# דו"ח פיקוח רוחב

## ממצאי הליך פיקוח הרוחב
## בקרב מגזר בתי חולים



## תוכן עניינים

**1.תקציר מנהלים..... 3**

1.1.מגזר בתי חולים..... 3

1.2.תהליך העבודה..... 3

1.3.ליקויים, מסקנות והמלצות עיקריות..... 4

**2. בתי חולים - תמונת מצב ..... 5**

2.1.כללי..... 6

2.2.רקע על המגזר..... 6

2.3.תהליך עבודה..... 8

2.4.הקריטריונים הנבדקים ואופן חישוב רמת העמידה בהוראות חוק הגנת הפרטיות והתקנות מכוחו..... 9

**3. ממצאים – ליקויים מרכזיים לפי קריטריונים ובמבט השוואתי והמלצות: ..... 10**

3.1.בקרה ארגונית..... 11

3.2.העברת מידע בין גופים..... 13

3.3.אבטחת מידע..... 15

3.4.ניהול מאגרי מידע..... 18

**4.מסקנות/ תמונת מצב ..... 20**

**5.מעקב תיקון ליקויים ..... 21**

**6.סיכום..... 21**

# 1. תקציר מנהלים

מערך פיקוח הרוחב ברשות להגנת הפרטיות מופקד על עריכת פיקוחי רוחב מגזריים 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 "תקנות הגנת הפרטיות" או "התקנות"**).
מטרות הליך פיקוח הרוחב הן להתניע ולהגביר מודעות ותהליכי ציות לחוק ולתקנות בקרב הגופים המפוקחים, להסיק מסקנות בדבר דגשים נדרשים לצמצום פערים קיימים הן ברמת הגופים המפוקחים והן ברמת המגזר, להגביר את האכיפה היזומה של הרשות, וכן להציג תמונת מצב לציבור בנוגע לדרישות הציות להגנת הפרטיות ואבטחת המידע בקרב המגזר הנבחר.

לנוכח העובדה כי הליך פיקוח הרוחב מעצם טיבו וטבעו מתמקד בעצם קיום נהלים ובקרות, וכן נסמך על תשובות הגופים המפוקחים ומספר מצומצם של מסמכים מאמתים – ההליך אינו מהווה בהכרח סוף פסוק ובידי הרשות יש מנעד רחב של כלי אכיפה נוספים, משלימים או עומדים בפני עצמם, אשר מאפשרים בירור עומק במערכות עצמן לצורך בחינת עמידה בהוראות החוק והתקנות.

## 1.1. מגזר בתי החולים

במסגרת תהליך הערכת מצב שנתי שערכה הרשות להגנת הפרטיות, אשר בוחן את סיכוני הפרטיות במשק, מגזר בתי החולים אותר כאחד מיעדי פיקוח הרוחב המשמעותיים, וזאת בשל מאפייניו הייחודיים של מגזר זה בהיבטי הפרטיות, הבאים לידי ביטוי במספר נקודות:

1. רגישות רבה של המידע המנוהל – ניהול מידע אישי בהיקפים גדולים של רבבות חולים ומטופלים (הכוללים בעיקר מידע רפואי מלא על המטופל, נתונים דמוגרפיים, נתונים כספיים, קשרים משפחתיים וכד').
2. ניהול מידע אישי של כלל עובדי בית החולים (להלן: "הצוות הרפואי").
3. העברת מידע רפואי בהיקפים נרחבים בין גופים שונים: בין בתי החולים, בין בתי החולים לקופות החולים, בין בתי החולים למשרד הבריאות ועוד.

ניהול מידע אישי רגיש על אודות חולים, מטופלים וצוות רפואי מחייב את אותם בתי החולים לעמוד בדרישות אבטחת המידע, כולל הסדרת נהלי עבודה בתחום אבטחת המידע והתמודדות עם אירועי אבטחת מידע, וכן מתן מידע בהתאם להוראות החוק והתקנות לנושא המידע לצורך קבלת הסכמתו לשמירתו במאגר.

כמו-כן, על בתי החולים לקיים מנגנון הרשאות גישה יעיל בהתאם לצורך לדעת, וכן לקיים מעקב ובקרה בקרב ספקים חיצוניים המקבלים גישה למידע.

## 1.2. תהליך העבודה

בהליך פיקוח הרוחב במגזר זה, הרשות פנתה בדרישה למילוי שאלוני ביקורת ל- 28 גופים במגזר בתי החולים, המנהלים מאגרי מידע של מטופלים וצוות רפואי. 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 ארבעה קריטריונים עיקריים בתחום הגנת הפרטיות: בקרה ארגונית; ניהול מאגרי מידע ושימוש בשירותי מיקור חוץ; אבטחת מידע; העברת מידע בין גופים ציבוריים. הציונים שניתנו לגופים עוסקים במהותם בהוראות ציות ואחריות תאגידית. הציונים ניתנו בהתאם למענה ולמסמכים שסופקו על ידי הגופים, ומשקפים את מודעותם להוראות החוק ותקנות אבטחת מידע. לאחר קבלת השאלונים המלאים מהגופים המפוקחים, בחנה הרשות את המענה והמסמכים הנלווים.

