14 בפברואר 2024
ה' באדר א', התשפ"ד

הגנה על פרטיות מטופלים בהעברת מידע רפואי באמצעים דיגיטליים

נוסח מעודכן בעקבות תיקון 13

רקע

1. בשנים האחרונות מתפתחת תופעה לפיה גורמים המעניקים שירותי בריאות וטיפול רפואי (להלן: 'גורמי רפואה'),[1] מעבירים מידע על אודות מטופלים באמצעות מכשירים דיגיטליים (טלפונים חכמים, מחשבי כף יד, מחשבים ניידים) ותוכנות שאינן ייעודיות להעברת מידע רפואי (כגון **WhatsApp**; **Gmail**; **Telegram**; **Signal**), וכל זאת באופן העלול לפגוע בפרטיות מטופלים.

2. תופעה זו – הנמצאת בליבת המסמך – מיוחסת להעברת מידע רפואי על-ידי גורמי רפואה בשלושה אופנים:

   א. העברת מידע באמצעות **תוכנות ייעודיות** להעברת מידע רפואי המותקנות במכשירים **דיגיטליים אישיים-פרטיים** של גורמי רפואה (להלן: 'מכשירים פרטיים');[2]

   ב. העברת מידע באמצעות **תוכנות לא ייעודיות** המותקנות במכשירים דיגיטליים **שבבעלות הארגון או המוסד הרפואי**, ושנמצאים בשימוש, לרבות שימוש אישי, של גורמי רפואה (להלן: 'מכשירים מוסדיים');

   ג. העברת מידע באמצעות **תוכנות לא ייעודיות** המותקנות במכשירים **פרטיים** של גורמי הרפואה.[3]

3. העברת המידע נעשית, בין היתר, כחלק מתקשורת של גורמי רפואה עם מטופלים וגורמי רפואה אחרים. כך לדוגמה, רופאת עור, שבמסגרת מתן טיפול רפואי מבקשת להתייעץ עם עמיתה, עשויה להשתמש בטלפון החכם שברשותה להעברת ממצאי בדיקות ותיעוד ויזואלי של גוף המטופל, באמצעות אפליקציה להעברת מסרים מסוג WhatsApp. דוגמה אחרת עשויה להיות

---

[1] במסמך זה, המונח גורמי רפואה מתייחס לכלל הגורמים המעניקים "טיפול רפואי", לרבות "מטפל", וכן עובדים מנהליים המועסקים במסגרת "מוסד רפואי" – והכל כמוגדר בחוק זכויות החולה, התשנ"ו-1996, (להלן: 'חוק זכויות החולה'). מסמך זה חל גם על גורמי רפואה הפועלים בארגונים ומוסדות פרטיים המספקים שירותי בריאות וטיפולים רפואיים, כגון עובדי חברות המפעילות אמבולנסים, עובדי מוקדי רפואה דחופה, ועל כל מטפל עצמאי המספק שירותי בריאות וטיפול רפואי.

[2] מצב בו גורמי רפואה משתמשים במכשירים אישיים-פרטיים במסגרת הליכי הטיפול הרפואי הוא חלק מתופעה נרחבת יותר הקרויה בשם BYOD (Bring Your Own Device), המתארת שימוש בכלים ובאמצעים פרטיים במסגרת מקומות עבודה, מוסדות חינוך וכדומה.

[3] מסמך זה לא מתייחס למצב בו גורם רפואי משתמש בתוכנה ייעודיות המותקנות על מכשיר ייעודי שלא נועד לשימוש אישי וזאת מתוך הנחה שמצב זה הוא האופטימלי מבחינת אבטחת מידע.

העברת צילום של טופס הפנייה או של מכתב סיכום לרופא מטפל מטלפון של גורם רפואי, לטלפון או לכתובת דוא"ל פרטית של מטופל.

4. התופעה האמורה מחדדת את הצורך באיזון בין הזכות לבריאות ולשלמות הגוף של מטופלים מחד גיסא, לבין זכותם לפרטיות ולכך שלא ייאסף ולא ייעשה שימוש במידע רפואי על אודותיהם אלא בהתאם לקבוע בהוראות הדין, מאידך גיסא.

5. מטרת המסמך היא להציב זרקור על התופעה, לסקור את הוראות הדין הרלוונטיות לה, ולהציג מספר הבהרות והמלצות ביחס אליה, כאשר המרכזית בהן היא להביא לצמצום שימוש גורמי רפואה בתוכנות שאינן ייעודיות להעברת מידע רפואי מזוהה, ככל שהדבר אפשרי. התמקדות המסמך בהעברת מידע רפואי נובעת מרגישותו של מידע זה.

6. **יובהר כי המסמך אינו מבקש למנוע את העברת המידע באמצעות מכשירים דיגיטליים פרטיים או בתוכנות לא ייעודיות, אלא לספק המלצות בעניין זה בראי הגנת פרטיות המטופלים, ולחדד את החובות המוטלות בהקשר זה על בעלי השליטה במאגרי מידע רפואי**.

