית, או רכישת המכשירים הרפואיים. במקרים רבים, הסכמה זו ניתנת בנוסף להסכמה לקבלת השירות מטעם ספק השירות עצמו.

בנסיבות אלו, קיים חשש כי מטופלים המשתמשים בשירות אינם מודעים לכך שמידע על אודותיהם נאסף לא רק על-ידי ארגוני הבריאות, אלא גם על-ידי ספקים חיצוניים. כפועל יוצא מכך, מטופלים רבים עלולים שלא לדעת איזה מידע על אודותיהם נאסף על ידי הספקים, ולאילו מטרות. מכאן קצרה הדרך גם לשימוש לרעה במידע, או לשימוש למטרה אחרת מזו שהמטופל הסכים לה. מקרים שכאלו קרו בעבר.[14]

מקרה מיוחד שבו חשש זה בא לידי ביטוי הוא שירותי אבחון רפואי המבוססים על מערכות של בינה מלאכותית ואלגוריתם "לומד". מאפיין מרכזי של מערכות אלו, המוגדרות לעיתים כ"קופסה שחורה", הוא שאופן ניתוחן את המידע הנאסף על-ידן אינו שקוף ואינו

[13] במקרים רבים, שירותי הרפואה מרחוק ניתנים בפועל על-ידי ספקי משנה שלהם האמצעים והידע הטכנולוגי למתן השירותים. על-פי רוב, מדובר בחברות פרטיות המתקשרות בהסכם עם ארגוני הבריאות (כגון קופות החולים), לאספקת השירות למטופלים. במצב זה, שימוש מטופלים בשירותי הרפואה מרחוק מביא גם לאיסוף מידע על אודותיהם על-ידי ספקים אלו.

[14] בשנת 2016 ניהלה הרשות להגנת הפרטיות חקירה אודות פרשה של סחר במידע רפואי רגיש על אודות חולים קשישים מאושפזים ("פרשת והדרת"). החקירה חשפה כי המעורבים, ביניהם – עובדי בית חולים בצפון הארץ, עובד בכיר בקופת חולים, ועובדי חברת שירותי טלרפואה – מכרו מידע רפואי על אודות מטופלים לידי חברות סיעוד, אשר רכשו את המידע על מנת לבצע שיווק ממוקד למטופלים. הסחר במידע הרפואי נעשה ללא ידיעה או הסכמה של המטופלים; בשנת 2017 חקרה הרשות להגנת הפרטיות עבירות פרטיות שבוצעו ממניע אחר, שאינו כלכלי. החקירה ("פרשת אנשים טובים") חשפה כי מזכירה רפואית העבירה מידע רגיש על אודות נשים שהתכוונו לבצע הפלה לידיהן של מנהלות עמותה אשר פעלה להניא נשים מביצוע הפלות. נגד מוסרת המידע ונגד מקבלות המידע הוגשו כתבי אישום, וההליך הפלילי עודנו מתנהל. לפירוט ולהרחבה בדבר שתי הפרשות, ראו: https://www.gov.il/he/departments/general/criminal_enforcement_files.

בהיר דיו.[15] במציאות שכזו, עשוי להתעורר קושי למטופל לדעת איזה מידע על אודותיו נאסף על-ידי המערכת, מה ייעשה עם המידע שלו, ולאיזו מטרה.

יש לזכור כי העובדה שמטופלים אינם יודעים כי מידע הנוגע אליהם נשמר במאגרי מידע מסוימים, מביא לכך שהם לא יוכלו לכלכל את צעדיהם ולנקוט בפעולות לצמצום הפגיעה בפרטיותם, אם יתרחש אירוע דלף מידע ממאגרים אלו. כך לדוגמה, מטופלים שאינם יודעים כי פרטיהם האישיים (כגון סיסמאות) שמורים במאגר של ספק משנה, לא יפעלו לצמצום הפגיעה בפרטיותם במקרה של אירוע דלף מידע מן המאגר, גם אם ישמעו על האירוע. זאת, להבדיל מאירוע דלף מידע ממאגר של קופת חולים, שההנחה היא כי מטופלים יודעים שמידע על אודותיהם שמור בו.

ד. חשיפת מידע עודף במסגרת מפגש וירטואלי – במסגרת מפגש וירטואלי, שלרוב יחשוף בפני המטפל את סביבת ביתו של המטופל, עלולים להיחשף גם פרטים אינטימיים על אודות המטופל שלא בהכרח יהיו רלוונטיים לטיפול, וכפי הנראה לא היו מתגלים במסגרת מפגש פיזי במרפאה או בית החולים. כך לדוגמה, במסגרת המפגש הווירטואלי יכול מטפל להבחין בפרטים המעידים על נטייתו המינית של מטופל (כגון היותו מתגורר עם בן/בת זוג), אדיקותו מבחינה דתית (כגון לאור תיעוד מכשיר טלוויזיה בביתו של אדם חרדי), עמדתו הפוליטית (ככל שסביבת ביתו עשויה להעיד על כך), ומצבו הכלכלי. כלומר, המעבר למפגשים וירטואליים יוצר סיכון לחשיפת מידע "חדש", שייתכן ולא היה נחשף במסגרת מפגשים פיזיים במרפאות ובבתי חולים. שמירת מידע שכזה ושימוש בו לצרכים שונים עלולה לפגוע בפרטיות המטופל ולהשפיע על חייו בהקשרים חברתיים שונים. יצוין כי הסיכון המפורט בחלק זה נכון עקרונית גם ביחס למקרים בהם טיפול רפואי ניתן באופן פיזי בבית המטופל, וכן ביחס לפרטיות המטפלים עצמם, שבמתן טיפול רפואי במפגש וירטואלי שהם מעניק מביתם עלול להיחשף מידע רגיש על אודותיהם ועל אודות בני ביתם.

ה. חשיפת מידע בפני גורמים לא מורשים בסביבת המטפל – ככלל, טיפול רפואי מרחוק יכול להינתן על-ידי מטפל בזמן שהוא נמצא בביתו או במרחבים אחרים, לרבות מרחבים ציבוריים. לאור כך, מידע רפואי על אודות מטופל – כגון צילום גופו או פרטים רגישים אחרים אותם הוא מציין בשיחה עם המטפל – יכול להיחשף בפני גורמים לא מורשים, כגון בני ביתו של המטפל או גורמים אחרים הנמצאים בקרבה אליו בזמן הטיפול.

10. מידע רפואי כאמור הינו מידע אישי בעל רגישות מיוחדת ולזליגתו עשויות להיות השלכות קשות, הן ברמת המטופל, והן ברמת אמון הציבור במוסדות הבריאות במדינה. אי-אבטחתו כנדרש עלולה גם להביא לשיבושו, באופן העלול לשמש בסיס להחלטות רפואיות שגויות, ומכאן

[15] תבורי ציינה בעניין מערכות אלו כי: "החשש למצב הידוע כ"קופסה שחורה" בו הזיקה בין המידע שהוזן (הקלט) לתובנה ולהמלצה הרפואית שהופקה (הפלט) אינה ברורה ואינה ניתנת להסבר". תבורי, לעיל ה"ש 22, בעמ' 901.

