דו"ח פיקוח רוחב

ממצאי הליך פיקוח הרוחב
בקרב מגזר רפואה דיגיטלית



ניסן תשפ"ג
אפריל 2024

תוכן עניינים

1. תקציר מנהלים 3

1.1 מגזר רפואה דיגיטלית 3

1.2 תהליך עבודה 4

1.3 ליקויים, מסקנות והמלצות עיקריות 5

2. מגזר רפואה דיגיטלית- תמונת מצב 8

2.1 כללי 8

2.2 רקע על המגזר 8

2.3 תהליך עבודה 9

3. ממצאים – ליקויים מרכזיים לפי קריטריונים ומבט השוואתי 11

3.1 ניהול מאגרי מידע ומיקור חוץ 13

3.2 אבטחת מידע 14

3.3 בקרה ארגונית 14

4. מסקנות/תמונת מצב והמלצות 17

5. שיפור ותיקון ליקויים בעקבות הליך הפיקוח בעת ביקורת המעקב 16

6. סיכום 18

נספח א' – ליקויים מרכזיים שנמצאו במגזר והתיקון הנדרש בגינם 19

1. תקציר מנהלים

מערך פיקוח הרוחב ברשות להגנת הפרטיות, מופקד על עריכת פיקוחי רוחב מגזריים או נושאיים לבחינת יישום הוראות חוק הגנת הפרטיות, התשמ"א-1981 (להלן: "חוק הגנת הפרטיות" או "החוק") ותקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017 (להלן: "תקנות אבטחת מידע" או "התקנות"), במטרה לאתר הפרות של החוק והתקנות, לשם הגברת מודעות המשק להוראות החוק, הגברת האכיפה היזומה של הרשות, לאתר כשלים ענפיים וכלל- משקיים הדורשים התייחסות מוגברת של הרגולטור, וקבלת תמונת מצב כלל-מגזרית לגבי עמידה בהוראות החוק והתקנות.

1.1. מגזר רפואה דיגיטלית

במסגרת סקר רוחבי שערכה הרשות להגנת הפרטיות שבוחן את סיכוני הפרטיות במשק, מגזר רפואה דיגיטלית בישראל אותר כאחד מיעדי פיקוח הרוחב המשמעותיים, הן בשל היותו תחום חדשני אשר היקף השימוש בו גדל באופן משמעותי בתקופת הקורונה לנוכח הביקוש לקבלת שירותי רפואה מרחוק, אשר יחסכו הגעה פיזית למרפאות קופות החולים, והן בשל העובדה כי הגופים במגזר זה אוספים ומעבדים כמות רבה במיוחד של מידע רגיש, ובכלל זה מידע רפואי.

<u>מגזר זה בעל מאפיינים ייחודיים בהיבטי הפרטיות, הבאים לידי ביטוי במספר היבטים</u>:

- מאגרי מידע ארוכי שנים - בשל חשיבות המידע שאוספים הגופים במגזר זה והרלוונטיות הממושכת שלו, מאגרי מידע רפואי נשמרים למשך זמן רב. המערכת הרפואית בישראל מתאפיינת במאגרי מידע בני 15 שנים הכוללים היסטוריה רפואית דיגיטלית מבתי החולים ומהרפואה הקהילתית.
- רגישות המידע - הגופים במגזר זה אוספים ומעבדים מידע רגיש ביותר ובמיוחד מידע רפואי הטומן בחובו תועלות מהותיות לאדם. פגיעה אפשרית במאגרי המידע של הגופים במגזר, עלולה להיות משמעותית במיוחד לאור רגישות המידע השמור, ולכן יש לאבטח ולהגן על המידע.
- סוגי מידע - במסגרת מתן שירותי רפואה דיגיטלית, נאסף ונשמר מידע רפואי ייחודי ורגיש שלא קיים כמעט במערכות אחרות, הכולל נתונים פיזיולוגיים, ביומטריים ונפשיים, ואף הדמיות של גוף האדם, תפקודו ואישיותו.

מתן שירותי רפואה מרחוק כרוך באיסוף, תיעוד, שמירה ועיבוד של מידע רפואי על אודות מטופלים - קטינים ובגירים. ככלל, מידע זה נאסף ונשמר הן על-ידי הגורם המספק את השירות כגון קופות חולים, 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. ניהול מאגרי מידע רגישים אלו, בהתאם למאפייניו הייחודיים של המגזר, הביא לבחירת היעדים במגזר זה ולביצוע פיקוח הרוחב עליהם בכדי לבחון את יישום חוק הגנת הפרטיות ותקנותיו, ולסייע לגופים הפועלים במגזר בה במימוש אחריותם לשמירה על פרטיות המשתמשים. שירותי רפואה מרחוק, האוספים, שומרים ומשתמשים במידע באופן שאינו מאובטח כראוי, יוצרים סיכוני אבטחה העלולים להוביל לזליגתו ולחשיפתו של מידע רפואי רגיש.

1.2. תהליך העבודה

כחלק מהליך פיקוח הרוחב במגזר זה, פנתה הרשות ל- 11 גופים המספקים שירותי רפואה מרחוק בדרישה למילוי שאלוני ביקורת. יצוין כי בהליך בחירת הגופים נלקחו בחשבון היקפי המידע ורגישות המידע הנאסף. בחלק מן המקרים נדרשו הגופים בהמשך לספק מידע, מסמכים והבהרות נוספות לרשות. שאלוני הביקורת בחנו שלושה קריטריונים עיקריים בתחום הגנת הפרטיות: בקרה ארגונית וממשל תאגידי ,ניהול מאגרי מידע ואבטחת מידע.