בסיום ההליך, נמצאו ליקויים הדורשים תיקון בכלל הגופים שנבדקו, ובהתאם דרשה הרשות מאותם גופים לתקן את הליקויים שנמצאו, ולספק תכנית מפורטת לתיקונם בליווי הצהרת נושא משרה לביצוע והשלמת התיקונים. כחלק מההליך, ביצעה הרשות ביקורת חוזרת לבדיקת יישום הדרישה לתיקון הליקויים בחלק מן הגופים. ממצאי הביקורת החוזרת העלו, כי הגופים שיפרו את עמידתם בהוראות החוק והתקנות באופן משמעותי.

### 1.3. ליקויים, מסקנות והמלצות עיקריות

במגזר בתי חולים בישראל מרבית הגופים הציגו רמת עמידה גבוהה בשקלול כל התחומים שנבדקו. כ-37% מהגופים מצויים ברמת עמידה חלקית.

בשקלול הציונים שניתנו לגבי מידת ההיענות להוראות החוק והתקנות, נמצא כי הציון הממוצע של המגזר עומד על 76%.

באשר לרמת העמידה בדרישות אבטחת המידע, ממצאי פיקוח הרוחב העלו כי

כ-11% מן הגופים נמצאים ברמת עמידה נמוכה; וקרוב ל-20% מן הגופים נמצאים ברמת עמידה בינונית.

בתחום ניהול מאגרי מידע, שליש מן הגופים נמצאים ברמת עמידה נמוכה בלבד וכשליש מן הגופים נמצאים ברמת עמידה בינונית.

בתחום בקרה ארגונית וממשל תאגידי, מחצית הגופים מצויים ברמת עמידה מלאה בדרישות החוק.

בתחום העברת מידע בין גופים ציבוריים, שליש מן הגופים נמצאים ברמת עמידה נמוכה בלבד, ושני שליש מצויים ברמת עמידה בינונית.

נוכח הממצאים שעלו מהליך פיקוח הרוחב, כל הגופים שנבדקו (28 מתוך 28) קיבלו הנחיות ספציפיות לתיקון הליקויים שנמצאו אצלם.

# ממצאי הליך פיקוח רוחב בקרב מגזר בתי החולים

## דו"ח פיקוח רוחב 2021-2022

### אתגרים ומאפיינים ייחודיים של מגזר בתי החולים

במגזר קיימים מספר סוגים של בתי חולים:
בתי חולים כלליים, כולל רפואה דחופה.
בתי חולים לאוכלוסיות מיוחדות – לשיקום (לוינשטיין), לילדים (שניידר) וכו'.
מרכזים לטיפולי יום.

מדובר במגזר אשר מאופי עיסוקו מחזיק במידע רגיש במיוחד על צנעת פרטיותו ובריאותו של ציבור החולים המטופלים על ידו.

הנתונים במאגרי המידע חשופים לגורמים רבים בתוך בתי החולים, ומועברים בין בתי החולים, וכן מבתי החולים אל קופות החולים.

### התהליך שבוצע במספרים

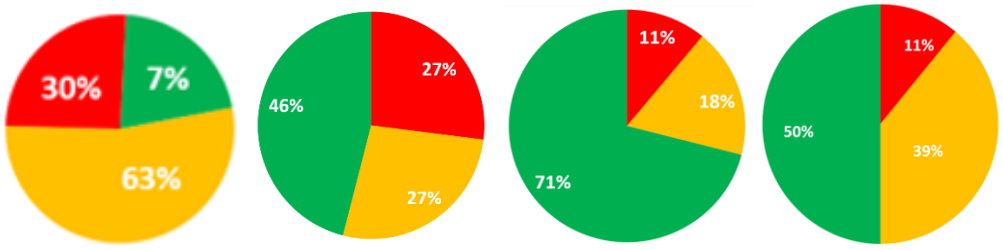
**28** שאלונים שהופצו

**28** דרישות להשלמת מידע חסר בכתב

**28** הנחיות לתיקון ליקויים

## ממצאים – ליקויים מרכזיים:

### ממצאי ליקויים בחתך קריטריונים על פני פירוט עמידת מפוקחי המגזר




בקרה ארגונית | אבטחת מידע | ניהול מאגרי ושימוש במיקור חוץ | העברת מידע בין גופים ציבוריים

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

## 2. בתי חולים- תמונת מצב

### כללי

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

### רקע על המגזר

בבתי החולים מתבצע ניהול מידע אישי בהיקפים גדולים של רבבות חולים ומטופלים (הכוללים בעיקר מידע רפואי מלא על המטופל, נתונים דמוגרפיים, נתונים כספיים, קשרים משפחתיים וכד'), וכן ניהול מידע אישי של כלל העובדים המועסקים בבתי החולים (להלן: "הצוות הרפואי").