לפגוע בבריאות מטופלים.[16] כל אלו מחדדים את הצורך לפעול בדרכים שונות לצמצום אפשרות הפגיעה בפרטיות מטופלים בעת מתן שירותי רפואה מרחוק.

רפואה מרחוק – ריכוז הוראות דין והנחיות רלוונטיות

חוק הגנת הפרטיות והתקנות שהותקנו מכוחו

11. הוראות חוק הגנת הפרטיות, התשמ"א-1981 (להלן: 'חוק הגנת הפרטיות') והתקנות שהותקנו מכוחו מעניקות התייחסות מיוחדת להגנה על מידע רפואי.

12. כאמור, על-פי ההגדרה בסעיף 3 לחוק הגנת הפרטיות, מידע אישי המתייחס למצב בריאותו של אדם, ובכלל זה מידע רפואי כהגדרתו בחוק זכויות החולה, התשנ"ו-1996 (להלן: 'חוק זכויות החולה') מהווה "**מידע בעל רגישות מיוחדת**".

13. כמו כן, על-פי התוספת הראשונה לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: 'התקנות' או 'תקנות אבטחת מידע'), **מאגר מידע שכולל מידע רפואי מחויב ברמת אבטחה בינונית ומעלה.** על-פי התקנות, מידת רגישותו של המידע השמור במאגר מהווה קריטריון ביחס לאופן יישום היבטים שונים של אבטחת מידע, כגון אופן ההתמודדות עם אירועי אבטחת מידע והאבטחה הפיזית והסביבתית של מאגר המידע. מידת רגישותו של המידע משפיעה גם על רמת אימות הזהות הנדרשת בעת מתן גישה מרחוק למאגר.[17]

חוק זכויות החולה

14. סעיף 10 לחוק זכויות החולה, התשנ"ו-1996 (להלן: 'חוק זכויות החולה') קובע באופן כללי את החובה בדבר שמירה על כבודו ופרטיותו של מטופל. סעיף 19 לחוק זה קובע חובת סודיות לפיה **על מטפלים ועובדי מוסד רפואי לשמור בסוד כל מידע הנוגע למטופל שהגיע אליהם תוך כדי מילוי תפקידם או במהלך עבודתם**.[18]

15. סעיף 20(א) לחוק זכויות החולה קובע את התנאים למסירת מידע רפואי על ידי מטפל או מוסד רפואי, בעוד סעיף 20(ג) לחוק קובע כי על גורם המקבל מידע רפואי באחד מתנאים אלו חלה חובת הסודיות הקבועה בסעיף 19. סעיף זה מטיל למעשה על ספקי משנה את החובה והאחריות לשמירתו בסוד של מידע רפואי המועבר אליהם.

---

[16] ראו סעיף 1.3 לחוזר מנכ"ל משרד הבריאות "הגנה על מידע במערכות ממוחשבות במערכת הבריאות" מיום 15.2.2015, (להלן: 'חוזר מנכ"ל הגנה על מידע').

[17] ראו לעניין זה סעיף 4.2 להנחית הרשות להגנת הפרטיות מאגרי מידע מס' 1-2010 "דרישת מינימום לתהליכי אימות זהות של נשוא מידע לצורך מתן גישה למידע שעליו במאגר מידע" (18.11.2009), (להלן: 'הנחית הרשות להגנת הפרטיות מאגרי מידע בנושא תהליכי אימות זהות').

[18] מטפל מוגדר בחוק זכויות החולה כ"רופא, רופא שיניים, סטז'ר, אח או אחות, מיילדת, פסיכולוג, מרפא בעיסוק, פיזיותרפיסט, קלינאי תקשורת, תזונאי-דיאטן, קרימינולוג קליני, פודיאטר, פודיאטר מנתח, כירופרקט, וכן כל בעל מקצוע שהכיר בו המנהל הכללי, בהודעה ברשומות, כמטפל בשירותי הבריאות".

16. סעיף 13 לחוק זכויות החולה עוסק בסוגיות ההסכמה מדעת לטיפול רפואי.[19] סעיף זה קובע כי לא יינתן טיפול רפואי למטופל אלא אם כן נתן לכך המטופל הסכמה מדעת. סעיף 13(ב) לחוק זכויות החולה קובע כי "**לשם קבלת הסכמה מדעת, ימסור המטפל למטופל מידע רפואי הדרוש לו, באורח סביר, כדי לאפשר לו להחליט אם להסכים לטיפול המוצע**". סעיף 13(ג) קובע כי "המטפל ימסור למטופל את המידע הרפואי, בשלב מוקדם ככל האפשר, ובאופן שיאפשר למטופל **מידה מרבית של הבנת המידע לשם קבלת החלטה בדרך של בחירה** מרצון ואי תלות".

<u>הנחיות משרד הבריאות</u>

17. בתאריך 5.1.2020 פרסם משרד הבריאות קוד אתי לשמירת הסודיות ופרטיות מידע אישי על אודות מטופלים (להלן: 'קוד אתי').[20] מסמך זה מציין היבטים שונים הנוגעים להגנה על פרטיות מטופלים.

הקוד מציין כי יש להקפיד, ככל האפשר, על התנהלות מכבדת השומרת על פרטיות כל אדם בעת טיפול בענייניו, ובין היתר, להקפיד על שמירת הפרטיות בעת שיחות עם מטופלים. **הקוד מציין גם שכאשר יש אישור והרשאה מטעם המטופל לחשיפת מידע אישי או רפואי על אודותיו, יש לנקוט "צעדים לצמצום הפגיעה בפרטיות למינימום ההכרחי, כגון: בקשת הסכמה לגילוי המידע, העברת מידע מצרפי/סיכומי, מחיקת פרטים העלולים לזהות את האדם או הצפנתם, צמצום היקף המידע הנמסר וכיוצא באלה, בהתאם לנושא ולהנחיות להתממה"**. כמו כן, הקוד מציין כי אדם שהסכים לגילוי מידע אודותיו רשאי לחזור בו מהסכמתו עד להפצת המידע.

18. הנחיה רלוונטית נוספת היא חוזר מנכ"ל משרד הבריאות בנושא אמות מידה להפעלת שירות בריאות מרחוק.[21] מסמך זה, החל על ארגוני ומוסדות הבריאות בישראל, קובע מספר כללים בהקשרי הגנה על פרטיות מטופלים, כגון:

א. סעיף 4.1 קובע כי ארגוני הבריאות אחראיים להבטחת איכות ובטיחות השירות הרפואי.

ב. סעיף 4.5 לחוזר קובע כי בטרם הפעלת השירות על ארגוני ומוסדות הבריאות, יש לגבש "תיק שירות טלה-רפואה", מפורט ומנומק הכולל, בין היתר, פירוט בדבר אמצעי אבטחת מידע בשירות.

---

[19] טיפול רפואי מוגדר בסעיף 2 לחוק זכויות החולה כ"לרבות פעולות איבחון רפואי, טיפול רפואי מונע, טיפול פסיכולוגי או טיפול סיעוד".

[20] https://www.health.gov.il/hozer/mk02_2020.pdf.