הציונים ניתנו לגופים בהתאם למענה ולמסמכים שסופקו על ידם, המעידים על רמת עמידתם בהוראות חוק הגנת הפרטיות ובתקנות מכוחו. לאחר קבלת השאלונים המלאים מהגופים המפוקחים, בחנה הרשות את המענה והמסמכים הנלווים. בסיום ההליך, נמצאו ליקויים הדורשים תיקון במרבית הגופים שנבדקו, ובהתאם, דרשה הרשות מאותם גופים לתקן את הליקויים שנמצאו, ולספק תכנית מפורטת לתיקונם, בליווי הצהרת נושא משרה לביצוע והשלמת התיקונים. כחלק מההליך, בדקה הרשות באמצעות ביקורת חוזרת את אופן תיקון הליקויים בחלק מן הגופים. ממצאי הביקורת החוזרת העלו כי הגופים שיפרו את עמידתם בהוראות החוק והתקנות באופן משמעותי.

ליקויים, מסקנות והמלצות עיקריות

במגזר הרפואה הדיגיטלית מרבית הגופים הציגו רמת עמידה גבוהה בשקלול כל התחומים שנבדקו, ורק כ-30% מהגופים מצויים ברמת עמידה חלקית-בינונית.

בשקלול הציונים שניתנו לגבי מידת ההיענות להוראות החוק והתקנות, נמצא כי הציון הממוצע של המגזר עומד על 64%.

ביתר פירוט, ממצאי הליך פיקוח הרוחב מלמדים על חוסר בקיאות מספקת בדרישות תקנות אבטחת מידע. יצוין, כי ממצאי פיקוח הרוחב העלו כי רמת העמידה בדרישות בקרה ארגונית וממשל תאגידי גבוהה באופן מובהק, שכן כ-100% מן הגופים עומדים בדרישות החוק במלואן.

בתחום ניהול מאגרי מידע, מחצית מן הגופים עומדים בדרישות החוק ברמת עמידה חלקית, ומחצית נמצאים ברמת עמידה גבוהה.

בהתאם לממצאים שעלו מהליך פיקוח הרוחב, 8 מתוך הגופים שנבדקו קיבלו הנחיות ספציפיות לתיקון הליקויים שנמצאו אצלם.

הרשות להגנת הפרטיות
THE PRIVACY PROTECTION AUTHORITY
سلطة حماية الخصوصية

משרד המשפטים
MINISTRY OF JUSTICE | وزارة العدل

ממצאי הליך פיקוח רוחב
בקרב מגזר רפואה דיגיטלית

דו"ח פיקוח רוחב 2021-2022

אתגרים ומאפיינים ייחודיים של מגזר רפואה דיגיטלית

פגיעה אפשרית במאגרים עלולה להיות משמעותית במיוחד לאור רגישות המידע השמור במאגרים.

איסוף ושמירת מידע רפואי ייחודי שלא קיים כמעט במערכות אחרות.

הגופים מחזיקים במאגרי מידע בהקפים עצומים.

התהליך במספרים שבוצע

11
שאלונים שהופצו

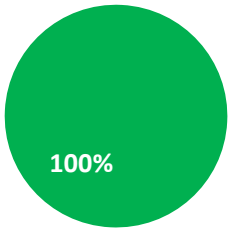
11
גופים שהשתתפו בפועל בהליך הפיקוח (למעט גופים שהוסרו מההליך או לא שיתפו פעולה)

8
הנחיות לתיקון ליקויים

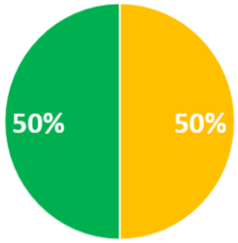
ממצאים – ליקויים מרכזיים:

ממצאי ליקויים בחתך קריטריונים על פני פירוט עמידת מפוקחי המגזר

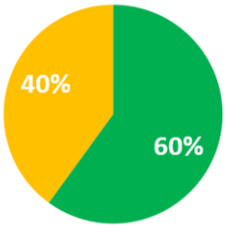
- רמת עמידה גבוהה
- רמת עמידה בינונית/חלקית
- רמת עמידה נמוכה



בקרה ארגונית



אבטחת מידע



ניהול מאגרי מידע

- מיקור חוץ - בהתאם לתקנה 15 לתקנות הגנת הפרטיות (אבטחת מידע),
- על הגופים המסתייעים בגורם חיצוני לצורך עיבוד מידע, לבחון, עוד בטרם ההתקשרות, את סיכוני אבטחת המידע הכרוכים בהתקשרות. בנוסף, על הגופים, בעלי המאגר, לוודא עריכת הסכם מול כל גורם חיצוני עימו הם התקשרו לצורך קבלת שירות הכרוך במתן גישה למאגר, כאשר יש לקבוע במפורש בהסכם את כל הוראות תקנה 15(א)(2) לתקנות הגנת הפרטיות (אבטחת מידע).
- מיקור חוץ – יש לודא כי כל גורם חיצוני אשר נותן שרותי מיקור חוץ בתחום מאגרי המידע נוקט באמצעים הנדרשים כדי להגן על מאגר המידע מידי תקופה, בהתאם לתקנה 15 ולהוראות ההסכם עימו, תוך נקיטה באמצעי בקרה ופיקוח על עמידתו של הגורם החיצוני בהוראות ההסכם ובהוראות התקנות.
- ניסוח הודעה לכל פניה בדיוור ישיר אשר תכיל את הנושאים הנדרשים

יש למנות ממונה על אבטחת מידע שיהיה כפוף ישירות למנהל מאגר המידע או למנהל פעיל של בעל המאגר או המחזיק בו, לפי העניין, או לנושא משרה בכירה אחת הכפוף ישירות למנהל המאגר.

עריכת ביקורות בנושא אבטחת מידע מידי 24 חודשים במאגר ברמת אבטחה בינונית ומעלה.