היבטי איסוף המידע הפרטי של המשתמשים מתקיימים במגזר זה בשני תחומי ליבה:

**<u>פלטפורמת בתי חולים</u>**

תחום זה מאפשר שילוב בין בתי החולים השונים – ציבוריים ופרטיים, והנגשת המידע המוחזק על ידם למשתמשים דרך פלטפורמות שבאמצעותן ניתן לקבוע תורים על פי העדפות שמגדיר.

**<u>איסוף ושיתוף מידע כבסיס לתכנון, פיקוח ולפיתוח שוק בתי חולים</u>**

העברת מידע רפואי בהיקפים נרחבים בין גופים שונים: בין בתי החולים, בין בית החולים לקופות החולים ובין בית החולים למשרד הבריאות.

במסגרת הליך הערכת מצב שנתית הבוחן את סיכוני הפרטיות במגזרים השונים, נמצא מגזר בתי החולים כיעד פיקוח רוחב משמעותי וזאת בשל מספר מאפיינים ייחודיים למגזר, כדלהלן:

## מאגרי מידע בהיקף גדול במיוחד

- ניהול המידע אודות מטופלים וצוות רפואי מצריך החזקה במאגרי מידע עם מידע אישי רב ורגיש, כגון: מידע רפואי, פרטי מטופלים, נתונים דמוגרפיים, ועוד.
- משמעות הדבר הוא צבירה של היקף עצום של מידע על רוב האוכלוסייה.
- איסוף מידע אישי בהיקפים עצומים אלו, מהווה סיכון פוטנציאלי משמעותי לפרטיות של נושאי המידע שמידע אודותיהם מצוי במאגרים.

## רגישות המידע

- ניהול נתונים אישים בהיקפים של רבבות חולים ומטופלים, הכוללים בעיקר מידע רפואי מלא על המטופלים.
- פגיעה אפשרית במאגרי המידע, עלולה להיות משמעותית במיוחד לאור רגישות המידע השמור במאגרי בתי החולים.

## היקף גישה למידע

- גישה לרשת ניתנת לצוות המטפל בלבד על-פי הרשאות קיימות, בהתאם לפרופיל ולתפקיד במוסד הרפואי
- ריבוי מורשים מעבר לצורך ההכרחי לדעת, עשוי לפגוע בפרטיות נושאי המידע, ולהוות סיכון לאבטחת המידע במאגרים.

## איסוף מידע ושמירתו

- המערכת מאפשרת לרופא המטפל גישה למידע רפואי חשוב ומדויק באופן ישיר ומהיר. מדובר בעיקרי המידע הרפואי מתוך התיק הרפואי של המטופל, שמקורו בבתי החולים ובקופות החולים.
- הנתונים במאגרי המידע חשופים לגורמים רבים בתוך בתי החולים, ומועברים בין בתי החולים ולקופות החולים.
- כמו כן, היקף המידע והשוני בין סוגי המידע הרפואי, מחייבים בדיקה ופיקוח כי לא נעשה במידע שימוש מעבר למטרה שלשמה נמסר.

### 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. על מנת לעמוד במכלול האתגרים העומדים לפתחה, פועלת הרשות על-פי תהליך שנתי סדור המנתח את הסיכונים לפרטיות בכלל מגזרי המשק. תהליך זה 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. בחירת מגזרי הפיקוח מבוצעת 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 נעשה ב- 28 בתי חולים, שנבחרו על ידי הרשות. בסיום ההליך, ב-28 הגופים 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 השלמת התיקונים.