[21] ראו ה"ש 3. בנוסף לכך ראו גם מסמך נהלי אבטחת מידע של משרד הבריאות מחודש יולי 2015 והוראות חוזר מנכ"ל הגנה על מידע, לעיל ה"ש 16.

ג. סעיף 5.1 קובע כי על ספק השירות לקבוע נהלי עבודה שוטפת לרבות נהלים במקרים של אירוע כשל בתקשורת.[22]

ד. סעיף 5.6 קובע כי יש לוודא שימוש במערכת מאובטחת ברמת האבטחה המתאימה לסוג המידע, וכי ספקי שירותי הבריאות בישראל נדרשים להיות מוסמכים בתקני אבטחת המידע הבינלאומיים, ISO 27799, ו-ISO 27001. הסעיף מבהיר כי באחריות ספקי השירותים לוודא הפעלה תדירה וסדירה של מערכי פיקוח ובקרה על מנגנון ההתקשרות לאתר.

ה. סעיף 5.8 לחוזר קובע כי ספק השירות יקבל הסכמה מדעת מהמטופל בטרם מתן השירות, וכי על הספק לפרסם מסמך הסכמה מדעת אשר יפרט, בין היתר, את "מגבלות המערכת בתחומי שמירה על פרטיות וחיסיון רפואי ואפשרות אירועי כשל תקשורתי". הסעיף מציין גם כי יש ליידע את המטופל בדבר האחריות שלו לפרטיותו בכל הנוגע למידע המופיע בצג הדיגיטלי האישי, ואפשרות הגישה למידע או לשירות.

<u>מסמך כללי אתיקה – ההסתדרות הרפואית בישראל</u>

19. מסמך רלוונטי נוסף הוא מסמך כללי אתיקה במתן שירותי רפואה מרחוק מטעם ההסתדרות הרפואית בישראל, העוסק באחריות רופאים במסגרת מתן טיפול רפואי מקוון.[23]

20. המסמך מבהיר כי על הרופא המטפל חלה אחריות מקצועית בעת מתן ייעוץ וטיפול מרחוק, וכי על ה"רפואה הווירטואלית" חלים כל כללי האתיקה. המסמך מציין כי על פי כללים אלו, **רופא יימנע ממתן ייעוץ רפואי או מהעברת מידע רפואי באמצעי תקשורת מקוונים שאינם מוגנים על ידי מערכת אבטחה ממוחשבת התואמת את רגישות המידע הרפואי**.

21. לפי המסמך, שימוש במערכות בית חולים או קופת חולים ייחשבו כעומדות בתנאי אבטחת מידע וכתואמות את רגישות המידע הרפואי. המסמך מבהיר כי "**אפליקציות ורשתות חברתיות כגון Facebook או WhatsApp אינם כלי מאובטח למתן טיפול או ייעוץ רפואי פרטני**".

22. המסמך מבהיר בהקשר זה כי הכלל היסודי בדבר שמירה על כללי אבטחת מידע ופעילות באמצעים מאובטחים בעת מתן טיפול מרחוק "מחייב גם את הרופא הפעיל באופן עצמאי".

23. **המסמך מחדד גם את הצורך בקבלת הסכמה מדעת מצד המטופל, אשר תתקבל על-ידי ספק השירות, "כמקובל באמצעים אלקטרונים וביישומים אחרים"**. המסמך מבהיר כי הסכמה לטיפול רפואי צריכה להתבסס על מידע רפואי שיימסר למטופל על ידי הרופאה "ביושר, בשקיפות, ובאופן סביר ומאוזן".

---

[22] ספק השירות עשוי להיות ארגוני בריאות או ספקים חיצוניים של ארגונים אלו המספקים בפועל את השירות.
[23] <u>ההסתדרות הרפואית בישראל, "Telemedicine כללי אתיקה במתן טיפול רפואי מרחוק" (ספטמבר 2019)</u>.

24. לגישת המסמך, הסכמה מדעת בנויה משני רבדים: האחד, הסכמה מדעת לעצם קבלת טיפול רפואי באמצעות כלים של רפואה מרחוק, והשני, הסכמה מדעת לגבי הייעוץ או הטיפול המסוים שניתן למטופל.

המסמך מציין בעניין זה כי "**ראוי כי ההסכמה לקבל טיפול מרחוק תתבקש בכל פנייה ראשונה לרופא, וראוי כי תינתן למטופל האפשרות לחזור בו מהסכמתו בכל זמן נתון**". המסמך מציע גם כי "תאופשר ברירת יציאה (Out-Opt) מתחומים מסוימים, לפי בחירת המטופל, אותם ירצה להחריג מהשימוש הכללי בטל־רפואה; ואף ניתן לקבוע כי סוגיות מסוימות יהיו טעונות הסכמה מדעת פרטנית נוספת לשימוש בטל־רפואה לגביהן".

<u>הגנה על פרטיות בשירותי רפואה מרחוק – הבהרות והמלצות</u>

<u>כללי</u>

25. על כלל הגורמים הפועלים בתחום שירותי הבריאות מרחוק להקפיד לפעול בהתאם להוראות הדין וההנחיות השונות שחלות עליהם (שחלקן צוינו במסמך זה).

26. ככלל, על כל הגורמים האוספים ומעבדים מידע רפואי על אודות מטופלים כתוצאה מהסכמתם לקבלת שירותי רפואה מרחוק, להקפיד לאסוף את המידע ולהשתמש בו **אך ורק למטרות להן העניק המטופל את הסכמתו**. כמו כן, **על ארגוני הבריאות והספקים החיצוניים מוטלת החובה לפעול לאבטחת המידע הרפואי שנאסף על ידם** במסגרת מתן שירותי רפואה מרחוק, וזאת בהתאם להוראות חוק הגנת הפרטיות והתקנות שהותקנו מכוחו, ועל-פי הנחיות משרד הבריאות.[24]

27. הרשות להגנת הפרטיות מבקשת להדגיש גם כי עריכת תסקיר השפעה על פרטיות בשלב מוקדם של תכנון מערכות המידע הינה דרך יעילה ואפקטיבית למזער את הסיכון לפגיעה בפרטיות במסגרת מתן שירותי רפואה מרחוק.[25] עריכת תסקיר שכזה הינה חלק מתפיסה רחבה יותר של עיצוב לפרטיות.[26]

להלן יפורטו המלצות והבהרות הרשות להגנת הפרטיות בהיבטים שונים הנוגעים לפרטיות מטופלים בשירותי רפואה מרחוק:

---

[24] ככלל, ספקי השירות והספקים החיצוניים אינם אחראים לאירועי אבטחת מידע המתרחשים בצדו של המטופל והנובעים מהתנהלותו, כגון דלף מידע שמקורו בכשלי אבטחת מידע במכשירו הפרטי של המטופל או ברשת בה הוא משתמש, או חשיפת מידע עודף מצד המטופל במסגרת מפגש וירטואלי. על ספקי השירות וספקי המשנה להבהיר בפני המטופל, עם קבלת הסכמתו לשירות, כי באחריותו לפעול לאבטחת המידע במכשיריו, תוך הבהרת הסיכונים המרכזיים לפרטיות הקיימים במסגרת שימוש בשירות שכזה.