<u>הסיכונים לפרטיות</u>

7. מידע רפואי הוא מידע רגיש. על רגישותו של מידע רפואי ועל הצורך למנוע חשיפה לא תקינה שלו ניתן ללמוד, בין היתר, מפסיקת בית המשפט העליון, אשר קבע כי "פרטים רפואיים מצויים בליבת הפרטיות, ועל כן יש לצמצם במידת האפשר את חשיפתם".[4]

8. ככלל, העברת מידע רפואי על אודות מטופלים בשלושת האופנים שתוארו לעיל נובע מיעילותם וזמינותם של התוכנות והאמצעים הדיגיטליים השונים.

9. עם זאת, מצב זה עשוי להביא לכך שמידע רגיש יישמר במכשירים דיגיטליים (פרטיים או מוסדיים) ובמספר רב של מאגרי מידע. לדוגמה, צילום טופס רפואי במכשיר טלפון חכם של גורם רפואי עשוי להביא לשמירתו של המידע ב"זיכרון" המכשיר וייתכן שגם באמצעי גיבוי שהוגדרו בו (לרבות בשירותי "ענן" של חברות פרטיות). כמו כן, שליחת המידע באופן מקוון באמצעות תוכנות לא ייעודיות עשויה להביא לכך שהמידע ייאסף וישמר במאגרי מידע של החברות המסחריות המספקות את תשתיות העברת המידע.

כל האמור מהווה סיכון לפרטיות מטופלים וזאת במספר היבטים מרכזיים:

א. איסוף ושמירת מידע רפואי על אודות מטופלים במכשירים או במאגרי מידע שאינם מאובטחים דיים, וכן העברתו באופן מקוון שאינו מאובטח דיו, עלולים **להביא לזליגתו ולחשיפתו של המידע**, וזאת בין כתוצאה מפריצה מכוונת לאותם מכשירים או מאגרים, ובין כתוצאה מכשל פנימי בהם.

---

[4] רע"א 8019/06 **ידיעות אחרונות בעמ' נ' לוין**, פסקה ב' לפסק דינו של השופט רובינשטיין (פורסם בנבו, 13.10.2009). ראו לעניין זה גם ע"ע (ארצי) 34784-10-16 **תרכובות ברום בע"מ נ' יהודית בורוכוב**, פסקאות 57-59 לפסק דינה של השופטת ס' דוידוב-מוטולה (פורסם בנבו, 15.10.2018).

ב. חשיפת מידע רפואי עלולה להתרחש גם כתוצאה **מטעויות אנוש**. זמינות השימוש במכשירים דיגיטליים וערבוב השימוש בהם, הן לצרכי עבודה והן לצרכים אישיים, מגבירים את הסיכון שגורמי רפואה יעבירו בטעות מידע רפואי השמור במכשיריהם לגורמים שאינם מורשים ושאינם אמורים להיחשף לו. חשיפה שכזו עלולה להתרחש גם במסגרת החלפת המכשיר בו שמור המידע, או תיקונו.

ג. מידע רפואי הוא מידע אישי רגיש **ולגניבתו** עשויות להיות השלכות קשות, הן ברמת המטופל שמידע על אודותיו נחשף ברבים, והן ברמת אמון הציבור במוסדות הבריאות במדינה. כמו כן, אי-אבטחתו כנדרש של מידע רפואי עלולה להביא גם **לשיבושו**, באופן העלול לשמש בסיס להחלטות רפואיות שגויות, ומכאן לפגוע בבריאותם של מטופלים.[5]

ד. שמירת והעברת מידע רפואי על אודות מטופלים בתוכנות הנמצאות בבעלות חברות תקשורת ומידע מסחריות עלולות להביא גם לכך שחברות אלו **ישתמשו במידע (או בחלקים ממנו) לצרכיהן**. חשש זה הוא קריטי בעיקר ביחס לתוכנות ואפליקציות "חינמיות" להעברת מידע, אשר המודל הכלכלי שלהן מבוסס על מתן שירותים ללא עלות כספית בתמורה לאיסוף ועיבוד המידע הנשמר והמועבר באמצעותן.

ה. בנוסף לכל האמור יש לזכור כי השימוש של גורמי רפואה במכשיריהם הפרטיים או בתוכנות ואפליקציות שאינן ייעודיות להעברת מידע רפואי, **עשוי להיעשות שלא בידיעתם או בהסכמתם של המטופלים**.[6]

<u>איסוף, שמירה והעברת מידע רפואי – סקירת הוראות הדין</u>

<u>חוק הגנת הפרטיות והתקנות שהותקנו מכוחו</u>

10. הוראות חוק הגנת הפרטיות, התשמ"א-1981 (להלן: 'חוק הגנת הפרטיות') והתקנות שהותקנו מכוחו מעניקות התייחסות מיוחדת להגנה על מידע רפואי במסגרת שמירתו במאגרי מידע והעברתו לגורמים שונים.

11. כך, 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**".

12. 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

---

[5] 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').