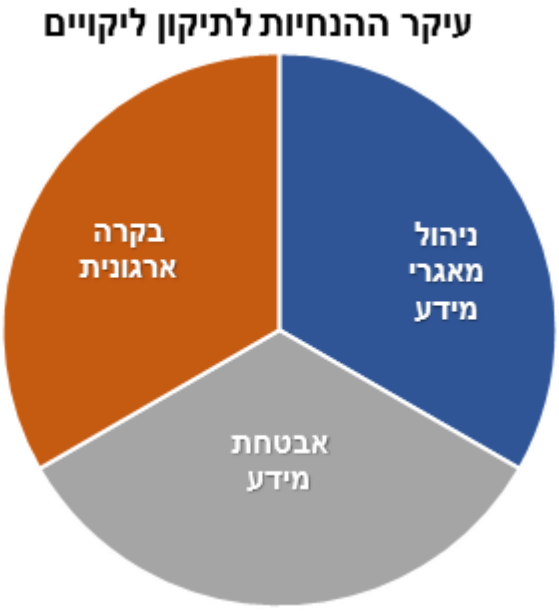
- יש להבטיח כי מערכות המאגר יישמרו במקום מוגן, המונע חדירה וכניסה ללא הרשאה התואמת את אופי פעילות המאגר ורגישות המידע בו. במאגרי מידע עליהם חלה רמת אבטחת מידע בינונית או גבוהה על בעל המאגר לנקוט בנוסף באמצעים לבקרה ולתיעוד של הכניסות והיציאות מאתרים שבהם מצויות מערכות תשתיות, חומרה, סוגי רכיבי תקשרות ואבטחת מידע, ושל כל הכנסה והוצאה של ציוד אל מערכות המאגר ומהן.

- יש לבצע תיעוד של כל אירוע המעלה חשש לאירוע אבטחה, בנוסף נוהל העבודה יכלול התייחסות לפעולות הנדרשות לביצוע, מנגנוני הדיווח, אופן הדיווח והליך הפקת לקחים במקרה של אירוע אבטחת מידע.

- יש לבחון את הצורך בחיבור התקנים ניידים ולפעול להגבלת או מניעת אפשרות לחיבור התקנים ניידים. במקרים בהם יוגדר כי קיים צורך בשימוש בהתקנים ניידים, יש להצפין את הנתונים תוך שימוש בשיטות הצפנה מקובלות כנקיטת אמצעים סבירים להגנה על מידע שהועתק להתקן הנייד.

- התקנת אמצעי הגנה מתאימים מפני חדירה לא מורשית או מפני תוכנות המסוגלות לגרום נזק או שיבוש למחשב או לחומר מחשב במאגר המידע המחוברים לרשת האינטרנט או לרשת ציבורית אחרת, בהתאם לדרישות התקנות.

- במאגר מידע שחלה עליו רמת האבטחה הגבוהה יש לבצע מבדקי חדירה מידי אחת לשנה וחצי, ולקיים דיון בממצאיהם תוך בחינת הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה בעקבותיהן, ותיקון הליקויים שהתגלו במסגרת המבדקים.



2. מגזר הרפואה הדיגיטלית- תמונת מצב

כללי

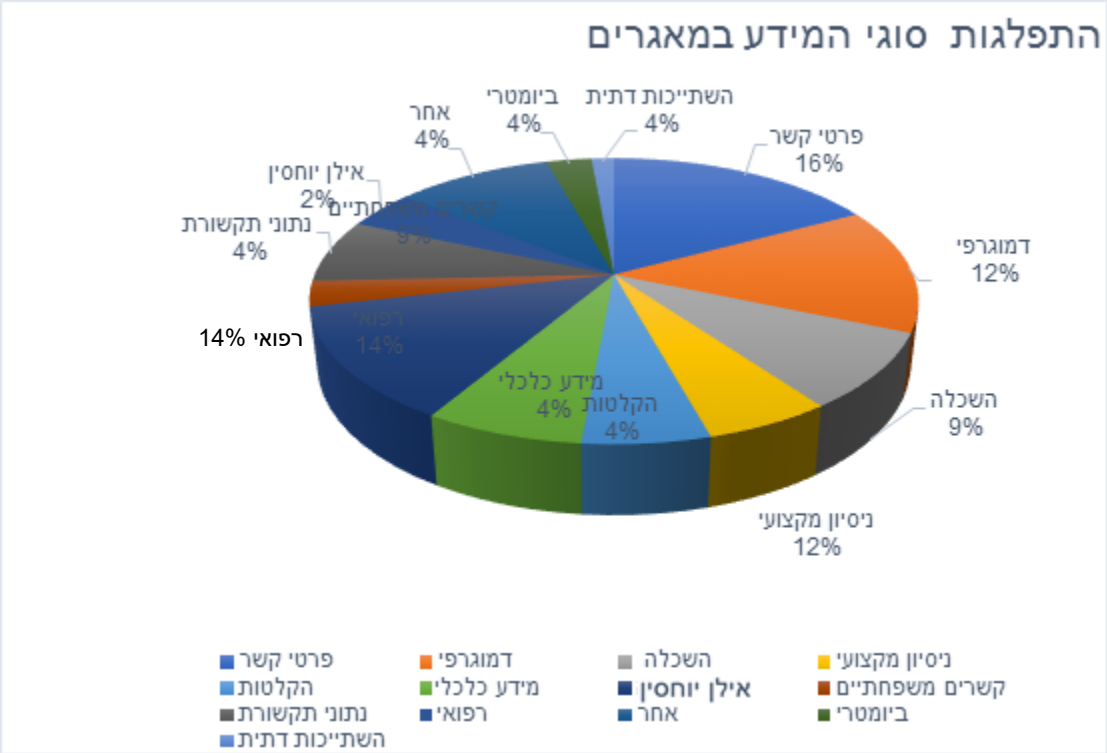
הדו"ח מתייחס לפיקוחי הרוחב שביצעה הרשות להגנת הפרטיות בתקופה שבין השנים 2021-2022 במגזר הרפואה הדיגיטלית.

רקע על המגזר

הרפואה הדיגיטלית מובילה לשינוי פרדיגמטי בפרקטיקה, במחקר, בפיתוח ובמבנה שוק הרפואה העולמי. זמינות נתונים ויכולת הצלבה ואנליזה של תשתיות מידע ובסיסי נתונים מגוונים (נתונים גנטיים, היסטוריה רפואית, נתונים תפעוליים וכד') פותחים פתח ליצירת חזיתות מחקר, פיתוח ופרקטיקה פורצות דרך. היקף המידע, מגוון המקורות שלו (מידע קליני, אופרטיבי, גנטי, מדיה חברתית ועוד) והשימושים שנעשים בו, מציבים אתגרים רבים בתחום הרגולציה, הגנת הפרטיות והגנת המידע.