[25] ראו מדריך עזר לביצוע תסקיר השפעה על הפרטיות שפרסמה הרשות להגנת הפרטיות (2022). המדריך זמין כאן.

[26] דוגמה לעיצוב לפרטיות בהקשר זה ניתן לראות בתכנון מערכת למפגש וירטואלי בין מטופל למטפל המציעה למטופל, עם התחלת המפגש ובאופן אוטומטי, להשתמש ברקע המטשטש את אפשרות הצילום של כל המתרחש מאחוריו.

PPA@justice.gov.il | 02-6467064 | 073-3928555
WWW.PPA.JUSTICE.GOV.IL | 6107202 קרית הממשלה, ת.ד. 7360, תל אביב

יידוע והסכמה לקבלת שירותי רפואה מרחוק

28. ככלל, ארגון בריאות המספק שירותי רפואה מרחוק הוא בעל השליטה במאגר המידע הרפואי שנאסף במסגרת מתן השירותים.

29. על ארגון בריאות המספק שירותי רפואה מרחוק לקבל את הסכמתם מדעת של המטופלים למתן השירותים. במסגרת קבלת ההסכמה על הארגון לפרט בפני המטופל (נושא המידע) את הנתונים הנדרשים לשם קבלת הסכמתו.[27]

30. במסגרת זו יש לפרט, לכל הפחות, איזה מידע ייאסף כתוצאה מקבלת ההסכמה, נתונים על המטרה לשמה מבוקש המידע, למי יימסר המידע, את פירוט מטרות המסירה האמורה, וכן את תוצאות אי-ההסכמה לאיסוף המידע (כגון, האם ישנה אפשרות לקבל את השירות הרפואי הרגיל, אף אם לא ניתנה הסכמה לקבלת שירותי רפואה מרחוק). בנוסף, יש ליידע את המשתמשים בדבר שמו של בעל השליטה במאגר המידע ודרכי ההתקשרות עמו, וכן ליידע אותם על קיומן של זכות עיון במידע האישי לפי סעיף 13 לחוק, ובדבר הזכות לבקש את תיקון המידע לפי סעיף 14 לחוק.[28]

31. יצוין כי סעיף 8(ד)(1) לחוק הגנת הפרטיות מבהיר כי חל איסור על עיבוד מידע אישי במאגר אם המידע "נוצר, התקבל, נצבר או נאסף בניגוד להוראות חוק זה, או להוראות כל דין אחר המסדיר עיבוד מידע". הוראה זו חלה גם בנוגע למידע שנאסף שלא מתוקף הסכמה תקפה לפי החוק, אלא אם קיימת הסמכה בדין לאיסופו והאיסוף נעשה בהתאם להוראות הדין.

32. כמו כן, מכוח הנחיות משרד בריאות שפורטו לעיל, בעת קבלת ההסכמה לשירות, או לחילופין בעת ההתחברות או הכניסה למערכת באמצעותה ניתן שירות הרפואה מרחוק, על ארגון בריאות המספק את השירות להבהיר למטופל בצורה ברורה, גם את הסיכונים הכרוכים בקבלת שירות מעין זה בכל הנוגע לאבטחת מידע.

33. במצבים מסוימים עשויים ספקים חיצוניים לשמש בעלים משותפים במאגר המידע הנאסף במסגרת שירותי הרפואה מרחוק, וזאת במשותף עם ארגון הבריאות. מצבים אלו מתרחשים בעיקרם כאשר הספקים החיצוניים מבקשים לעשות שימוש במידע **למטרות אחרות ושונות ממטרת הטיפול**, כגון לצרכי מחקר, פרסום, ייעול שירותים אחרים הניתנים על-ידו וכדומה (בתנאי שגם ספק השירות העיקרי הסכים לכך). במצבים שכאלו נדרשים ספקים חיצוניים לקבל **הסכמה ספציפית** ממטופלים לשימוש במידע למטרות אלו, וזאת בנוסף להסכמה שמעניקים המטופלים לארגון הבריאות לעצם מתן השירות.

[27] על פני הדברים יתכנו מצבים בהם שירות רפואה מרחוק יינתן במצבי חירום בהם לא ניתן לקבל את הסכמת המטופל.

[28] סעיף 11 לחוק הגנת הפרטיות. זכות מטופלים לעיון ולקבלת מידע רפואי הנוגע אליהם קבועה מפורשות גם בהוראות סעיף 18 לחוק זכויות החולה.

מעבר לכך, מכיוון שמידע רפואי הוא מידע בעל רגישות מיוחדת, ומכיוון שבמקרים רבים לא עומדת למטופלים ברירה אלא להשתמש בשירותי רפואה מרחוק לשם קבלת טיפול רפואי (כדוגמת מטופלים בעלי מוגבלויות המתקשים לצאת מביתם), **על ארגוני הבריאות המספקים את השירות להבטיח כי למטופלים תעמוד האפשרות לקבל שירותי רפואה אלו מבלי שיהיו מחויבים, דה-פקטו, להסכים גם לשימוש במידע על אודותיהם למטרות אחרות ממטרת הטיפול**. ללא אפשרות כזו יהיה קשה לראות בהסכמת מטופל לאיסוף ולשימוש במידע על אודותיו למטרות אחרות מהטיפול עצמו, כהסכמה מדעת.

במצבים בהם ספק חיצוני עשוי לבקש את הסכמת המטופל לאיסוף ולשימוש במידע מעבר לנדרש מבחינה מינימלית לצורך הטיפול - על ארגון הבריאות המספק את השירות (כגון קופת החולים) ליידע ולהבהיר למטופל שאין הוא מחויב לתת הסכמתו לשימושים הנוספים במידע אודותיו, ושהסכמה זו לא תהיה תנאי לקבלת השירות הרפואי.

34. התייחסות מיוחדת יש להעניק בעניין זה לאבחון מבוסס אלגוריתם מסוג **בינה מלאכותית**. לאור אופיו של השירות רצוי כי במסגרת הליך קבלת הסכמה לשירות יפורט, ככל הניתן, אופן פעילות המערכת והשימוש שהיא עושה במידע על אודות מטופלים. **רצוי כי פירוט זה יכלול התייחסות לסוגי המידע הנאספים במסגרת האבחון, מטרת האיסוף, אופן ניתוח המידע, וכן מה ייעשה עמו לאחר סיום האבחון**.[29]

מעבר לכך, אם במסגרת השירות נאסף מידע אישי ומזוהה (או הניתן לזיהוי) על אודות מטופל אשר אמור לשמש למטרה שונה ממטרת מתן האבחון, כגון לצרכי מחקר או לצרכי "למידה" של מערכת בינה מלאכותית, **יש להבהיר את הדברים מפורשות ולקבל הסכמה נפרדת מצד המטופל למטרה זו**.[30]

<u>צמצום מידע</u>

35. על פי עיקרון צמצום המידע העודף, **על כלל הגורמים להימנע ככל הניתן מאיסוף ושמירה של מידע על אודות מטופלים שאינו הכרחי למטרת השירות הרפואי מרחוק, או למטרת המאגר בו מידע זה נשמר**.[31]

36. מכוח תקנה 2(ג) לתקנות אבטחת המידע על ספקי השירות והספקים החיצוניים, בכובעם כבעלי השליטה במאגרי המידע בו נשמר מידע רפואי הנאסף במסגרת שירותי הרפואה מרחוק, לבחון, אחת לשנה, אם המידע שהם שומרים במאגר אינו חורג מן הנדרש ביחס למטרותיו.