[6] לדוגמה, במחקר שנערך בבית חולים באירלנד נמצא כי 97% מהרופאים שנחקרו ציינו כי הם העבירו מידע רפואי רגיש על אודות מטופלים באפליקציית WhatsApp, ללא קבלת הסכמת המטופלים לכך.

קריטריון ביחס לאופן יישום היבטים שונים של אבטחת מידע, כגון אופן ההתמודדות עם אירועי אבטחת מידע והאבטחה הפיזית והסביבתית של מאגר המידע.

13. בכל הנוגע לשמירתו של מידע אישי במכשירים דיגיטליים והעברתו ביניהם, יובהר כי הוראות חוק הגנת הפרטיות חלות ככלל על כל פעולה של עיבוד ושימוש במידע אישי, לרבות "קבלתו, איסופו, אחסונו, העתקתו, עיון בו, גילוי, חשיפתו, העברתו, מסירתו, או מתן גישה אליו".[7] העובדה שמידע מסוים הוא מידע רפואי רלוונטית באופן ספציפי גם ביחס להעברתו בין גופים ציבוריים. על-פי תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו-1986 (להלן: 'תקנות העברת מידע בין גופים ציבוריים'), מידע על מצב בריאותו של אדם מוגדר כ"מידע מוגבל". תקנה 11 לתקנות אלו קובעת כי קבצים ותדפיסי מחשב המכילים מידע מוגבל ומופקים עבור גוף ציבורי אחר יופקו בלוויית כתובת בולטת לעין בכל עמוד, בה יירשם "מכיל מידע מוגן לפי חוק הגנת הפרטיות - המוסרו שלא כדין עובר עבירה".

14. עד כאן החובות הרלוונטיות המרכזיות הנובעות מדיני הגנת הפרטיות. ואולם, החובה על הגנת פרטיות מטופלים, לרבות בהקשר של שמירת מידע רפואי על אודותיהם, נובעת גם מהוראות דין אחרות העוסקות בזכויות מטופלים.

<u>חוק זכויות החולה</u>

15. סעיף 10 לחוק 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**.[8]

16. סעיף 17 לחוק זכויות החולה מסדיר את חובת הניהול של רשומה רפואית.[9] סעיף זה קובע כי **על מטפלים (כהגדרתם בחוק) לתעד את מהלך הטיפול הרפואי ברשומה רפואית הכוללת, בין השאר, פרטים מזהים של המטופל, מידע רפואי בדבר הטיפול הרפואי שקיבל, ועברו הרפואי**. רשומה רפואית כוללת סוגים שונים של תיעוד (בכתב, בצילום וכו') שנוצר, בין היתר, עקב טיפול רפואי שניתן למטופל, והיא עשויה להישמר גם באופן ממוחשב.[10]

17. סעיף 20 לחוק זכויות החולה מסדיר את סוגית מסירתו של מידע רפואי. סעיף 20(א)(1) קובע כי מטפל או מוסד רפואי רשאים למסור מידע רפואי על אודות מטופל על יסוד הסכמתו לכך.

---

[7] ראו הגדרת "עיבוד, שימוש" בסעיף 3 לחוק הגנת הפרטיות.

[8] 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".

[9] נושא ניהול רשומות רפואיות מוסדר גם בסעיפים 29, 29א(2), 29א(3), 29ז, 29י(ד), 34א(10), 35(א) ו- 36(א)(7) לפקודת בריאות העם, 1940.

[10] לעניין זה ראו תקנות בריאות העם (שמירת רשומות), התשל"ז-1976, ותקנות זכויות החולה (תשלום מרבי בעד מסירת העתק רשומה רפואית או עיון בה), התשע"ט-2019, שם מוגדרת "רשומה ממוחשבת" כ"רשומה רפואית השמורה בקובץ מחשב, לרבות כל סוג של מדיה מגנטית".

לפי סעיף 20(א)(3), מטפל או מוסד רפואי רשאים למסור מידע רפואי גם ללא הסכמת המטופל, אם המסירה היא למטפל אחר ולצורך טיפול במטופל. ואולם, סעיף זה **אינו עוסק <u>באופן</u> העברת המידע** בין הגורמים המטפלים. סעיף 20(ב) לחוק זכויות החולה קובע כי מסירת מידע רפואי תיעשה **רק במידה הנדרשת לצורך העניין, ותוך הימנעות מרבית מחשיפת זהותו של המטופל**.

18. עד כאן ההוראות הרלוונטיות הקבועות בדין. חובות נוספות בהקשר של שמירת מידע רפואי והעברתו ניתן למצוא גם במסמכים והנחיות שפורסמו מטעם משרד הבריאות, שחלקן יוזכרו להלן:

<u>הנחיות משרד הבריאות</u>

19. בתאריך 5.1.2020 פרסם משרד הבריאות קוד אתי לשמירת הסודיות ופרטיות מידע אישי על אודות מטופלים (להלן: 'קוד אתי').[11] מסמך זה מציין היבטים שונים הנוגעים להגנה על פרטיות, לרבות כאלו העשויים להיות רלוונטיים לסוגיית שימוש גורמי רפואה באמצעים דיגיטליים ובתוכנות לא ייעודיות להעברת מידע רפואי על אודות מטופלים.