במסגרת סקר הבוחן את סיכוני הפרטיות במגזרים השונים, נמצא מגזר רפואה דיגיטלית כיעד פיקוח רוחב משמעותי וזאת בשל מספר מאפיינים ייחודיים למגזר, כדלהלן:





2.3. תהליך עבודה

במטרה לפעול באופן המיטבי למען שמירה על האינטרס הציבורי וקידום הזכות לפרטיות, הרשות להגנת הפרטיות נוקטת בגישה מבוססת סיכון, הבוחנת תדיר את אפקטיביות מהלכיה ואת פוטנציאל ההשפעה הרוחבית שיש לפעולותיה על המשק. הרשות פועלת על פי תהליך הערכת מצב שנתי סדור המנתח את הסיכונים לפרטיות בכלל המשק. על מנת לעמוד במכלול האתגרים העומדים לפתחה, פועלת הרשות על-פי תהליך שנתי סדור המנתח את הסיכונים לפרטיות בכלל מגזרי המשק. סקר סיכוני פרטיות ממקד את תחומי הפעילות ומאפשר לרשות לעסוק, בין היתר, במגזרים שונים הכוללים מספר רב של נושאי מידע ומידע רגיש, וליישם את ממצאי הפעילות בצורה רוחבית.

תהליך העבודה של הליך פיקוח הרוחב כולל בתוכו מספר שלבים מובנים, ומתחיל בשלב של בניית תכנית עבודה שנתית ובחירת מגזרי הפיקוח בהתאם לתחומים בסיכון מוגבר לפרטיות שזיהתה הרשות, ולמדיניות השנתית של הרשות. התוכנית נבנית בהתחשב בגורמים הבוחנים את כמות והיקף המידע במגזר, רמת רגישות המידע, מידע שהצטבר ברשות בנוגע למגזר/נושא, תלונות ספציפיות שהתקבלו ברשות והצורך בבחינה מגזרית והבאתו לרמת עמידה נאותה.

הליך הפיקוח החל ב- 11 גופים המשתייכים למגזר רפואה דיגיטלית, שנבחרו על ידי הרשות.

בסיום ההליך, ב-8 מהגופים המפוקחים נמצאו ליקויים הדורשים תיקון. בהתאם לכך, הנחתה הרשות את הגופים לתקן את הליקויים שנמצאו, לספק תכנית מפורטת לתיקונם בליווי הצהרת נושא משרה בדבר יישומה. כחלק מההליך, בדקה הרשות באמצעות ביקורת חוזרת את אופן תיקון הליקויים בחלק מן הגופים, ממצאי הביקורת החוזרת העלו כי הגופים שיפרו את עמידתם בהוראות החוק והתקנות באופן משמעותי.

2.4. הקריטריונים הנבדקים ואופן חישוב רמת העמידה בהוראות חוק הגנת הפרטיות והתקנות מכוחו

במטרה לבחון את רמת העמידה המגזרית בהוראות החוק והתקנות, פנתה הרשות כאמור בדרישה למילוי שאלוני ביקורת, הבוחנים זאת על בסיס קריטריונים שונים ובהם:



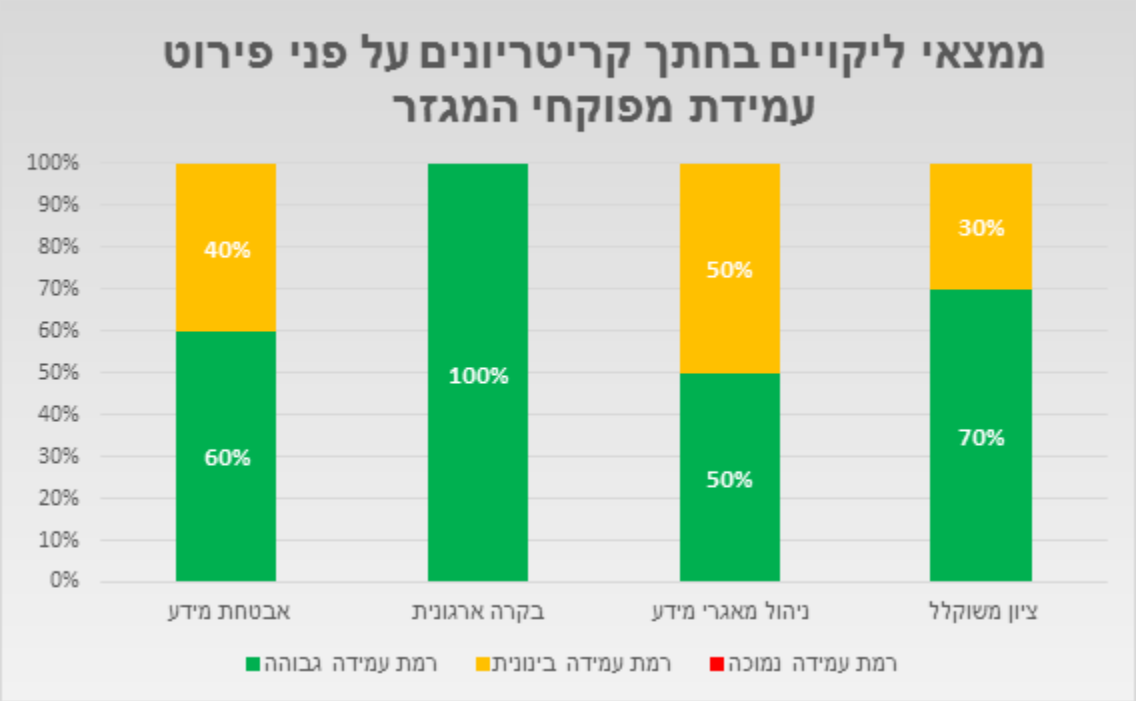
רמות העמידה ביחס לקיום הוראות חוק הגנת הפרטיות והתקנות מכוחו נקבעו בהתאם לשקלול הציונים שקיבלו הגופים, וזאת בהתבסס על בחינת הרשות את תשובותיהם לשאלוני הביקורת והמידע שנאסף במסגרתו:

עמידה של בין 80%-100% בקריטריונים, מוגדרת כרמת עמידה גבוהה;

עמידה של בין 50%-80% מוגדרת כרמת עמידה בינונית/חלקית;

עמידה של מתחת ל- 50% מוגדרת כרמת עמידה נמוכה.

