

הגנה על פרטיות מטופלים במתן שירותי רפואה מרחוק עדכון לקוחות - מחלקת הייטק וטכנולוגיה – מרץ 2022

לקוחות יקרים,

ביום 16.2.2022 פרסמה הרשות להגנת הפרטיות ("הרשות") טיוטת מסמך שכותרתו "הגנה על פרטיות מטופלים במתן שירותי רפואה מרחוק" ("המסמך"). מטרת המסמך היא להציב זקוק על תופעת מתן שירותי רפואה מרחוק ועל אתגרי הפרטיות הכרוכים בה, לרכז את הוראות הדין הרלוונטיות לתחום הפרטיות בשירותים מסוג זה, ולתת הבהרות והמלצות לצורך הגנה על פרטיות המטופלים.

שירותי הרפואה מרחוק התפתחו מאד בשנים האחרונות, ולאור זאת מצאה הרשות לנכון לפרסם את המסמך, כדי שבמתכונתו הסופית יחדד את החובות המוטלות על הגורמים הלוקחים חלק במתן שירותי רפואה מרחוק – דוגמת ספקי השירות (ארגוני בריאות, קופות חולים וכו'), ספקים חיצוניים (כגון גורמים המספקים את התשתית הטכנולוגית, הפלטפורמה והמכשירים הרפואיים המקוונים בהם נעשה שימוש במסגרת השירות), ומטפלים (למשל רופאים עצמאיים המעניקים שירות של רפואה מרחוק).

ראינו לנכון לסקור בתמצית את עיקרי המסמך הן משום שהוא כבר במתכונתו הנוכחית (כטייטה להערות הציבור) מצביע על האופן בו הרשות רואה את שירותי הרפואה מרחוק, והן משום שניתן להעביר לרשות התייחסות למסמך עד ליום **31.3.2022**.

אנו נשמח לעמוד לרשותכם לצורך הגשת התייחסות למסמך, וכן על מנת לסייע לארגונכם לעמוד בהוראות דיני הגנת הפרטיות ואבטחת המידע החלים עליו.

להלן נפרט את עיקרי המסמך.

כידוע, מידע רפואי על אדם הוא רגיש ביותר וזליגתו או חשיפתו עלולים לפגוע במטופל קשות. כיום, בניגוד לעבר, תופעת מתן שירותי רפואה מרחוק הפכה נפוצה בקרב כלל גורמי הרפואה. על אף היתרונות הרבים בשירותים אלה, השימוש בהם טומן בחובו אתגרים רבים בתחומי אבטחת המידע והשמירה על פרטיות המטופלים.

במסמך, הרשות מחלקת את שירותי הרפואה הניתנים מרחוק לחמישה סוגים עיקריים:

- א- **הצגת מידע רפואי וביצוע פעולות מרחוק** – שירות זה כולל אפליקציות ואתרי אינטרנט להצגת מידע רפואי על אודות מטופל (כגון מרשמים ותוצאות בדיקות).
- ב- **מפגש וירטואלי בין מטופל למטפל בזמן אמת (סינכרוני)** – שירות המאפשר מפגש מקוון בזמן אמת בין מטופל למטפל הנמצאים במקומות גיאוגרפיים שונים.
- ג- **בדיקה עצמית במכשיר רפואי מקוון לשם התייעצות, אבחון או טיפול במועד מאוחר יותר (א-סינכרוני)** – שירות זה מתייחס לשימוש עצמאי של מטופל במכשירי בדיקה רפואיים מקוונים לניטור מצבו הרפואי, שלא בזמן מפגש מקוון עם מטפל.
- 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 הרפואי, זאת באמצעות מכשירי בדיקה רפואיים ייעודיים מקוונים (לבישים או מושתלים בגוף המטופל).
- ה- **שירותי אבחון ראשוני מבוסס בינה מלאכותית** – שירות זה מתייחס לשימוש מטופלים באלגוריתם "לומד" מסוג בינה מלאכותית, המנתח מידע רפואי, במטרה לזהות דפוסים חוזרים, ועל-פיהם להציע אבחנה רפואית וטיפול אפשרי.