20. הקוד מציין כי טרם העברת מידע לגורם אחר יש לבדוק האם הוא מוסמך ומורשה לקבלו, ובאילו תנאים, וכי "יש לשמור על פרטיות וסודיות המידע האישי והרפואי גם כאשר שיתופו מתבקש לצורך רפואי...". הקוד מציין גם **שכאשר יש אישור והרשאה לחשיפת מידע אישי או רפואי על אודות מטופל, "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.

21. הנחיה רלוונטית נוספת היא מסמך "אמות מידה לניהול רשומת מטופל במערכת הבריאות" מיום 15.12.2019 (להלן: 'מסמך אמות מידה לניהול רשומות').[12] מסמך זה מציין כי לכל מטופל תהיה רשומה אחת אחודה הכוללת, בין היתר, "**כל מידע רפואי אודות המטופל בכל אמצעי טכנולוגי או מדיה בו הוא נוצר או נשמר**", וכן "תוצאות בדיקות בתרשים, בפלט ו/או בקובץ דיגיטלי ממכשירי בדיקה וניטור וכדומה". המסמך מתייחס להיבטים של אבטחת מידע וקובע, בין היתר, כי "**רשומת המטופל תישמר במקום שיבטיח את שמירת הסודיות הרפואית והגנת הפרטיות**" וכן שרשומת מטופל תהיה "**במקום קבוע ומאובטח שיועד לכך בהתאם לכללים**".

---

[11] <u>משרד הבריאות "קוד אתי לשמירת הסודיות ופרטיות המידע האישי" (5.1.2020)</u>.

[12] ראו: <u>משרד הבריאות "אמות מידה לניהול רשומת מטופל במערכת הבריאות" (15.12.2019)</u>. המסמך חל על מוסדות רפואיים המוגדרים בו כ"מרפאה, בית חולים או כל מקום אחר בו מטפלים נותנים טיפול רפואי למטופלים, ובכלל זה - אמבולנס, מוקדי רפואה דחופה וכל גורם ארגוני-מוסדי או מטפל עצמאי המספק שירותי בריאות וטיפול רפואי לציבור הרחב או ללקוחות מוגדרים".

22. על-פי מסמך אמות המידה לניהול רשומות, האחריות ליישום הוראות הדין בנוגע לרשומה רפואית חלה על המטפל או מנהל המוסד הרפואי. מנהל המוסד, או מי מטעמו, אחראיים בין היתר על ניהול, שמירה ובקרה של כלל רשומות המטופלים במוסד הרפואי, ועל קביעת נהלים פנימיים בנושא.

<u>שימוש במכשירים דיגיטליים ותוכנות לא ייעודיות להעברת מידע רפואי – הבהרות והמלצות</u>

<u>כללי</u>

23. הרשות להגנת הפרטיות (להלן: 'הרשות') מבקשת להבהיר כי מידע רפואי על אודות מטופלים (או חלק ממידע זה), הנשמר במכשירים דיגיטליים או המועבר באמצעות תוכנות להעברת מידע, מעבר להיותו מידע בעל רגישות מיוחדת על פי חוק הגנת הפרטיות, **עשוי להיחשב גם חלק מ"רשומה רפואית" ממוחשבת**. כפועל יוצא מכך, שמירת והעברת המידע האמור כפופות לא רק לחובות אבטחת המידע החלות על מידע בעל רגישות מיוחדת, **אלא גם להנחיות משרד הבריאות בנושא רשומות רפואיות, שמירתן ואופן אבטחתן**.

<u>אבטחת מידע – חובת ארגונים ומוסדות המספקים שירותי בריאות ורפואה</u>

24. ככלל, ארגונים ומוסדות המספקים שירותי בריאות ורפואה הם בעלי השליטה במאגרים בהם נשמר המידע הרפואי על אודות מטופלים המקבלים טיפול במסגרתם. כפי שפורט, חוק הגנת הפרטיות ותקנותיו מטילים חובות שונות על בעל שליטה במאגר של מידע רפואי.

25. עמדת הרשות היא שמידע הנוגע למטרות הארגון, כגון מידע על אודות מטופלים, המועבר באמצעות מכשירים דיגיטליים (פרטיים או מוסדיים) ותוכנות לא ייעודיות הוא מידע אישי המוגן על פי חוק הגנת הפרטיות ותקנותיו, וחלה חובה להגן עליו ולאבטחו, ללא קשר לשאלה באיזה אופן הוא מועבר.

26. **כלומר, אישור שנותן ארגון או מוסד המספק שירותי בריאות ורפואה להשתמש במכשירים דיגיטליים (פרטיים או מוסדיים) ובתוכנות שאינן ייעודיות לצורך העברת מידע על אודות מטופלים, מטיל על הארגון חובות ספציפיות בנוגע לאבטחת המידע בשימוש במכשירים ובמערכות האמורות, כמפורט בתקנות**.