3. ממצאים – ליקויים מרכזיים לפי קריטריונים ובמבט השוואתי והמלצות:



את טבלת הממצאים העיקריים שנמצאו במגזר וההנחיות שניתנו לתיקון הליקויים לגופים הספציפיים ניתן למצוא בנספח א' להלן.

בשקלול כל התחומים שנבדקו, כשליש מן הגופים הציגו רמת עמידה בינונית.

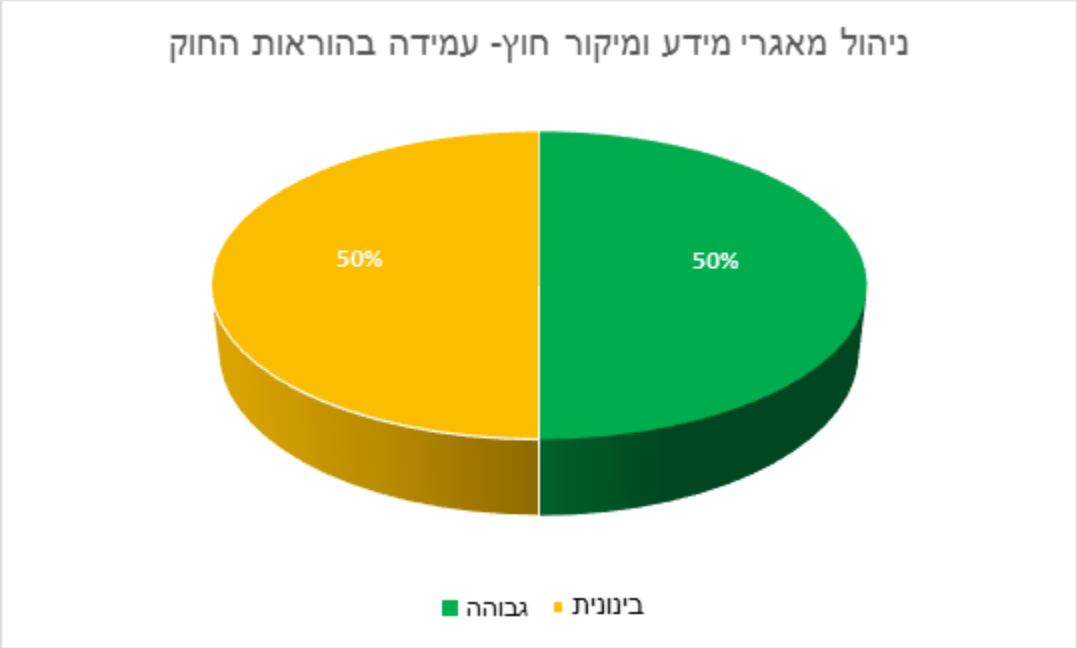
בתחום ניהול מאגרי מידע, מחצית מן הגופים עומדים בדרישות החוק ברמת עמידה חלקית, ומחצית נמצאים ברמת עמידה גבוהה.

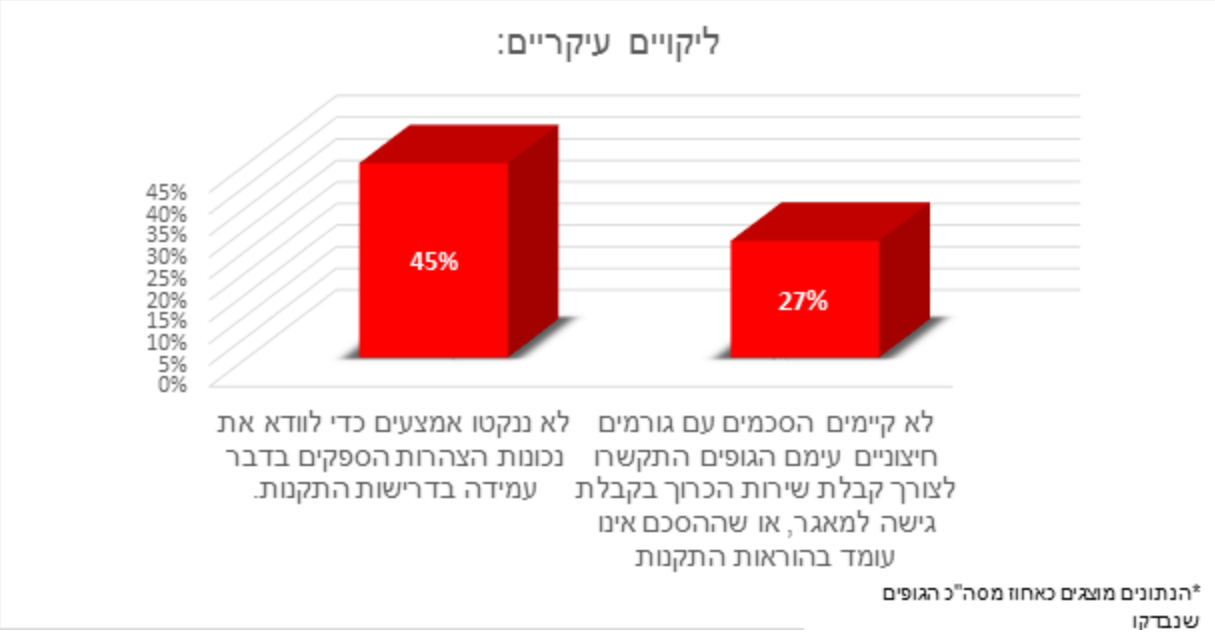
בתחום אבטחת מידע, כ-40% מן הגופים מצויים ברמת עמידה חלקית.