הסיכונים העיקריים לפרטיות המטופל, אותם מפרטת הרשות במסמך, הם:

- א- **זליגת מידע** – סיכון שמקורו בכשלים הטכניים האפשריים במצב של שירות מרחוק (למשל האפשרות שייפגעו התשתיות הרלוונטיות לשירות, רשת האינטרנט, מכשיר המטופל, מכשיר המטפל, המכשיר החכם שבאמצעותו ניתן השירות, שירותי הענן וכו'), בגורם האנושי הלוקח חלק בשירות (למשל מצבים בהם מטופלים שאינם מודעים לסיכוני האבטחה בשירות מרחוק עלולים לצאת באופן לא מאובטח (או לא לצאת בכלל) מהשירות בסיום משך שימוש (session) ספציפי) ועוד.
- ב- **היעדר מודעות מטופלים לאיסוף מידע ולמטרות השימוש בו** – בשירותי רפואה מרחוק המידע אודות המטופלים נשמר לא אחת אצל ספקים חיצוניים. קיים חשש שהמטופלים המשתמשים בשירות אינם מודעים לכך ואינם מכירים את המטרות שלשמן נשמר המידע.
- ג- **חשיפת מידע בפני גורמים לא מורשים בסביבת המטפל** – מאחר וטיפול רפואי מרחוק יכול להינתן על ידי מטפל בזמן שהוא נמצא בביתו או במרחבים ציבוריים, המידע הרפואי שהמטופל חושף בפני המטפל עלול להיחשף בפני גורמים לא מורשים.

מסגרת נורמטיבית

במסגרת המסמך ריכזה הרשות בתמצית את הוראות הדין אשר לדעתה רלוונטיות לשמירה והגנה על מידע רפואי.¹ לפי הרשות, מידע שנאסף במאגרים הרלוונטיים לשירותי רפואה מרחוק כולל על פי רוב (לכל הפחות) נתונים על מצב בריאותו של אדם, וככזה הוא מידע רגיש, כהגדרתו בחוק הגנת הפרטיות, התשמ"א-1981 ("חוק הגנת הפרטיות"). מאגר מידע רגיש חייב ברישום ולפי התוספת הראשונה לתקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 ("התקנות") על מאגר מידע הכולל מידע רפואי תחול רמת אבטחה בינונית ומעלה.

פרט לחוק הגנת הפרטיות והתקנות, מונה הרשות מקורות נורמטיביים נוספים דוגמת חוק זכויות החולה, התשנ"ו-1996 המקים גם הוא (בין היתר) חובת סודיות ביחס לכל מידע הנוגע למטופל שמגיע למטפל תוך כדי מילוי תפקידו או עבודתו, וכן חובות נוספות בכל הנוגע להסכמת המטופל לטיפול (גם במצב בו הוא נעשה מרחוק).

בנוסף, מונה הרשות הנחיות שונות של משרד הבריאות, המקימות (בין היתר) חובות נוספות דוגמת חובות צמצום המידע שנאסף על ידי ספקי השירות ואבטחתו, וכן את כללי האתיקה של ההסתדרות הרפואית בישראל, המקימים (בין היתר) דרישות להימנע משימוש באמצעים שאינם מאובטחים² בעת מתן שירותי רפואה מרחוק וקובעים כי "ראוי כי תינתן למטופל האפשרות לחזור בו מהסכמתו בכל זמן נתון".

הבהרות והמלצות

במסגרת המסמך הרשות מפרטת מספר המלצות והבהרות ביחס לשמירה על פרטיות מטופלים בשירותי רפואה מרחוק. אלה העיקריות שבהן:

א- כללי: ככלל, עמדת הרשות היא שעל כל הגורמים האוספים 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 גורמים אלה מוטלת החובה לפעול לאבטחת המידע הרפואי שנאסף על ידם בהתאם להוראות חוק הגנת הפרטיות והתקנות שהותקנו מכוחו (מבלי לגרוע מחובות אחרות בדין).

ב- יידוע, שקיפות והסכמה מדעת:

1. עמדת הרשות היא שעל מטופלים לתת את הסכמתם לאיסוף מידע אודותם, הן לספק השירות והן לספקים החיצוניים.
2. הרשות מציינת שעל בסיס סעיף 11 לחוק הגנת הפרטיות, על גורם המבקש הסכמה לציין את כל המידע המהותי הרלוונטי. בין היתר יש לפרט איזה מידע ייאסף כתוצאה מקבלת ההסכמה, אילו שימושים ייעשו בו, למי הוא עשוי להיות מועבר ולאילו מטרה. ההסבר צריך להיעשות בשפה ברורה ורצוי שיכלול פירוט בדבר זכויות המטופל במידע, לרבות הזכות לעיין במידע.
3. במקרים בהם הספק החיצוני מבקש לעשות שימוש במידע אודות המטופל למטרות שונות ממטרת הטיפול, על ספק השירות (כגון קופת החולים) להבהיר את הדברים למטופל, ולקבל ממנו הסכמה נפרדת לשם כך. מעבר לכך, על ספק השירות להבטיח כי למטופלים תעמוד האפשרות לקבל את השירותים הרפואיים מבלי שהם יהיו מחויבים, דה-פקטו, להסכים גם לשימוש במידע על אודותיהם למטרות אחרות ממטרת הטיפול. בהקשר זה הרשות נותנת התייחסות מיוחדת לאבחון מבוסס אלגוריתם מסוג בינה מלאכותית, ומביעה את עמדתה לפיה אם במסגרת השירות נאסף מידע אישי מזוהה (או הניתן לזיהוי) 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.