27. כך, חלה על בעל השליטה במאגר חובה לאבטח את המידע בעת העברתו מהמאגר, לרבות נקיטת אמצעי הגנה בעת שימוש בהתקן נייד (תקנה 12); אבטחת התקשורת בעת העברת המידע ברשת ציבורית (תקנה 14(ב)) וחובת דיווח על קרות אירוע אבטחה חמור (תקנה 11).

28. למען הסר ספק יובהר כי **ארגונים ומוסדות המספקים שירותי בריאות ורפואה, נושאים באחריות לאבטחת כלל המידע האישי על אודות מטופלים**, אשר נאסף ומועבר במסגרת

פעילותם,[13] ועליהם לוודא כי מידע שכזה אינו מועבר בניגוד להוראות הדין ואינו נחשף לגורמים שאינם רלוונטיים.

חובת מינוי ממונה הגנת פרטיות

29. 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 וככאלו 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 מחויבים ככלל במינוי ממונה על הגנת פרטיות.

30. 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.

31. משכך, לעמדת הרשות, הממונה על הגנת הפרטיות הוא הגורם המתאים לתכנון ולבחינת הצעדים הננקטים בארגון לצמצום הפגיעה בפרטיות מטופלים, העלולה להיגרם כתוצאה מהעברת מידע רפואי באמצעים דיגיטליים, כולל אמצעים לא-ייעודיים.

הבהרות והמלצות לגורמי רפואה

32. ככלל, על גורמי רפואה לפעול בנושא בהתאם להנחיות מעסיקיהם. במצב בו מעסיקים מפרסמים הנחיות פנימיות בנושא, על גורמי הרפואה הפועלים במסגרתם לפעול בהתאם להנחיות אלו.

עמדת הרשות היא שהעברת מידע בעל רגישות מיוחדת ממאגרי מידע של ארגון על-ידי עובד הארגון אל מחוצה לו, <u>ללא אישור או הרשאה מטעם הארגון</u>, עשויה בנסיבות מסוימות להיחשב אירוע אבטחה חמור, וזאת בהתאם לקבוע בהוראות הדין.[14] כך לדוגמה, שליחה בטעות של מסמך סיכום טיפול הכולל פרטים אישיים על אודות מטופל לאדם מחוץ לארגון שאינו מורשה לקבל את המסמך, ייחשב אירוע אבטחה חמור. כך גם מקרה בו מטפל אפשר

[13] סעיף 17 (א) לחוק הגנת הפרטיות קובע כי "בעל שליטה במאגר מידע ומחזיק במאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר המידע". חובה זו מפורטת במסגרת תקנות אבטחת מידע.

[14] להרחבה ראו הרשות להגנת הפרטיות "אירועי אבטחה חמורים - מקרים לדוגמא" (9.6.2020). יצוין גם כי סעיף 16 לחוק הגנת הפרטיות קובע מפורשות כי: "לא יגלה אדם מידע שהגיע אליו בתוקף תפקידו כעובד, כמנהל או כמחזיק של מאגר מידע, אלא לצורך ביצוע עבודתו או לביצוע חוק זה או על פי צו בית משפט בקשר להליך משפטי". מדובר באיסור פלילי, שהעונש הקבוע בצדו הוא עד 5 שנות מאסר.

לילדו להשתמש בטלפון הנייד שלו ותוך כדי כך נחשף ילדו למידע אישי ורגיש על אודות מטופלים. אירוע אבטחה חמור יכול להתרחש גם בעת גניבה או אובדן של מכשיר הטלפון של המטפל, אשר החזיק בו מידע רפואי רגיש על אודות מטופלים.

33. במקרים בהם ארגון בריאות/מוסד רפואי מאשר לעובדיו להשתמש במכשירים דיגיטליים (פרטיים או מוסדיים) ובתוכנות לא ייעודיות להעברת מידע על אודות מטופלים, הרשות מבקשת להדגיש, כדלקמן:[15]

א. ככלל, העברת מידע רפואי על אודות מטופל צריכה להיעשות בהתאם להוראות סעיף 20 לחוק זכויות החולה. העברת מידע שלא על-פי הוראות הסעיף עלולה לפגוע בזכויות המטופל, לרבות בפרטיותו.[16]

ב. **הרשות סבורה כי על גורמי רפואה לצמצם, ככל האפשר, את השימוש של עובדיהם בתוכנות שאינן ייעודיות להעברת מידע רפואי מזוהה. בתוך כך, ראוי גם להימנע מלשמור מידע רפואי על אודות מטופלים במכשירים פרטיים.**

גם כאשר אין כל אפשרות אחרת אלא להעביר מידע רפואי באמצעים אלו, יש לעשות כל מאמץ להשמיט סוגי מידע אשר עלולים, באמצעים סבירים, להביא לזיהוי המטופל. בכלל זה יש להשמיט מזהים ישירים כגון: שם, מס' תעודת זהות, תמונת פנים או תמונה אחרת המאפשרת לזהות את נושא המידע, וכיוצא באלה.