בתחום בקרה ארגונית וממשל תאגידי כל הגופים מצויים ברמת עמידה גבוהה.

ניהול מאגרי מידע ומיקור חוץ

ממצאים:





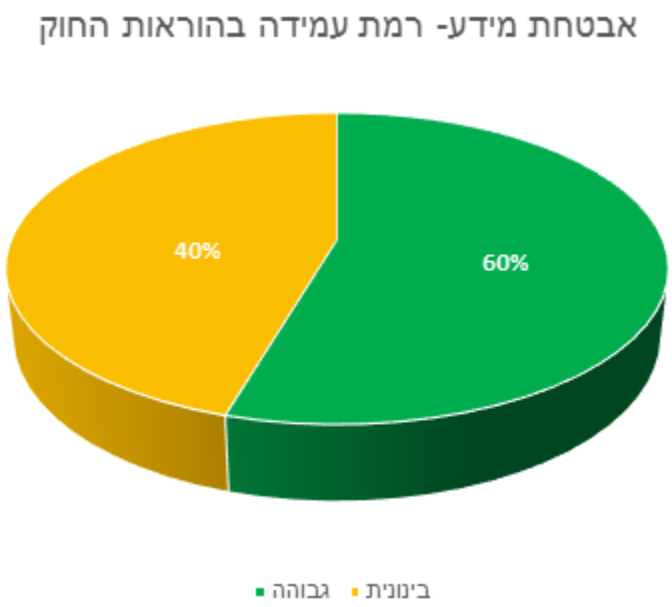
*הנתונים מוצגים כאחוז מסה"כ הגופים שנבדקו

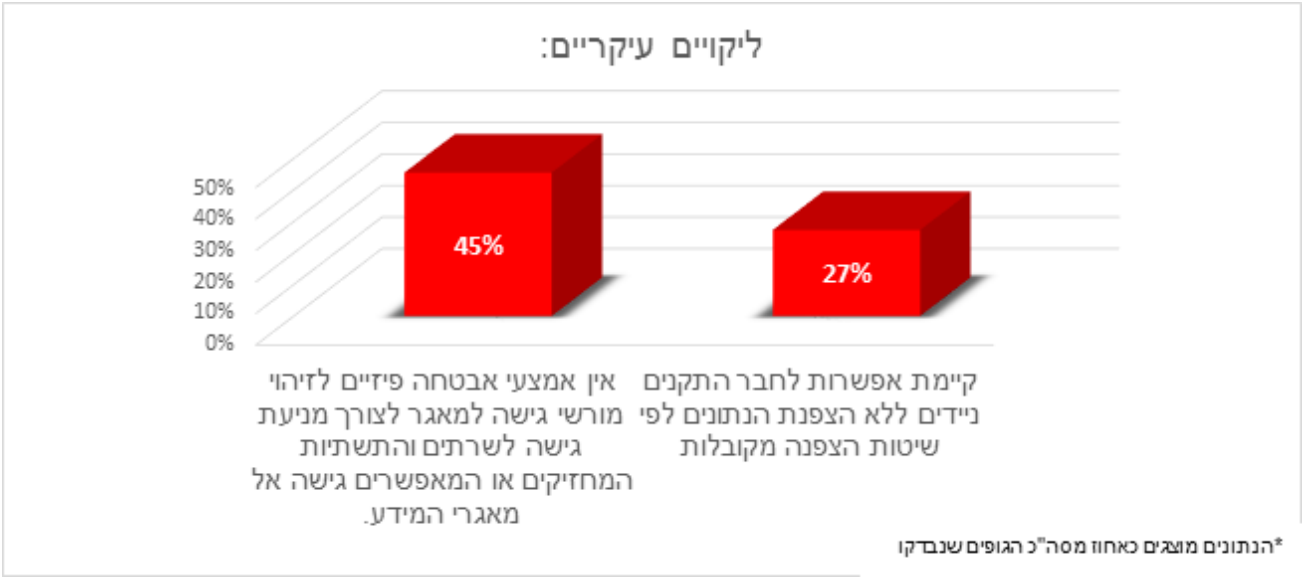
המלצות:

- יש ליידע את נושא המידע בדבר מקור הסמכות לאיסוף המידע על אודותיו. אם לא קיים מקור סמכות בחוק, יש לקבל את הסכמתו עבור איסוף המידע ושמירת פרטיו במאגרי המידע. זאת, תוך מתן הודעה בעת איסוף המידע, הכוללת התייחסות לשאלה האם חלה עליו חובה חוקית למסור את המידע כאמור, או שמסירת המידע תלויה ברצונו ובהסכמתו, וכן ציון המטרה אשר לשמה מבוקש המידע, למי יימסר המידע ומטרות המסירה, בהתאם להוראת סעיף 11 לחוק.
- בהתאם לתקנה 15 לתקנות אבטחת מידע, על הגופים המסתייעים בגורם חיצוני לצורך עיבוד מידע לבחון, עוד בטרם ההתקשרות, את סיכוני אבטחת המידע הכרוכים בהתקשרות.
- בנוסף, על הגופים לוודא עריכת הסכם מול כל גורם חיצוני שמחזיק במאגר, בו ייקבעו במפורש כל הרכיבים המנויים בתקנה 15(א) (2)לתקנות, לרבות חובתו של הגורם החיצוני לדווח, אחת לשנה לפחות, לבעל מאגר המידע על אודות אופן ביצוע חובותיו לפי התקנות וההסכם, ולהודיע לבעל המאגר במקרה של אירוע אבטחה.
- בעניין זה יש לנקוט אמצעי בקרה ופיקוח נאותים על עמידת הגורם החיצוני בהוראות ההסכם 6 והתקנות, כנדרש בתקנה 15 ובהנחיית רשם מאגרי המידע מס' 2011/2.

