

## הגנה על פרטיות מטופלים בהעברת מידע רפואי באמצעות מכשירים דיגיטליים ותוכנות לא ייעודיות עדכון לקוחות - מחלקת הייטק וטכנולוגיה – נובמבר 2022

### לקוחות יקרים,

ביום 6.11.2022 פרסמה הרשות להגנת הפרטיות ("הרשות") טיוטת מסמך שכותרתו "הגנה על פרטיות מטופלים בהעברת מידע רפואי באמצעות מכשירים דיגיטליים ותוכנות לא ייעודיות" ("המסמך"). מטרת המסמך היא להציג את עמדת הרשות בנוגע להעברת מידע רפואי באמצעות מכשירים דיגיטליים ותוכנות לא ייעודיות, להמליץ על אופן השימוש בהם וכן לחדד את הוראות הפרטיות החלות מכוח הדין בקשר עם העברת מידע כאמור.

ראינו לנכון לסקור בתמצית את עיקרי המסמך הן משום שהוא כבר במתכונתו הנוכחית (כטיוטה להערות הציבור) מצביע על האופן בו הרשות רואה סוגיה המשפיע על שגרת החיים של ארגוני הבריאות וצוותי הרפואה בארץ, והן משום שניתן להעביר לרשות התייחסות למסמך עד ליום 6.12.2022 בשעה 12:00.

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.

### רקע

במסגרת המסמך, הרשות מתארת תופעה לפיה בשנים האחרונות, מתרחבת תופעת העברת מידע רפואי על ידי ארגוני בריאות, מטפלים וגורמי רפואה, בשלושה אופנים – (א) באמצעות תוכנות ייעודיות להעברת מידע רפואי המותקנות במכשירים דיגיטליים אישיים של גורמי רפואה ("מכשירים פרטיים"); (ב) באמצעות תוכנות לא ייעודיות ("תוכנות גנריות") במכשירים של ארגון הבריאות ("מכשירים מוסדיים"); (ג) באמצעות תוכנות גנריות המותקנות במכשירים פרטיים.

הרשות מציינת במסמך כי כוונתה היא שהמסמך יחול על כלל הגורמים המעניקים "טיפול רפואי", לרבות "מטפל", עובדים מנהליים המועסקים במסגרת "מוסד רפואי", כהגדרתם בחוק זכויות החולה, התשנ"ו-1996 ("חוק זכויות החולה") וכן 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.

נכנה את הארגונים והמוסדות הרפואיים לשם הנוחות "ארגוני בריאות" ואת כל המטפלים וגורמי הרפואה כ-"גורמי רפואה".

### המסגרת הנורמטיבית

המסגרת הנורמטיבית, כפי שמתוארת במסמך הינה חוק הגנת הפרטיות, התשמ"א-1981 ("חוק הגנת הפרטיות"), ולפיו לדעת הרשות במקרים רבים ארגוני הבריאות הינם בעלים של מאגרי מידע המכילים מידע על מצבו הבריאותי של אדם (המהווה "מידע רגיש" לפי חוק הגנת הפרטיות), הכפופים לרמת אבטחה בינונית או גבוהה, לפי תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 ("תקנות אבטחת מידע").

בנוסף, חוק זכויות החולה (א) מקים למטפלים ולעובדי מוסד רפואי לשמור בסוד כל מידע הנוגע למטופל שהגיע אליהם תוך כדי מילוי תפקידם או במהלך עבודתם, (ב) מהווה מקור נורמטיבי ראשי להסדרת ניהולה של הרשומה רפואית של מטופלים<sup>1</sup>, ו-(ג) מסדיר את המצבים בהם ניתן להעביר מידע רפואי.

פרט לכך משרד הבריאות פרסם אף הוא מספר הנחיות הרלבנטיים להעברת מידע רפואי במכשירים מוסדיים או במכשירים פרטיים, ובתוכנות ייעודיות או בתוכנות גנריות. כך למשל פרסם המשרד "קוד אתי לשמירת הסודיות ופרטיות מידע אישי על אודות מטופלים", לפיו גם כאשר ניתן לחשוף מידע אישי או רפואי 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". כן פרסם משרד הבריאות "אמות מידה לניהול רשומת מטופל במערכת הבריאות" לפיהן "רשומת המטופל תישמר במקום שיבטיח את שמירת הסודיות הרפואית והגנת הפרטיות" וכן שרשומת מטופל תהיה "במקום קבוע ומאובטח שיועד לכך בהתאם לכללים".