ג. בעת שמירת מידע רפואי על אודות מטופלים במכשירים דיגיטליים פרטים ובעת העברתו יש להקפיד ולשמור על פרטיות מטופלים ועל מידע הנוגע אליהם. זליגת וחשיפת מידע אישי על אודות מטופלים בפני גורמים לא מורשים (כגון גורמים שאינם רלוונטיים לטיפול הרפואי) עלולה להוות פגיעה בפרטיות המטופל, הפרה של הוראות חוק הגנת הפרטיות, והפרה של חובת הסודיות הרפואית הקבועה בסעיף 19 לחוק זכויות החולה. זליגת מידע שכזו יכולה גם להוות אירוע אבטחה חמור כהגדרתו בתקנות אבטחת מידע, המחייב את בעלי השליטה במאגרים לדווח לרשות באופן מיידי על קרות האירוע ודרכי הטיפול בו.[17]

ד. בהתאם לעיקרון צמצום מידע עודף, **בעת שימוש במכשירים דיגיטליים (פרטיים או מוסדיים) ובתוכנות לא ייעודיות להעברת מידע, יש לשמור ולהעביר אך ורק את המידע הרפואי המינימלי הנדרש למטרת שמירתו והעברתו.**[18]

---

[15] במקרה של סתירה בין הנקודות וההמלצות המפורטות בחלק זה להנחיות מוסדות רפואיים או ארגוני הבריאות בנושא, מומלץ לפנות לגורמים הרלוונטיים לבקשת הבהרות.

[16] העברת מידע על אודות מטופל שלא על-פי הוראות סעיף 20 (א) (2) עד (7) לחוק זכויות החולה, או מכוח הסכמה בדין אחר, חייבת להיעשות בהסכמת המטופל.

[17] הרשות להגנת הפרטיות "דיווח על אירוע אבטחה חמור" (4.9.2022).

[18] עיקרון צמצום מידע עודף נגזר מעיקרון צמידות המטרה. על-פי עיקרון זה, יש להימנע ככל הניתן מאיסוף ושמירה של מידע על אודות אדם שאינו הכרחי למטרת האיסוף או למטרת המאגר בו הוא שמור. על פי העיקרון יש לאסוף ולשמור אך ורק את המידע המינימלי הנדרש וההכרחי למטרות האמורות, וזאת מבחינת היקף המידע הנשמר, סוג

ה. לאחר השגת המטרה לשמה נשמר המידע במכשיר (לדוגמה, אם מידע נשמר בטלפון חכם לצורך התייעצות מקצועית שהסתיימה) **מומלץ להעביר את המידע, בהקדם האפשרי, לשמירה במערכות הרפואיות הייעודיות שנועדו לכך, והכל בהתאם להנחיות משרד הבריאות והמוסד הרפואי**.

ו. לאחר שמירת המידע במערכות הייעודיות, ולאחר וידוא כי המידע הועבר ונשמר כנדרש, **מומלץ למחוק בהקדם האפשרי את המידע**, הן מזיכרון המכשיר והן מזיכרון התוכנה הלא ייעודיות שבה הוא הועבר.[19] זאת, בין השאר, מפני שגם על מידע זה חלות כל ההוראות הרלוונטיות המוטלות על בעל המאגר מכוח תקנות אבטחת מידע, כמפורט בסעיף 25-27 למסמך זה.

ז. **מומלץ כי מידע רפואי על אודות מטופלים, שנשמר במכשיר דיגיטלי ומועבר באמצעות תוכנות לא ייעודיות, לא יישמר במקביל גם בשירותי גיבוי ענן פרטיים ושאינם ייעודיים**, כגון Google Drive או Dropbox. היה והמידע נשמר במקביל גם בשירותי ענן שאינם ייעודיים – מומלץ למחוק את המידע משירותים אלו בהקדם האפשרי. יצוין כי אף שגיבוי המידע הוא חשוב, גיבוי שכזה צריך להיעשות במסגרת המנגנונים הייעודיים של המוסד הרפואי.[20]

ח. **יש להשתמש באמצעי אבטחה למכשירים ולתוכנות בהם נעשה שימוש להעברת מידע רפואי**, כגון שימוש בסיסמת כניסה חזקה ומורכבת למכשירים, אימות דו-שלבי, זיהוי ביומטרי וכו'. מומלץ להקפיד שלא לעשות שימוש בסיסמה אחת למגוון של אמצעים ולהחליף את הסיסמאות באופן קבוע, לפחות אחת לשישה חודשים. יש להקפיד גם על אופן ומקום שמירת הסיסמאות וזאת על מנת למנוע את חשיפתן בפני גורמים לא מורשים או בפני כאלו העלולים לעשות שימוש לא מותאם במידע.

כך לדוגמה, יש להימנע מלרשום את סיסמת הכניסה למחשב הנייד בקרבת המחשב ובאופן החשוף לכל. מעבר לכך מומלץ שתוגדר נעילה אוטומטית של המכשיר לאחר 30 שניות. מומלץ גם להימנע מלהעניק לגורמים שונים גישה למכשירים הפרטיים בהם נשמר ונעשה שימוש במידע על אודות מטופלים.