3.1. אבטחת מידע

ממצאים:





*הנתונים מוצגים כאחוז מסה"כ הגופים שנבדקו

המלצות:

- על הגופים לבצע בחינה עצמית לצורך סיווג רמת אבטחת המידע של מאגרי המידע בהתאם לקבוע בתוספת בתקנות. על הגופים לבדוק את סוג המידע שהם אוספים, את המטרות והשימושים שנעשה במידע הנ"ל. בעניין זה, עמדת הרשות היא כי רמת אבטחת המידע הנדרשת של מאגרי המידע לא משתנה, גם אם מאגרי המידע מנוהלים או מעובדים בצורה מפוצלת על גבי מספר מערכות טכנולוגיות שונות בעלות מספר בעלי הרשאה שונה, שכן הבחינה לצורך סיווג רמת האבטחה הינה מהותית, ואינה תלויה בהיבטים הטכניים של אופן ניהול המידע. בהתאם לכך, מספר בעלי ההרשאה לצורך קביעת רמת האבטחה של המאגר הינו סך כל בעלי ההרשאה לכלל המערכות הטכנולוגיות המשמשות את מאגר המידע הרלוונטי.
- על הגופים לוודא כי תיעוד של אירועי אבטחת מידע יישמר, ויגובש נוהל עבודה סדור בנושא ,בהתאם לתקנה 11 לתקנות. בנוסף, נוהל העבודה יכלול התייחסות לפעולות הנדרשות לביצוע, מנגנוני הדיווח, אופן הדיווח והליך הפקת לקחים במקרה של אירוע אבטחת מידע .במאגרי מידע ברמת אבטחה גבוהה יש לקיים דיון רבעוני (וברמת אבטחה בינונית אחת לשנה)באירועי האבטחה ולבחון את הצורך בעדכון הנוהל.
- על הגופים לבחון את הצורך בחיבור אמצעים נתיקים. ככל שיוחלט כי לא קיים צורך ממשי או שהצורך מינימאלי – מוצע להגביל השימוש למתכונת ההולמת את רמת אבטחת המידע שחלה על המאגר, את רגישות המידע, הסיכונים המיוחדים למערכות המאגר או למידע הנובעים מחיבור ההתקן הנייד למערכת, ואת קיומם של אמצעי הגנה מתאימים מפני סיכונים אלה. במקרים בהם יוגדר כי קיים צורך בשימוש באמצעים נתיקים, יש להצפין הנתונים באמצעות שיטות הצפנה מקובלות.
- על הגופים לוודא שבכניסה לאתר האינטרנט המאפשר גישה למאגר המידע נעשה שימוש באמצעי פיזי הנתון לשליטתו הבלעדית של המורשה, בהתאם לתקנה 9(ב)(1)לתקנות, וכן לוודא קיום תיעוד עבור אירועי אבטחת מידע, בהתאם לתקנה 11 לתקנות.
- על הארגון לקבוע מדיניות סיסמאות חזקה הכוללת סיסמאות מורכבות המוחלפות בתדירות של עד 6 חודשים. כמו כן יש לעגן את מדיניות הסיסמאות בנוהל עבודה כנדרש בתקנה 9 (ב) לתקנות.
- על הארגון לנהל מנגנון תיעוד אוטומטי, שיאפשר ביקורת על הגישה למערכות המאגר ויכלול את הנתונים הבאים: זהות המשתמש, התאריך והשעה של ניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה, כנדרש בתקנה 10 .נתוני התיעוד של מנגנון הבקרה יישמרו למשך 24 חודשים לפחות.
- בנוסף, על בעל מאגר המידע לקבוע נוהל בדיקה שגרתי עבור נתוני התיעוד של מנגנון הבקרה.