---

[29] להרחבה בנושא זה ראו הרשות להגנת הפרטיות "חובת יידוע במסגרת איסוף ושימוש במידע אישי".

[30] לעניין זה ראו סעיפים 2(9) ו-8(ב) לחוק הגנת הפרטיות המבטאים את עיקרון צמידות המטרה לפיו מידע שנמסר למטרה מסוימת יכול לשמש אך ורק לאותה המטרה, אם נקבעה כדין.

[31] עיקרון זה מושתת על הוראות סעיף 2(9) ו- 8(ב) לחוק הגנת הפרטיות. להרחבה ראו טיוטת מסמך מדיניות הרשות להגנת הפרטיות בנושא צמצום מידע.

בעניין זה יובהר כי לגישת הרשות להגנת הפרטיות יתכנו מצבים בהם רצוי שבדיקה כזו תיערך מספר פעמים לאורך השנה וזאת, בין היתר, כתלות בסוג המידע השמור ומטרת איסופו. במקרה זה, לאור כך שמידע רפואי הוא מידע רגיש במיוחד, **מומלץ כי הבחינה תיעשה במסגרת פרקי זמן קצרים יותר מהקבוע בתקנות, קרי מספר פעמים בשנה**.

חובת מינוי ממונה על הגנת הפרטיות

37. סעיף 17ב1(א)(4) לחוק הגנת הפרטיות קובע, כי בעל שליטה או מחזיק במאגר מידע שעיסוקם העיקרי כולל עיבוד בהיקף ניכר של מידע אישי הכלול באחת או יותר מן הקטגוריות של הגדרת המונח "מידע בעל רגישות מיוחדת" מחויבים במינוי ממונה על הגנת פרטיות. בתוך כך, הסעיף קובע מפורשות כי **בית חולים וקופת חולים נכללים בקטגוריה זו וכאלו הם מחויבים במינוי ממונה על הגנת פרטיות**. יובהר כי לגישת הרשות, **עיבוד מידע רפואי על אודות מטופלים נכלל בעיסוקם העיקרי של ארגונים ומוסדות המספקים שירותי בריאות ורפואה**.

לאור האמור, **עמדת הרשות היא כי ארגונים ומוסדות המספקים שירותי בריאות ורפואה, לרבות כאלו המספקים שירותי רפואה מרחוק, מחויבים ככלל במינוי ממונה על הגנת פרטיות**.

38. תפקידי הממונה על הגנת הפרטיות מפורטים בסעיף 17ב2(א) לחוק הגנת הפרטיות. ייעודו של הממונה, כפי שנקבע ברישא לסעיף 17ב2(א) לחוק, אינו רק להבטיח את קיום הוראות החוק בארגון, אלא גם לפעול לקידום ולשיפור ההגנה על הפרטיות ואבטחת המידע בו, מעבר לדרישות הקבועות בדין.

39. משכך, לעמדת הרשות, הממונה על הגנת הפרטיות הוא הגורם המתאים לתכנון ולבחינת הצעדים הננקטים בארגון לצמצום הפגיעה בפרטיות מטופלים, לרבות במסגרת מתן שירותי רפואה מרחוק.

אחריות ספק שירות המתקשר עם ספק חיצוני למתן שירותי רפואה מרחוק

40. כפי שנטען, סביר להניח שמטופלים רבים המסכימים לקבלת שירות רפואה מרחוק אינם מודעים לכך שמידע רפואי על אודותיהם נאסף, נשמר ומעובד על-ידי ספקים חיצוניים. מצב זה מחדד את החובה המוטלת על ארגון הבריאות המספק את שירותי הרפואה מרחוק להבטיח כי התנהלות הספק החיצוני, בכל הנוגע להגנה על פרטיות מטופלים ואבטחת מידע, היא תקינה ותואמת את הוראות הדין.[32]

במובן זה, **על ארגון בריאות המתקשר עם ספק חיצוני למתן שירותי רפואה מרחוק, לרבות להספקת ולהפעלת הפלטפורמה הטכנולוגית והמכשירים הרפואיים המקוונים, מוטלות חובות שונות שעניינן פיקוח על התנהלות הספק החיצוני בהיבטי פרטיות ואבטחת מידע**.

[32] יובהר כי חובה זו אינה חלה על ארגון הבריאות במצבים בהם מטופל מתקשר ישירות עם חברה פרטית לקבלת שירות רפואי מרחוק, באופן המנותק לחלוטין מהשירות הניתן לו על-ידי ארגון הבריאות או עובדיו. במצבים אלו חובות אבטחת המידע חלות על החברה הפרטית כבעלת השליטה במאגר, וכגורם האוסף ומשתמש במידע רפואי על יסוד הסכמת המטופל.

41. תקנה 15 לתקנות אבטחת מידע מסדירה את החובות המוטלות על בעל השליטה במאגר מידע המתקשר עם גורם חיצוני לצורך קבלת שירות. התקנות מחייבות את בעל השליטה במאגר, בין היתר, לבחון, לפני ביצוע ההתקשרות עם הגורם החיצוני המסוים, את סיכוני אבטחת המידע הכרוכים בהתקשרות; לקבוע במפורש בהסכם עם הגורם החיצוני התייחסות לסוגיות כגון: המידע שהגורם החיצוני רשאי לעבד ומטרות השימוש המותרות בו לצורכי ההתקשרות; מערכות המאגר שהגורם החיצוני רשאי לגשת אליהן; סוג העיבוד או הפעולה שהגורם החיצוני רשאי לעשות; משך ההתקשרות, אופן השבת המידע לבעל המאגר בסיום ההתקשרות השמדתו מרשותו של הגורם החיצוני, חובתו של הגורם החיצוני לדווח, אחת לשנה לפחות, לספק השירות על אודות אופן ביצוע חובותיו לפי תקנות אלה וההסכם, להודיע לו במקרה של אירוע אבטחה וכדומה.

42. **ככלל, התנערות ארגון בריאות המספק שירותי רפואה מרחוק מאחריות בכל הנוגע להתנהלות ספק חיצוני בהיבטים של איסוף, שימוש, עיבוד ומסירת מידע על אודות מטופלים, עומדת בסתירה להוראות תקנה 15 לתקנות אבטחת מידע, ולחובות החלות מכוחה**. מעבר לכך, במצב בו ספק השירות הוא ארגון בריאות ציבורי (כגון קופת חולים), התנערות שכזו עשויה להוות גם הפרה של אחריותו כלפי מטופליו, החלה עליו מכוח עקרונות המשפט הציבורי.[33]

<u>אימות זיהוי וחובות אבטחת מידע</u>

43. ככלל, ארגוני הבריאות המספקים שירותי רפואה מרחוק הם בעלי השליטה במאגרים בהם נשמר המידע הרפואי שנוצר במסגרת הטיפול הרפואי. כפי שצוין לעיל, חוק הגנת הפרטיות ותקנותיו מטילים על בעל שליטה במאגר מידע רפואי חובות שונות הנוגעות לאבטחת המידע.