בהקשר זה יצוין כי רשימת המסמכים שמציינת הרשות במסמך, חסרה לדעתנו נהלים מסוימים החלים על ארגוני בריאות (במיוחד מוסדות רפואיים) הקובעים את האופן בו יש לגשת ולעבד (לרבות בתקשורת ובענן) מידע בריאות, וכן מסמכים של הסתדרות הרופאים בישראל ("הר"י"), דוגמת המסמך העוסק ב Telemedicine רפואת רחוק (מהדורה 2020) ("עמדת הר"י")<sup>2</sup>.

1. יחד עם מקורות נורמטיביים נוספים דוגמת תקנות בריאות העם (שמירת רשומות) התשל"ז-1976, תקנות 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".
2. אנו ממליצים ללקוחותינו להביא בחשבון טרם חיבור נהלים או ביצוע פעולות כמתבקש לפי המסמך.

יחד עם זאת, מהאמור לעיל ניתן לומר שככלל, לפי המסמך ארגוני בריאות הינם בעלי המאגרים הדורשים רמת אבטחה בינונית או גבוהה, והאחראים לשמירת המידע בהם, ארכובו (גם כחלק מהרשומה הרפואית של המטופל) ואבטחתו (לרבות כנגד שיבוש<sup>3</sup>), גם בעת אחסון (at rest) וגם בעת העברתו באמצעי תקשורת (in transit).

## סיכונים עיקריים

במסמך מונה הרשות את הסיכונים העיקריים שהיא מייחסת להעברת מידע רפואי באמצעות תוכנות גנריות או ייעודיות, במכשירים פרטיים ו/או מכשירים מוסדיים שאינם מאובטחים די הצורך. בין היתר מונה הרשות את החשש שמכשירים שרמת ההגנה עליהם נמוכה (במיוחד מכשירים פרטיים) יעמידו מידע רפואי בפני סיכון דלף ו/או שיבוש. סיכונים נוספים שמונה הרשות הם העברת מידע בריאות בענן ציבורי שאינו מאובטח דיו (במיוחד בתוכנות גנריות), טעויות אנוש (במיוחד במקרה של מכשירים פרטיים שנגישים גם על ידי מי שאינם נמנים על צוות ארגוני הבריאות) ושימוש במידע ללא ידיעת המטופל או גורמי הרפואה על ידי חברות המספקות את המכשירים והתוכנות באמצעותם ההתקשרות.

## המלצות ומסקנות הרשות

1. ככלל, העברת מידע רפואי על אודות מטופל צריכה להיעשות בהתאם להוראות חוק זכויות החולה (ובמיוחד סעיפים 19 ו-20), חוק הגנת הפרטיות (במיוחד סעיפים 16 ו-17), ותקנות אבטחת מידע (במיוחד סעיף 15), הנחיות הרשות והנחיות גופים סקטוריאליים (דוגמת משרד הבריאות).
2. עמדת הרשות היא שאישור שנותן ארגון בריאות להשתמש במכשירים פרטיים או מוסדיים ובתוכנות גנריות לצורך העברת מידע על אודות מטופלים, מטיל על הארגון חובות ספציפיות בנוגע לאבטחת המידע בשימוש במכשירים ובמערכות האמורות.
3. בהקשר זה חשוב להזכיר שסעיף 17 לחוק הגנת הפרטיות קובע כי "בעל מאגר מידע, מחזיק במאגר מידע או מנהל מאגר מידע, כל אחד מהם אחראי לאבטחת המידע שבמאגר המידע", וכי בעל מאגר צריך לפעול כאמור בתקנות אבטחת המידע, לרבות על ידי 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).
4. ביחס לאירועי אבטחה, ראוי לדעתנו לציין כי עמדת הרשות היא שהעברת מידע רגיש ממאגרי מידע של ארגון על-ידי עובד הארגון אל מחוצה לו, ללא אישור או הרשאה מטעם הארגון, עשויה בנסיבות מסוימות להיחשב אירוע אבטחה חמור.

3. ראו סעיף 3.1 לחוזר 3/15 "הגנה על מידע במערכות ממוחשבות במערכת הבריאות".

