

## הגנה על פרטיות מטופלים בהעברת מידע רפואי באמצעות מכשירים דיגיטליים עדכון לקוחות – מרץ 2024

### לקוחות יקרים,

ביום 5.3.2024 פרסמה הרשות להגנת הפרטיות ("הרשות") מסמך שכותרתו "הגנה על פרטיות מטופלים בהעברת מידע רפואי באמצעות מכשירים דיגיטליים" ("המסמך"). מטרת המסמך היא להציג את עמדת הרשות בנוגע להעברת מידע רפואי באמצעות מכשירים דיגיטליים ותוכנות מסוימות, להמליץ על אופן השימוש בהם ולחדד את הוראות דיני הגנת הפרטיות החלים בקשר עם העברת מידע כאמור. מצאנו לנכון לסקור את עיקרי המלצות ומסקנות הרשות.

אנו נשמח לעמוד לרשותכם ולסייע לארגונכם לעמוד בהוראות דיני הגנת הפרטיות ואבטחת המידע החלים עליו.

להלן נפרט את עיקרי המסמך.

### רקע

הרשות מתארת במסמך גידול בהעברת מידע רפואי על ידי ארגוני בריאות, מטפלים וגורמי רפואה, בניהם ובינם לבין מטופלים, 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 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 הגורמים שמעניקים טיפול רפואי לרבות מטפלים וארגוני הבריאות כ-"גורמי רפואה".

את המסגרת הנורמטיבית למסמך ניתן למצוא במזכר הלקוחות שערכנו עם צאת הטיוטה להתייחסות הציבור הזמינה [באן](#), לא נחזור עליהן במזכר זה.

### המלצות ומסקנות הרשות

1. ככלל, עמדת הרשות היא שהעברת מידע רפואי על אודות מטופל צריכה להיעשות בהתאם להוראות חוק זכויות החולה (ובמיוחד סעיפים 19 ו-20), חוק הגנת הפרטיות, תשמ"א-1981 ("חוק הגנת הפרטיות") (במיוחד סעיפים 16 ו-17), תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 ("תקנות 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 שאינן ייעודיות 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 (במיוחד במכשירים פרטיים או תוכנות שאינן ייעודיות), עשויה בנסיבות מסוימות להיחשב אירוע אבטחה חמור.
5. לפי המסמך הרשות סבורה כי הנהלות הארגונים והמוסדות המספקים שירותי בריאות ורפואה לפעול להגברת המודעות של גורמי הרפואה הפועלים תחתיהם בדבר הסיכונים לפרטיות הכרוכים בשימוש במכשירים דיגיטליים (פרטיים ומוסדיים) ובתוכנות לא ייעודיות להעברת מידע, וכן להנחות אותם ביחס להתנהלות נכונה בהקשר זה.
6. בנוסף בהקשר זה, סבורה הרשות כי על ארגון המתיר לעובדיו להשתמש בתוכנות לא ייעודיות להעברת מידע מזהה, לקבוע מדיניות פנים ארגונית שתכלול התייחסות, בין היתר, לנושאים הבאים: 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.

7. ביחס לתוכנות גנריות חשוב לפי עמדת הרשות שארגונים ומוסדות יבחנו את מגוון התוכנות הגנריות הקיימות, וינחו את צוותי הרפואה להשתמש רק בתוכנות שיימצאו על ידם כראויות מבחינת אבטחת מידע, ומבחינת ההתחייבות החוזית שלהן. רצוי לעשות שימוש בתוכנות המאפשרות את הצפנת המידע מקצה לקצה, אימות דו שלבי ושליטה רחבה במידע המועבר.
8. הרשות ממליצה להנהלות הארגונים לבחון אפשרות של אספקת מכשירים ייעודיים לעובדיהם, ולקדם הטמעה של מערכות "סגורות" (ייעודיות), וממליצה לארגונים ולמוסדות להשתמש במערכות לניהול התקנים ניידיים (MDM – Mobile Device Management).
9. 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>1</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>2</sup>
10. 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 –

- 10.1. הרשות סבורה כי על גורמי רפואה לצמצם, ככל האפשר, את השימוש של עובדיהם בתוכנות שאינן ייעודיות 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 (ההסתדרות הרפואית בישראל) לפיו יישומים (אפליקציות) ורשתות חברתיות כגון Facebook או WhatsApp אינם כלי מאובטח למתן טיפול או יעוץ רפואי פרטי.
- 10.2. 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 להשמיט סוגי מידע אשר עלולים, באמצעים סבירים,

<sup>1</sup> למזכרנו בדבר עריכת תסקיר השפעה על פרטיות לחצו [כאן](#).

<sup>2</sup> למזכרנו בדבר ממונה הגנת פרטיות בארגונים לחצו [כאן](#).

- 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.
- 10.3. בנוסף, מומלץ להעביר את המידע, בהקדם האפשרי, לשמירה במערכות הרפואיות הייעודיות שנועדו לכך, והכל בהתאם להנחיות משרד הבריאות והמוסד הרפואי. כן יש בהקדם האפשרי המידע למחוק את המידע הרפואי, הן ממכשירים פרטיים והן משרתי התוכנה הלא ייעודיות שבה הוא הועבר.
- 10.4. 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.
- 10.5. 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. כמו כן, יש לבחור את סוג התוכנה בה נעשה השימוש כך שתינתן עדיפות לתוכנות הפועלות לחיזוק פרטיות משתמשים ושליטתם במידע (למשל תוכנות המאפשרות הצפנה מקצה לקצה) וככל שמדובר באפליקציות יש לעשות שימוש רק באפליקציות שמקורן בחנויות רשמיות.
- 10.6. יש לבחון ולנהל את ההרשאות המוגדרות באפליקציות שנבחרות, באופן שיצמצם איסוף מידע שלא דרוש למטרה לשמה נאסף, ולהימנע ככלל משימוש ברשתות Wi-Fi פתוחות.
- 10.7. על גורמי רפואה להתנות שימוש בתוכנות גנריות להעברת מידע רפואי בהתקנת תוכנות להגנה על מידע ולמניעת חדירה למכשירים בהם מותקנות התוכנות.
- 10.8. אין להשאיר את מכשיר הקצה ללא השגחה.
- נשמח לסייע לארגונכם לעמוד בהוראות והמלצות המסמך 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.

נשמח לעמוד לרשותכם בכל שאלה או התייעצות:



עו"ד דפנה אחיעם טל, שותפה  
מחלקת הייטק טכנולוגיה והון סיכון  
dafnaa@agmon-law.co.il



עו"ד סער רוסמן, שותף  
מחלקת הייטק טכנולוגיה והון סיכון,  
ראש תחום סייבר ופרטיות  
saar@agmon-law.co.il



עו"ד הלל וייס  
מחלקת הייטק, טכנולוגיה והון סיכון  
hillel@agmon-law.co.il



עו"ד מרים שדה פישר  
מחלקת הייטק טכנולוגיה והון סיכון  
צוות סייבר ופרטיות  
miriamf@agmon-law.co.il