44. אימות זהותו של אדם בשירותי רפואה מרחוק הוא קריטי מבחינת היבטי פרטיות והגנת מידע. סעיף 5.7 לחוזר מנכ"ל משרד הבריאות בנושא אמות מידה להפעלת שירות בריאות מרחוק קובע מספר כללים בהקשר זה, החלים על ארגוני הבריאות מספקי השירותים. הסעיף קובע כי "מערכת שירותי בריאות מרחוק חייבת לכלול מנגנון לזיהוי המטפל ולזיהוי המטופל ברמת ודאות טובה, בדרגות הזדהות שונות ובאמצעים המותאמים לנסיבות ולסוג הפעולה המבוצעת".

45. בנוסף לאמור יובהר כי **תקנות אבטחת מידע מטילות על בעלי השליטה במאגרים את החובה לנקוט באמצעים מקובלים בנסיבות העניין ובהתאם לאופי המאגר וטיבו, על מנת לוודא כי הגישה למאגר ולמערכות המאגר נעשית בידי בעל הרשאה המורשה לכך בלבד לפי רשימת**

[33] יצוין כי על קופות חולים מוטלות חובות מתחום המשפט הציבורי ביחס לפעילות בה הן עוסקות. חובות כאלה מוטלות על קופות החולים ביחס לאספקת שירותים הכלולים בסל הבריאות מכוח מעמדן כגופים דו-מהותיים. ראו בג"ץ 6451/18 **חיון נ' בית הדין הארצי לעבודה** (פורסם בנבו, 19.7.2021), פס' 22 לפסק דינו של השופט גרוסקופף. למעמדן של קופות החולים כגופים דו-מהותיים ראו אסף הראל **גופים ונושאי משרה דו-מהותיים**, 91-94, 551-556 (2019).

ההרשאות התקפות.[34] מכיוון שמאגרי מידע רפואי הם מאגרים שחלה עליהם רמת אבטחה בינונית ומעלה, על בעלי השליטה במאגרים לעמוד בכללים המפורטים בהקשר זה בתקנה 9(ב) לתקנות אבטחת מידע.[35]

46. הכללים האמורים חלים בשירותי רפואה מרחוק המאפשרים למטופלים גישה מרחוק למאגר המידע, כגון שירותים המאפשרים הצגת מידע רפואי וביצוע פעולות מרחוק. **מכיוון שמכשירים רפואיים מקוונים מאפשרים גם הם חיבור מרחוק למאגרי המידע, עמדת הרשות להגנת הפרטיות היא כי מכשירים אלו נחשבים 'מערכות מאגר', על כל המשתמע מכך מבחינת אימות זיהוי מטופלים המשתמשים במכשירים אלו, וחובות האבטחה המוטלות על מערכות מאגר לפי תקנות אבטחת מידע**.[36]

47. הרשות מבקשת להבהיר גם כי מידע רפואי הנאסף במסגרת מתן שירותי רפואה מרחוק, מעבר להיותו מידע בעל רגישות מיוחדת על פי חוק הגנת הפרטיות, **עשוי להיחשב גם חלק מ"רשומה רפואית" ממוחשבת** לפי פרק ה' לחוק זכויות החולה. כפועל יוצא מכך, שמירת והעברת המידע האמור כפופות לא רק לחובות אבטחת המידע לפי תקנות אבטחת מידע, אלא גם להנחיות משרד הבריאות בנושא רשומות רפואיות, שמירתן ואופן אבטחתן.[37]

<u>סיום שימוש במכשירים רפואיים מקוונים וגריעתם</u>

48. בעת שימוש במכשירים רפואיים מקוונים בשירותי רפואה מרחוק, נשמר בזיכרון המכשירים מידע רפואי אישי ורגיש על אודות מטופלים. מצב זה מעלה חשש לזליגת המידע במצבים בהם מכשירים אלו מגיעים לסוף דרכם (End of Life), קרי כאשר הם אינם משמשים עוד את הגורם הרפואי וכפועל יוצא נגרעים או נמכרים לגורמים שונים.

---

[34] ראו לדוגמה, המלצות מערך הסייבר הלאומי בנושא "חיזוק זיהוי משתמשים במערכות ותשתית של ארגונים ע"י שימוש באימות רב-גורמי" (מאי 2020).

[35] בהתאם להוראת תקנה 9(ב) לתקנות אבטחת מידע, במאגר מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה, אופן הזיהוי ייעשה ככל האפשר על בסיס אמצעי פיזי הנתון לשליטתו הבלעדית של המורשה; ייקבעו בנוהל האבטחה גם הוראות בנושא זה, ובכללן בנושאים אלה: (א) אופן הזיהוי; היה אופן הזיהוי מבוסס על סיסמאות, יתייחס הנוהל גם לחוזק הסיסמה, מספר הניסיונות השגויים, ותדירות החלפת הסיסמאות שתיעשה בהתאם לתפקיד מורשה הגישה, ובכל מקרה לתקופה שלא תעלה על שישה חודשים; (ב) ניתוק אוטומטי לאחר פרק זמן של אי-פעילות; (ג) אופן הטיפול בתקלות הקשורות באימות זהות.

[36] יובהר כי הכוונה כאן היא למכשירים רפואיים מקוונים המסופקים על-ידי ספקי השירות או הספקים החיצוניים (כגון מכשיר אולטרסאונד ביתי המעביר מידע רפואי ברשת, מבית המטופלת לגורם המטפל שבארגון הבריאות), ולא למכשירי הקצה של המטופלים, כגון הטלפונים החכמים שבהם הם עשויים להשתמש לצורך קבלת השירות.

[37] ראו לדוגמה "אמות מידה לניהול רשומת מטופל במערכת הבריאות" שפורסמו על ידי משרד הבריאות ביום 15.12.2019.

49. לאור כך **מומלץ כי ארגוני הבריאות המספקים את השירות והספקים החיצוניים יקבעו נהלים לאבטחת המידע האמור במועד הפסקת השימוש במכשירים האמורים וגריעתם, לרבות נהלים להשמדת המידע השמור בהם.**[38]

<u>היבטי פרטיות במפגש וירטואלי</u>

50. **על מטפלים להקפיד על כללי אבטחת המידע בתוכנות ובמכשירים הטכנולוגיים בהם הם משתמשים במסגרת המפגש הווירטואלי**. כך לדוגמה, יש לוודא שתוכנות ומכשירים אלו יישמרו במקום מוגן ותחת סיסמה שבכוחם למנוע חדירה וכניסה אליהם בלא הרשאה מתאימה.

כמו כן, בעת מפגש וירטואלי מומלץ שלא להשתמש ברשתות Wi-Fi ציבוריות, אלא ברשת פרטית המוגנת בסיסמה ובתוכנות הגנה כגון אנטי-וירוסים וחומת אש.