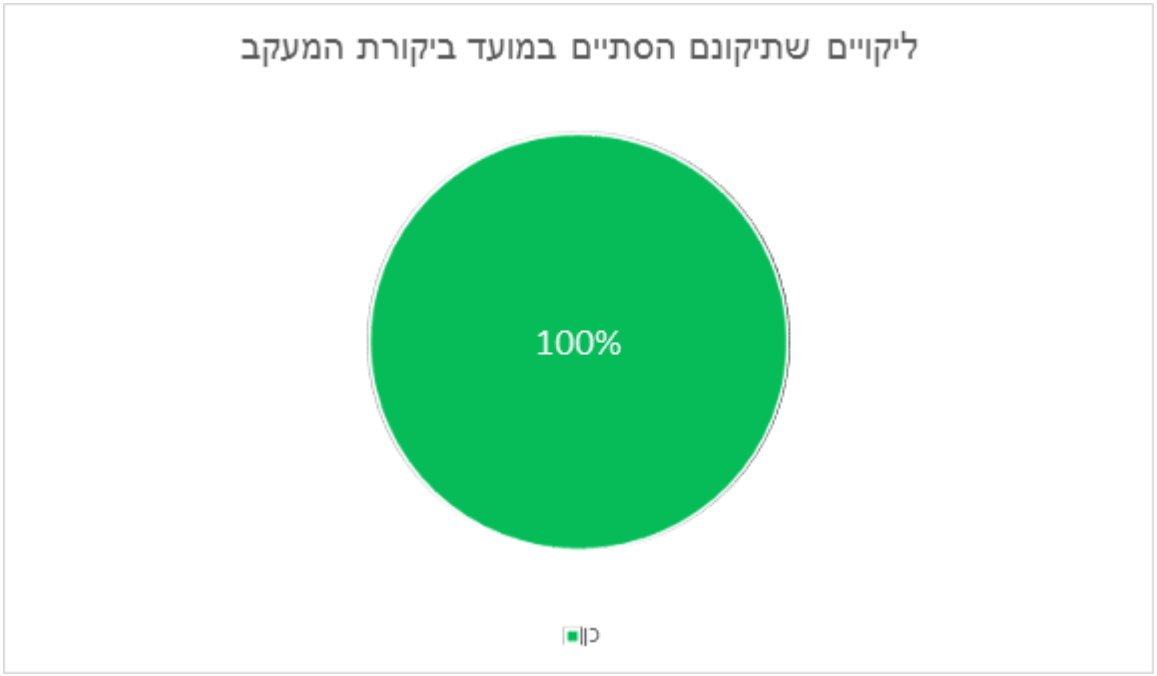
4. מסקנות - תמונת מצב

- התמונה העולה מהליך הפיקוח מצביעה על מודעות רבה של המפוקחים לדרישות החוק בנושאי **בקרה ארגונית וממשל תאגידי.** במבט משוקלל של הליך הפיקוח, מרבית הגופים נמצאים ברמת עמידה גבוהה בתחום זה.
- **בתחום אבטחת המידע**, כ- 40% מן הגופים מצויים ברמת עמידה בינונית בלבד. לנוכח העובדה כי המידע המצוי בגופים אלו הוא מידע רגיש, ובכלל זה מידע רפואי, וכן לנוכח העובדה שמדובר על מגזר דיגיטלי במהותו, נדרשת הגברת המודעות להפעלת המנגנונים שנבנו במסגרת הבקרה הארגונית באופן מלא ויעיל על מנת שיבטיחו עמידה מלאה בדרישות אבטחת המידע.
- בתחום **ניהול מאגרי מידע** כמחצית מן הגופים מצויים ברמת עמידה בינונית בלבד. הגורם המרכזי בתחום זה הינו עמידה חלקית בדרישות התקנות והנחיות הרשם בהתקשרות עם גורם חיצוני לצורך עיבוד או ניהול מידע
- על הגופים להגביר את המודעות לחובת עמידה מלאה בכלל הדרישות הנוגעות לאבטחת המידע, תוך הבנת החשיבות להגנה מלאה על מידע רפואי רגיש, הנאסף בהיקפים גדולים ותוך שימוש משמעותי באמצעי ניהול ועיבוד מידע דיגיטליים.
- נדרשת תשומת לב מיוחדת להגברת המודעות לדרישות החוק במתן גישה לגורם חיצוני לצורך עיבוד או ניהול מידע של הארגון.

5. שיפור ותיקון ליקויים בעקבות הליך הפיקוח בעת ביקורת המעקב

במהלך שנת 2023, נערך מעקב תיקון ליקויים במגזר זה, שבמסגרתו נדרשו הגופים המפוקחים לנקוט בגישה מבוססת סיכון, ומתן עדיפות, ככל הניתן, לטיפול תחילה בליקויים מתחום אבטחת המידע ולאחר מכן לתיקון הליקויים ביתר הקריטריונים. בנוסף, בוצעו ע"י הרשות להגנת הפרטיות, באופן מדגמי, פיקוחי מעקב על חלק מהגופים בהם נמצאו ליקויים. ההחלטה על קיום פיקוח המעקב בגופים מסוימים התקבלה לאחר שנלקחה בחשבון כמות הליקויים, מהות הליקויים והמסמכים אותם נדרשו הגופים להציג לרשות, בכדי לוודא את יישום דרישות הרשות לתיקון הליקויים. בעת פיקוח המעקב בחנה הרשות את אופן התקדמות תיקון הליקויים אצל הגופים, ואת העמידה בלוחות הזמנים שהגדירו ליישום התוכנית ותיקון יתרת הליקויים שטרם תוקנו.

במסגרת ביקורת המעקב שנעשתה בקרב 45% מהגופים במגזר רפואה דיגיטלית שקיבלו הנחיות לתיקון ליקויים, נמצא כי הגופים שנכללו בביקורת המעקב שיפרו את העמידה בתקנות אבטחת מידע באופן משמעותי וכי כלל הליקויים תוקנו וטופלו.



לגבי הגופים המפוקחים בכלל ולגבי גופים אלו בפרט, הרשות שומרת לעצמה את שיקול הדעת בכל הנוגע לביצוע הליכי אכיפה משלימים, לרבות בכל הנוגע למסירת תכניות העבודה לתיקון הליקויים וליישומן. פיקוחי המעקב שבוצעו במגזר רפואה דיגיטלית מעידים באופן חד משמעי על כך שעצם קיום הליכי פיקוח הרוחב מהווה תמריץ לגופים השונים לבצע הליך בחינה באשר לאופן הציות לחוק ולתקנות. אלה מעידים על שיפור משמעותי בעמידת הגופים המפוקחים ביישום הוראות הדין בתחום הגנת הפרטיות כתוצאה מהליך פיקוח הרוחב.

6. סיכום

בגופים במגזר הרפואה הדיגיטלית נשמר ומנוהל מידע רגיש אודות אחוז גבוה מהאוכלוסייה. ממצאי הליך פיקוח הרוחב במגזר רפואה דיגיטלית העלה ממצאים המצביעים על ליקויים בעיקר בנוגע לעמידה בהוראות החוק בתחום אבטחת מידע.
יצוין כי חלק משמעותי יחסית מן הגופים במגזר הרפואה הדיגיטלית, מחזיק ברמת אבטחה גבוהה, ולכן יש חשיבות רבה לביצוע היערכות מתאימה לצורך עמידה בדרישות תקנות אבטחת מידע.
ניכר, כי עצם קיום הליך פיקוח הרוחב עורר אצל הגופים שנבדקו תהליך בחינה והנעה לשיפור אופן הציות לחוק ולתקנות, כאשר בסיום ההליך כאמור, הגופים שבהתנהלותם נתגלו ליקויים, נדרשו להציג לרשות התחייבות נושא משרה ותכנית עבודה לתיקון הליקויים.

הרשות להגנת הפרטיות תמשיך לפעול לאכיפת מדיניותה בקרב בעלי מאגרי מידע והמחזיקים בהם באמצעות הליך פיקוחי הרוחב, לרבות באמצעות ביקורות חוזרות בגופים שהונחו לתקן ליקויים, וזאת לשם הגברת עמידתם בהוראות החוק והתקנות, ועל מנת לחזק את ההגנה על הזכות החוקתית לפרטיות.

במסגרת תכנית העבודה של הרשות ולשם בחינת ההשפעה שיצרה פעילות פיקוח הרוחב על המגזרים שנבדקו, תשקול הרשות לבחון את השינוי היחסי ברמת הציות להוראות החוק במגזר רפואה דיגיטלית, על ידי בחינת גופים נוספים ואחרים במגזר זה, במועד שייקבע לאחר פרסום הדו"ח המגזרי.