המידע, זמן שמירתו וכדומה. יצוין כי מוסדות רפואיים המוגדרים כמוסדות ציבוריים על-פי סע' 23 לחוק הגנת הפרטיות, ואשר מקבלים מידע רפואי על פי תקנות העברת מידע בין גופים ציבוריים, מחויבים במחיקת מידע עודף מיד עם קבלת הנתונים, בהתאם להוראת תקנה 6 לתקנות אלו. להרחבה ראו טיוטת מסמך מדיניות הרשות בנושא צמצום מידע.

[19] עיקרון דומה קבוע בפקודות משטרת ישראל של המפקח הכללי בנושא "שימוש בטלפון סלולארי אישי על ידי שוטרים לצורכי עבודה", שם נקבע בסעיף 3.ג(3) כי "עם סיום העברת החומר המתועד ווידוא כי אכן החומר הועבר כנדרש לאמצעי האחסון המשטרתיים, ימחק השוטר את החומר המתועד ממכשירו, לרבות מחיקה משירותי גיבוי המופעלים במכשירו".

[20] לעניין זה ראו גם: חוזר מנכ"ל משרד הבריאות "שימוש במחשוב ענן במערכת הבריאות" (21.2.21).

ט. יש להשתמש בגרסאות מעודכנות של התוכנות המותקנות במכשירים הדיגיטליים (כגון מערכת ה'חלונות' הפועלת במחשב וכו'). יש לוודא בעניין זה כי המכשירים עובדים בגרסת מערכת ההפעלה האחרונה ומעודכנים בעדכוני האבטחה האחרונים.

י. **יש להימנע ככלל משימוש ברשתות Wi-Fi פתוחות** ולעבוד באמצעות הרשת הסלולרית או באמצעות רשת ווירטואלית פרטית (VPN). במידה ומתחברים מרשת ה-Wi-Fi הביתית יש לוודא כי הרשת פרטית ומוגדרת סיסמת התחברות מוקשחת, אשר לא בוצע בה שימוש בחשבון אחר וסיסמת ברירת המחדל של הנתב הוחלפה בסיסמה מוקשחת.

יא. מכיוון שעשויה להיות שונות בין זהות התוכנות הלא ייעודיות להעברת מידע בכל הנוגע לפרטיות משתמשים, **מומלץ כי בעת בחירת סוג וזהות התוכנה בה תינתן עדיפות לתוכנות הפועלות לחיזוק פרטיות משתמשים ושליטתם במידע.** כך לדוגמה, בבחירה בין סוגי האפליקציות להעברת מסרים מיידים הקיימים בשוק מומלץ כי תיבחר האפליקציה המספקת אמצעים מתקדמים להגנה על פרטיות משתמשים, כגון הצפנה מקצה לקצה, אפשרות למחיקת מידע, וכדומה.

יב. בעת שימוש בתוכנות לא ייעודיות להעברת מידע יש להשתמש באפליקציות שמקורן אך ורק בחנויות אפליקציות רשמיות. כמו כן, מומלץ **לבחון ולנהל את ההרשאות המוגדרות באפליקציות, באופן שיצמצם איסוף מידע לא נדרש.**

יג. **על גורמי רפואה להתנות שימוש עובדיהם בתוכנות לא ייעודיות להעברת מידע רפואי בהתקנת תוכנות להגנה על מידע ולמניעת חדירה למכשירים,** כגון תוכנות חומת אש ואנטי-וירוס (Anti-Virus). למען הסר ספק, יצוין כי בנוסף לתוכנות אנטי-וירוס המיועדות למחשבים ישנן כיום גם תוכנות אנטי-וירוס רבות, לשימוש בחינם או בתשלום, המיועדות לטלפונים ניידים.

יד. אין להשאיר את מכשיר הקצה ללא השגחה. כמו כן, יש לדווח מידית לבעלי השליטה במאגר על כל חשש לחדירה למכשיר, העתקה או דליפה של מידע, או על דבר אחר שאינו שיגרתי העלול להצביע על בעיה של אבטחת המידע.

<u>הבהרות והמלצות להנהלות ארגונים ומוסדות המספקים שירותי בריאות ורפואה</u>

34. הרשות קוראת להנהלות הארגונים והמוסדות המספקים שירותי בריאות ורפואה לפעול להגברת המודעות של גורמי הרפואה הפועלים תחתיהם בדבר הסיכונים לפרטיות הכרוכים בשימוש במכשירים דיגיטליים פרטיים ובתוכנות לא ייעודיות להעברת מידע, וכן להנחות אותם ביחס להתנהלות נכונה בהקשר זה.

35. בהקשר זה סבורה הרשות כי ראוי שארגונים ומוסדות יבחנו את מגוון התוכנות הלא ייעודיות להעברת מידע רפואי, וינחו את צוותי הרפואה הפועלים במסגרתם להשתמש רק בתוכנות

שיימצאו על ידם כראויות מבחינת אבטחת מידע, ומבחינת ההתחייבות החוזית שלהן כלפי משתמשים וזכויותיהם במידע. כך לדוגמה, בעת בחירה בין תוכנות לא ייעודיות להעברת מידע רצוי כי תיבחר תוכנה המספקת כלי הצפנה מקצה לקצה והליך של אימות דו-שלבי, וכן כזו המאפשרת למשתמשים בה שליטה רחבה ככל האפשר במידע הנוגע אליהם.