51. ככלל, בעת מפגש וירטואלי על מטפלים להיות מודעים לכך שסרטון הווידאו של המפגש, והמידע הנחשף במסגרתו, עלולים, בנסיבות מסוימות, לזלוג ולהיחשף. לפיכך, **מומלץ כי מטפלים ינקטו משנה זהירות ויימנעו מלנקוט פעולות העלולות לחשוף את מטופליהם, מעבר לנדרש במסגרת הטיפול הרפואי**. כך לדוגמה, בעת בדיקה גופנית, רצוי להימנע מחשיפה של אזורים אינטימיים בגוף המטופל, אלא אם חשיפה זו נדרשת מבחינה רפואית.

52. **כמו כן מומלץ כי מטפלים יסבו את תשומת לב מטופליהם כאשר אלו חושפים את עצמם, או את בני-ביתם, שלא לצורך**. לדוגמה, אם בעת מפגש וירטואלי מציב מטופל את מצלמת הווידאו שלו באופן החושף ברקע את בני-משפחתו, מומלץ כי המטפל יציין את הדברים בפני המטופל, ויציע לו לשנות את זווית הצילום, ככל שהדבר אפשרי.[39]

53. **ראוי שמטפלים ינקטו בכל הפעולות הנדרשות על מנת להימנע מכך שגורמים הנמצאים בקרבתם ייחשפו לדברי מטופלים או לתמונות ולסרטוני הווידאו שלהם**. כך לדוגמה, מומלץ שמטפלים ישתמשו באוזניות, יימנעו מלהשתמש ברמקול ויקפידו בעת המפגש לשבת לבד ובחדר סגור.[40] בד בבד, חשוב להבהיר גם למטופל כי חשיפת מידע שאינו נדרש לצורך מתן הטיפול, כגון צילום בני ביתו ברקע במהלך הטיפול, עלול כשלעצמו לפגוע בפרטיות.

54. **מומלץ שמטפלים יפעלו לחיזוק כישוריהם הטכנולוגיים בכל הנוגע לשליטה במערכות המשמשות את המפגש הווירטואלי**. חיזוק זה עשוי לצמצם מצבים בהם מידע רגיש על אודות מטופלים זולג כתוצאה מטעויות אנוש כגון אי-יציאה מסודרת מהמערכת, מתן הרשאות גישה

---

[38] על-פי תקנה 15(א)(2)(ד) לתקנות אבטחת מידע, בעל שליטה במאגר מידע המתקשר עם גורם חיצוני לצורך קבלת שירות יקבע במפורש בהסכם עם הגורם החיצוני את משך ההתקשרות ביניהם, את אופן השבת המידע לידיו בסיום ההתקשרות, ואת השמדתו של המידע שבידי הגורם החיצוני.

[39] אין בדברים כדי להטיל אחריות על מטפל או ספק שירות לפגיעה בפרטיות המתרחשת כתוצאה מחשיפת מידע עודף בצדו של המטופל במסגרת מפגש וירטואלי.

[40] המלצות מסוג זה מפורטות במאמרה של תבורי, לעיל ה"ש 22, בעמ' 900.

לגורמים לא מורשים וכדומה. **בעניין זה רצוי גם כי ספקי השירות הרפואי, שהמטפלים פועלים במסגרתם, יפעלו להכשרת המטפלים מבחינה טכנולוגית ולפיקוח על התנהלותם בהקשרים שפורטו לעיל**.

<u>סיכום</u>

55. מתן שירותי רפואה באופן מקוון כרוך באיסוף, תיעוד, שמירה ועיבוד של מידע רפואי על אודות מטופלים. לשירותי רפואה מרחוק יתרונות רבים. עם זאת, השימוש בהם טומן בחובו גם אתגרים שונים מבחינת הגנה על פרטיותם של מטופלים ועל מידע הנוגע אליהם.

56. במסמך זה סקרה הרשות להגנת הפרטיות את הסיכונים לפרטיות הכרוכים במתן שירותי רפואה מרחוק ואת הוראות הדין הרלוונטיות לנושא לרבות בנוגע לחובת מינוי ממונה הגנת פרטיות, וכן הציגה המלצות להתנהלות מיטבית בהקשר זה בנושאי ההסכמה לקבלת השירות, צמצום מידע, מיקור חוץ, אימות זיהוי, סיום שימוש במכשירים רפואיים מקוונים, וביחס להיבטי פרטיות במפגש וירטואלי.

נספח א

הבהרות והמלצות לספקי שירותי רפואה מרחוק ולספקים חיצוניים

יידוע והסכמה לקבלת שירותי רפואה מרחוק

- על ארגון בריאות המספק שירותי רפואה מרחוק לקבל הסכמת מטופלים למתן השירותים. במסגרת קבלת ההסכמה על הארגון לפרט בפני המטופל (נושא המידע) את הנתונים הנדרשים לשם קבלת הסכמתו, כגון נתונים על המטרה לשמה מבוקש המידע, למי יימסר המידע, מטרות המסירה האמורה, וכן את תוצאות אי-ההסכמה לאיסוף המידע (כגון, האם ישנה אפשרות לקבל את השירות הרפואי הרגיל, אף אם לא ניתנה הסכמה לקבלת שירותי רפואה מרחוק). בנוסף, יש ליידע את המשתמשים בדבר שמו של בעל השליטה במאגר המידע ודרכי ההתקשרות עמו, וכן ליידע אותם על קיומן של זכות עיון במידע האישי לפי סעיף 13 לחוק, ובדבר הזכות לבקש את תיקון המידע לפי סעיף 14 לחוק.

- בעת קבלת ההסכמה לשירות, או לחילופין בעת ההתחברות או הכניסה למערכת באמצעותה ניתן שירות הרפואה מרחוק, על ארגון בריאות להבהיר למטופל בצורה ברורה גם את הסיכונים הכרוכים בקבלת שירות מעין זה בכל הנוגע לאבטחת מידע.

- יובהר כי איסוף מידע שאינו תואם להסכמה שניתנה עלול להוות הפרה של הוראות הדין.

- ספקים חיצוניים המבקשים להשתמש במידע על אודות מטופלים שנאסף במסגרת שירותי רפואה מרחוק **למטרות אחרות ושונות ממטרת הטיפול** (כגון לצרכי מחקר, פרסום, ייעול שירותים אחרים הניתנים על-ידו) צריכים לקבל את אישור ארגון הבריאות לכך, וכן לקבל ממטופלים **הסכמה ספציפית למטרות אלו** (בנוסף להסכמה לעצם מתן השירות אותה הם העניקו לארגון הבריאות).

- **על ארגוני הבריאות המספקים שירותי רפואה מרחוק להבטיח כי למטופלים תעמוד האפשרות לקבל שירותי רפואה מרחוק מבלי שהם יהיו מחויבים, דה-פקטו, להסכים גם לשימוש של ספקים חיצוניים במידע על אודותיהם למטרות אחרות ממטרת הטיפול**.

- על ארגוני בריאות המאשרים לספקים חיצוניים לבקש ממטופלים את הסכמתם לשימוש במידע למטרות אחרות ממטרת הטיפול, ליידע ולהבהיר למטופלים שהם אינם מחויבים לתת הסכמתם לשימושים הנוספים במידע על אודותיהם, ושהסכמה זו לא תהיה תנאי לקבלת השירות הרפואי.