5. 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 ומוסדיים) ובתוכנות גנריות להעברת מידע, וכן להנחות אותם ביחס להתנהלות נכונה בהקשר זה. בהקשר זה, המלצת הרשות מתמקדת בעיקר בפרסום מדיניות פנים ארגונית שתכלול התייחסות, בין היתר, לנושאים הבאים: הסכמת המטופל להעברת המידע, מחיקת המידע, מדיניות שימוש בסיסמאות כניסה למכשירים, שליטה על הרשאות גישה למידע וכדומה. הרשות ממליצה שמדיניות 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.
6. הרשות ממליצה להנהלות הארגונים לבחון אפשרות של אספקת מכשירים ייעודיים לעובדיהם, ולקדם הטמעה של מערכות "סגורות" (ייעודיות), וממליצה לארגונים ולמוסדות להשתמש במערכות לניהול התקנים ניידים (MDM – Mobile Management Device).
7. 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<sup>4</sup>. הרשות מבקשת להדגיש בהקשר זה גם את התועלת הרבה שבמינוי ממונה הגנת פרטיות בארגון, שבין יתר תפקידיו, הוא גם הגורם המתאים והיעיל לתכנון ולבחינת הצעדים הננקטים בארגון למזער הסיכון לפגיעה בפרטיות המטופלים<sup>5</sup>.
8. 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 –
- א. הרשות ממליצה לגורמי רפואה לצמצם, ככל האפשר, את שימושם בתוכנות גנריות להעברת מידע רפואי. הרשות ממליצה גם להימנע מלשמור מידע רפואי על אודות מטופלים במכשירים פרטיים. בהקשר זה אנו מוצאים לנכון לציין את מסמך הר"י לפיו יישומים (אפליקציות) ורשתות חברתיות כגון Facebook או WhatsApp אינם כלי מאובטח למתן טיפול או ייעוץ רפואי פרטני.

4. למזכרנו בדבר עריכת תסקיר השפעה על פרטיות לחצו [כאן](#).

5. למזכרנו בדבר ממונה הגנת פרטיות בארגונים לחצו [כאן](#).

ii. מומלץ שבעת שימוש במכשירים דיגיטליים (פרטיים או מוסדיים) ובתוכנות לא ייעודיות להעברת מידע, יישמר ויועבר אך ורק המידע הרפואי המינימלי הנדרש למטרת שמירתו והעברתו. גם כאשר אין אפשרות אחרת אלא להעביר מידע רפואי באמצעים אלו, עמדת הרשות היא כי יש לעשות כל מאמץ שלא יועבר מידע אישי מזוהה. בכלל זה יש להשמיט מזהים ישירים כגון: שם, מס' תעודת זהות, תמונת פנים או תמונה אחרת המאפשרת לזהות את נושא המידע, וכיוצא באלה.

iii. בנוסף, מומלץ להעביר את המידע, בהקדם האפשרי, לשמירה במערכות הרפואיות הייעודיות שנועדו לכך, והכל בהתאם להנחיות משרד הבריאות והמוסד הרפואי וכי המידע יימחק, הן מזיכרון המכשיר והן מזיכרון התוכנה הגנרית שבה הוא הועבר, אלא אם ניתן להצביע על סיבה מיוחדת לשמירת עותק מהמידע גם במכשיר.

iv. מומלץ כי מידע רפואי על אודות מטופלים, שנשמר במכשיר דיגיטלי ומועבר באמצעות תוכנות גנריות, לא יישמר במקביל גם בשירותי גיבוי ענן פרטיים ושאינם ייעודיים, כגון Google Drive או Dropbox.

v. יש להשתמש באמצעי ניטור והגנה (לרבות אימות דו-שלבי) במכשירים ולתוכנות בהם נעשה שימוש להעברת מידע רפואי ולהשתמש בגרסאות מעודכנות של התוכנות המותקנות במכשירים הדיגיטליים. יש לבחור את סוג התוכנה בה נעשה שימוש באופן שתינתן עדיפות לתוכנות הפועלות לחיזוק פרטיות משתמשים ושליטתם במידע (למשל תוכנות המאפשרות הצפנה מקצה לקצה). יש לבחון ולנהל את ההרשאות המוגדרות באפליקציות שנבחרות, באופן שיצמצם איסוף מידע לא נדרש, ולהימנע ככלל משימוש ברשתות Wi-Fi פתוחות.

נשמח לסייע לארגונכם להגיש התייחסות למסמך ולוודא עמידה בהוראות הגנת הפרטיות ואבטחת המידע החלות עליו.

לקריאת המסמך המלא יש לחוץ [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.

עו"ד אסנת סרוסי פירסטטר  
ראש מחלקת הייטק וטכנולוגיה  
[osnat@agmon-law.co.il](mailto:osnat@agmon-law.co.il)  
03-6078607



עו"ד סער רוסמן  
שותף, מחלקת הייטק וטכנולוגיה  
[saar@agmon-law.co.il](mailto:saar@agmon-law.co.il)  
03-6078607