36. על ארגון המתיר לעובדיו להשתמש בתוכנות לא ייעודיות להעברת מידע רפואי מזוהה, לקבוע מדיניות פנים ארגונית ברורה בדבר שמירת מידע רפואי על אודות מטופלים במכשירים דיגיטליים ובדבר העברת מידע זה במערכות שאינן ייעודיות, אשר תכלול התייחסות לסוגיות השונות שפורטו לעיל, כגון: מחיקת המידע, מדיניות שימוש בסיסמאות כניסה למכשירים, שליטה על הרשאות גישה למידע וכדומה. מומלץ כי מדיניות זו תכלול התייחסות גם למצבי "סוף חיים" של מכשירים מוסדיים בהם נשמר מידע רפואי על אודות מטופלים, אשר תקבע, בין היתר, את הצורך לפרמט מכשירים אלו ולמחוק מידע רפואי השמור בהם, בטרם הם נמכרים, נזרקים או מועברים הלאה לגורמים שונים. עמדת הרשות היא כי שקיפות המדיניות הפנים ארגונית היא בעלת ערך רב, ומומלץ כי מדיניות זו תשוקף לצוותים הרפואיים ולציבור הרחב, ככל שהדבר אפשרי.

37. בנוסף, הרשות ממליצה להנהלות הארגונים והמוסדות לבחון אפשרות של הספקת מכשירים ייעודיים לעובדיהם, ולקדם הטמעה של מערכות "סגורות" ויעילות להעברת מידע רפואי על אודות מטופלים המבטיחות רמת אבטחת מידע נאותה, ובכך לצמצם את היקף השימוש במכשירים דיגיטליים פרטיים ובתוכנות לא ייעודיות להעברת מידע רפואי. לכל הפחות, הרשות ממליצה לארגונים ולמוסדות להשתמש במערכות לניהול התקנים ניידים (Mobile – MDM Device Management). מערכות אלו מאפשרות לארגונים לפקח על פעילות המכשירים הניידים שבשימוש עובדיהם ולנהל אותה, וזאת, בין היתר, לשם יישום מדיניות אבטחת מידע.[21] יצוין כי ישנן מערכות MDM המותאמות לתחום הרפואי.

38. הרשות מבקשת להדגיש כי עריכת תסקיר השפעה על פרטיות בשלב מוקדם של תכנון מערכות המידע היא הדרך היעילה והאפקטיבית למזער את הסיכון לפגיעה בפרטיות המטופלים.[22] עריכת תסקיר שכזה היא חלק מתפיסה רחבה יותר של עיצוב לפרטיות..

<u>סיכום</u>

39. מידע רפואי הוא מידע בעל רגישות מיוחדת המצוי בליבת הפרטיות. מידע זה יש לאבטח כנדרש ולצמצם, ככל האפשר, את חשיפתו.

---

[21] להרחבה ראו פרסום של מערך הסייבר הלאומי בעניין "שיטות עבודה מומלצות למערכת ניהול התקנים ניידים (MDM/EMM)" (14.1.2021).

[22] ראו מדריך עזר לביצוע תסקיר השפעה על הפרטיות שפרסמה הרשות להגנת הפרטיות (נובמבר 2022).

40. שמירת מידע רפואי על אודות מטופלים במכשירים פרטיים או במכשירים מוסדיים המשמשים גם לשימושים אישיים, וכן העברתו של מידע שכזה באמצעות תוכנות לא ייעודיות, עלולות לסכן את פרטיותם של מטופלים. שימוש באמצעים האמורים עלול להביא לזליגה ולחשיפה של מידע רפואי הנוגע למטופלים, באופן שיהווה הפרה של הוראות חוק הגנת הפרטיות וחוק זכויות החולה.

41. במסגרת המסמך סקרה הרשות את הוראות הדין הרלוונטיות והציגה המלצות להתנהלות גורמי רפואה בהקשרים אלו. ככלל, הרשות ממליצה להימנע מלשמור מידע רפואי במכשירים פרטיים, ומלהשתמש בתוכנות לא ייעודיות להעברת מידע רפואי. היה ושימוש שכזה נעשה – יש לפעול בזהירות ותוך הקפדה על שמירה על פרטיות המטופלים ועל המידע הנוגע אליהם, לרבות אימוץ עיקרון צמצום המידע שאינו נדרש.

42. לאור רגישותו של מידע רפואי ופוטנציאל הנזק שעלול להיגרם כתוצאה מחשיפתו, הרשות לא תהסס להפעיל את הסמכויות העומדות לה על-פי דין במקרים של הפרה של הוראות חוק הגנת הפרטיות והתקנות שהותקנו מכוחו, בין השאר כמפורט במסמך זה.