- ביחס לאבחון מבוסס אלגוריתם מסוג בינה מלאכותית כגון מערכות אוטומטיות לאבחון רפואי על סמך ניתוח תסמינים - רצוי כי פירוט זה יכלול התייחסות לסוגי המידע על אודות מטופלים הנאספים במסגרת האבחון, מטרת האיסוף, אופן ניתוח המידע, וכן מה ייעשה עמו לאחר סיום האבחון. אם במסגרת השירות נאסף מידע אישי ומזוהה (או הניתן לזיהוי) על אודות מטופל

PPA@justice.gov.il | 02-6467064 | 073-3928555
WWW.PPA.JUSTICE.GOV.IL | 6107202 קרית הממשלה, ת.ד. 7360, תל אביב

אשר אמור לשמש למטרה שונה ממטרת מתן האבחון, יש להבהיר את הדברים מפורשות ולקבל הסכמה נפרדת מצד המטופל למטרה זו.

צמצום מידע

- בעל שליטה במאגר מידע מחויב לבדוק, אחת לשנה, האם במאגר המידע שבבעלותו נשמר מידע עודף שאינו נדרש לשם עמידה במטרת המאגר. עמדת הרשות היא כי ביחס למאגרים בהם נשמר מידע רפואי רצוי שבדיקה כזו תיערך מספר פעמים לאורך השנה.

חובת מינוי ממונה הגנת פרטיות

- על-פי הוראות חוק הגנת הפרטיות, בעל שליטה או מחזיק שעיסוקם העיקרי כולל עיבוד בהיקף ניכר של מידע רפואי חייבים במינוי ממונה על הגנת הפרטיות. החוק קובע מפורשות כי בתי חולים וקופות חולים מחויבים במינוי ממונה על הגנת הפרטיות.
- לאור האמור, **כל ארגון או מוסד רפואי המספק שירותי רפואה, לרבות שירותי רפואה מרחוק, חייב במינוי ממונה על הגנת הפרטיות**.

אחריות ספק שירות המתקשר עם ספק חיצוני למתן שירותי רפואה מרחוק

- על ארגון בריאות המתקשר עם ספק חיצוני למתן שירותי רפואה מרחוק מוטלות חובות שונות שעניינן בחינה טרם ביצוע ההתקשרות של סיכוני אבטחת המידע הכרוכים בהתקשרות ופיקוח על התנהלות הספק החיצוני בהיבטי פרטיות ואבטחת מידע, וזאת מכוח תקנה 15 לתקנות אבטחת מידע ('מיקור חוץ') והנחיית הרשות להגנת הפרטיות בעניין.[41]
- ככלל, התנערות ארגון הבריאות (ספק שירות) מאחריות בכל הנוגע להתנהלות הספק החיצוני בהיבטים של איסוף, שימוש, עיבוד ומסירת מידע על אודות מטופלים, עומדת בסתירה להוראות תקנה 15 לתקנות אבטחת מידע, ולחובות החלות מכוחה. מעבר לכך, במצב בו ספק השירות הוא ארגון בריאות ציבורי (כגון קופת חולים), התנערות שכזו עשויה להוות גם הפרה של אחריותו כלפי מטופליו, החלה עליו מכוח עקרונות המשפט הציבורי.

אימות זיהוי

- על בעלי שליטה במאגרי מידע מוטלת החובה לנקוט באמצעים מקובלים בנסיבות העניין ובהתאם לאופי המאגר וטיבו, על מנת לוודא כי הגישה למאגר ולמערכות המאגר נעשית בידי בעל הרשאה המורשה לכך בלבד לפי רשימת ההרשאות התקפות. מכיוון שמאגרי מידע רפואי הם מאגרים שחלה עליהם רמת אבטחה בינונית ומעלה, על בעלי השליטה במאגרים לעמוד בכללים המפורטים בהקשר זה בתקנה 9(ב) לתקנות אבטחת המידע.

[41] לעניין זה ראו הרשות להגנת הפרטיות "מדריך פעולה להתקשרות עם ספקי מיקור חוץ - תקנה 15 לתקנות הגנת הפרטיות (אבטחת מידע)" (ספטמבר 2023).

PPA@justice.gov.il | 02-6467064 | 073-3928555
WWW.PPA.JUSTICE.GOV.IL | 6107202 קרית הממשלה, ת.ד. 7360, תל אביב

- מכיוון שמכשירים רפואיים מקוונים מאפשרים חיבור מרחוק למאגרי המידע, עמדת הרשות להגנת הפרטיות היא כי מכשירים אלו נחשבים 'מערכות מאגר', על כל המשתמע מכך גם מבחינת אימות זיהוי מטופלים בשירותי רפואה בהם נעשה במכשירים אלו.

<u>סיום שימוש במכשירים רפואיים מקוונים וגריעתם</u>

- מומלץ כי ארגוני הבריאות והספקים החיצוניים יקבעו נהלים לאבטחת מידע במועד הפסקת השימוש במכשירים הרפואיים המקוונים וגריעתם, לרבות נהלים להשמדת המידע השמור בהם.

<u>מפגש וירטואלי</u>

- רצוי שארגוני הבריאות, שמטפלים פועלים במסגרתם למתן שירותי רפואה מרחוק, יפעלו להכשרת המטפלים מבחינה טכנולוגית ולפיקוח על התנהלותם בהקשרים של הגנה על פרטיות מטופלים ואבטחת מידע.

נספח ב

הבהרות והמלצות למטפלים במפגש מקוון

- על מטפלים להיות מודעים לכך שסרטון הווידאו של המפגש, והמידע הנחשף במסגרתו, עלולים לזלוג ולהיחשף. לפיכך, מומלץ כי מטפלים ינקטו משנה זהירות ויימנעו מלנקוט פעולות העלולות לחשוף את מטופליהם, מעבר לנדרש במסגרת הטיפול הרפואי.

- על מטפלים להקפיד על כללי אבטחת המידע בתוכנות ובמכשירים הטכנולוגיים בהם הם משתמשים במסגרת המפגש הווירטואלי. כך לדוגמה, יש לוודא שתוכנות ומכשירים אלו יישמרו במקום מוגן ותחת סיסמה המונעים חדירה וכניסה אליהם בלא הרשאה מתאימה.

- בעת מפגש וירטואלי מומלץ שלא להשתמש ברשתות Wi-Fi ציבוריות, אלא ברשת פרטית המוגנת בסיסמה ובתוכנות הגנה כגון אנטי-וירוסים וחומת אש.

- מומלץ כי מטפלים יסבו את תשומת לב מטופליהם כאשר אלו חושפים את עצמם, או את בני-ביתם, שלא לצורך.

- ראוי שמטפלים ינקטו בכל הפעולות הנדרשות על מנת להימנע מכך שגורמים הנמצאים בקרבתם ייחשפו לדברי מטופלים או לתמונות ולסרטוני הווידאו שלהם.

- מומלץ שמטפלים יפעלו לחיזוק כישוריהם הטכנולוגיים בכל הנוגע לשליטה במערכות המשמשות את המפגש הווירטואלי.

PPA@justice.gov.il | 02-6467064 | 073-3928555
WWW.PPA.JUSTICE.GOV.IL | 6107202 קרית הממשלה, ת.ד. 7360, תל אביב