ג- צמצום מידע: הרשות מבהירה כי על כלל הגורמים להימנע ככל הניתן מאיסוף ושמירה של מידע על מטופלים שאינו הכרחי למטרת השירות הרפואי מרחוק, או למטרת המאגר בו מידע זה נשמר. הרשות אף מזכירה שבעל מאגר מידע, ככלל, מחויב לבדוק אחת לשנה האם במאגר המידע שבבעלותו נשמר מידע עודף, שאינו נדרש לשם עמידה במטרת המאגר. בשים לב לכך שסוג המידע שנאסף בשירותי רפואה מרחוק הינו רפואי ורגיש, הרשות מביעה את עמדתה לפיה ראוי שהבחינה תיעשה במסגרת פרקי זמן קצרים יותר מהקבוע בתקנות – מספר פעמים בשנה.³

3. ראו גם מזכרנו בדבר טיטת מסמך הרשות בנושא [צמצום מידע עודף](#).

ד- אחריות ספק שירות המתקשר עם ספק חיצוני למתן שירותי רפואה מרחוק: הרשות מביעה את עמדתה כי על ספק השירות האמור מוטלות חובות שונות, ועליו לבחון סיכוני אבטחת מידע הכרוכים בהתקשרות טרם ביצוע ההתקשרות ולפקח על התנהלות הספק החיצוני בהיבטי פרטיות ואבטחת מידע (מכוח תקנה 15 לתקנות והנחיית רשם מאגרי המידע בעניין מיקור חוץ).

ה- אימות זיהוי: הרשות מבהירה כי על בעלי מאגרי המידע 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 (תקנה 9(ב) לתקנות). רשימת הרשאות צריכה לכלול את כל המשתמשים במערכת, ויש להקפיד על אמצעי זיהוי מתאימים לכל משתמש לפי שנגיש לו. בהקשר זה הרשות מציגה במסמך עמדה לפיה מכיוון שמכשירים רפואיים מקוונים מאפשרים גם הם חיבור מרחוק למאגרי המידע, גם מכשירים אלו נחשבים 'מערכות מאגר' – על כל המשתמע מכך מבחינת אימות זיהוי מטופלים המשתמשים במכשירים אלו, וחובות האבטחה המוטלות על מערכות מאגר לפי התקנות.

ו- סיום שימוש במכשירים רפואיים מקוונים וגריעתם: מומלץ כי ספקי השירות והספקים החיצוניים יקבעו נהלים לאבטחת המידע האמור במועד הפסקת השימוש במכשירים האמורים וגריעתם, לרבות נהלים להשמדת המידע השמור בהם.

ז- היבטי פרטיות במפגש וירטואלי: מובהר כי על המטפלים להקפיד על כללי אבטחת המידע בתוכנות ובמכשירים הטכנולוגים בהם הם משתמשים במסגרת המפגש הווירטואלי. הרשות מונה במסגרת המסמך מספר הנחיות שלעמדתה על המטפלים לפעול לפיהן.

לקריאת המסמך המלא לחצו [כאן](#).

*המידע האמור לעיל הינו מידע כללי ותמציתי בלבד, הוא אינו מהווה חוות דעת או ייעוץ משפטי ויש לקבל עצה מקצועית נפרדת בטרם נקיטת פעולה משפטית או אחרת בקשר עם הנושאים אותם סקרנו.

צוות מחלקת הייטק וטכנולוגיה ישמח לעמוד לרשותכם:

עו"ד אסנת סרוסי פירסטטר
ראש מחלקת הייטק וטכנולוגיה
osnat@agmon-law.co.il
03-6078607



עו"ד סער רוסמן
שותף, מחלקת הייטק וטכנולוגיה
saar@agmon-law.co.il
03-6078607