### 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 לבתי החולים בדרישה למילוי שאלוני ביקורת, הבוחנים זאת על בסיס קריטריונים שונים ובהם:



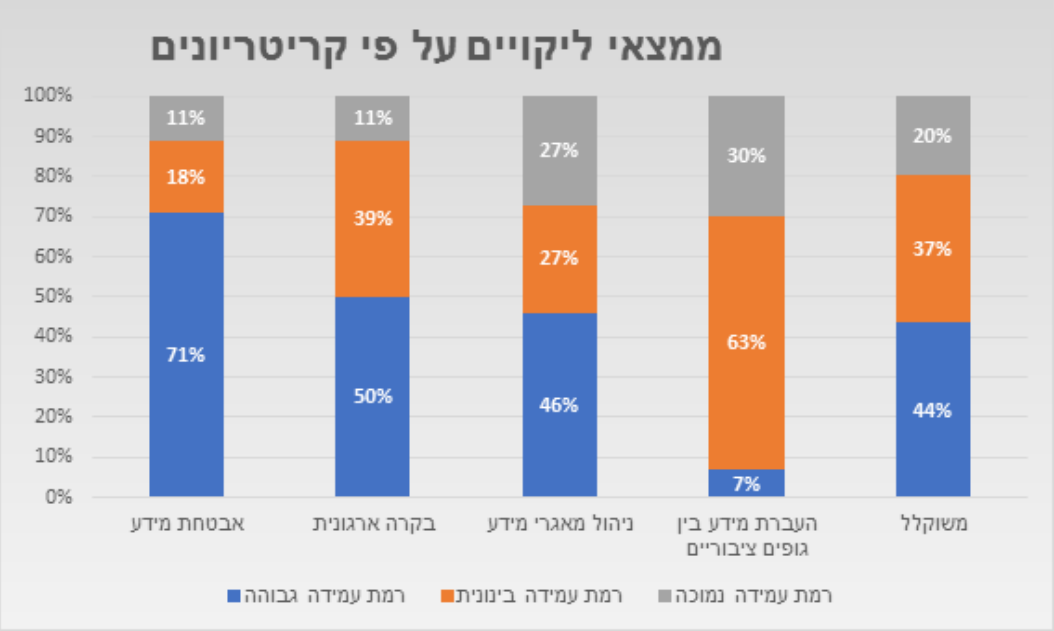

רמות העמידה ביחס למודעות ויישום הוראות חוק הגנת הפרטיות והתקנות מכוחו נקבעו בהתאם לשקלול הציונים שקיבלו הגופים, וזאת בהתבסס על בחינת הרשות את תשובותיהם לשאלוני הביקורת והמידע שנאסף במסגרתו:

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 והמלצות – ליקויים מרכזיים לפי קריטריונים




בתחום אבטחת מידע כ- 30% מן הגופים נמצאים ברמה נמוכה ובינונית בעמידה בהוראות החוק והתקנות.

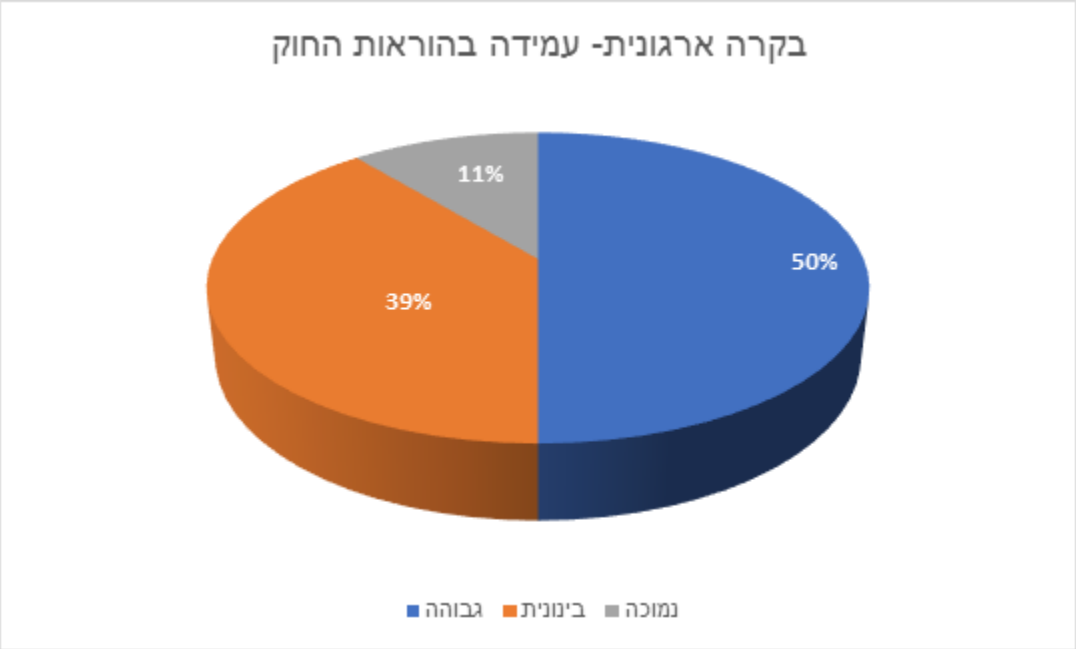
בתחום ניהול מאגרי מידע, כ- 30% מן הגופים נמצאים ברמת עמידה נמוכה בעמידה בהוראת החוק.

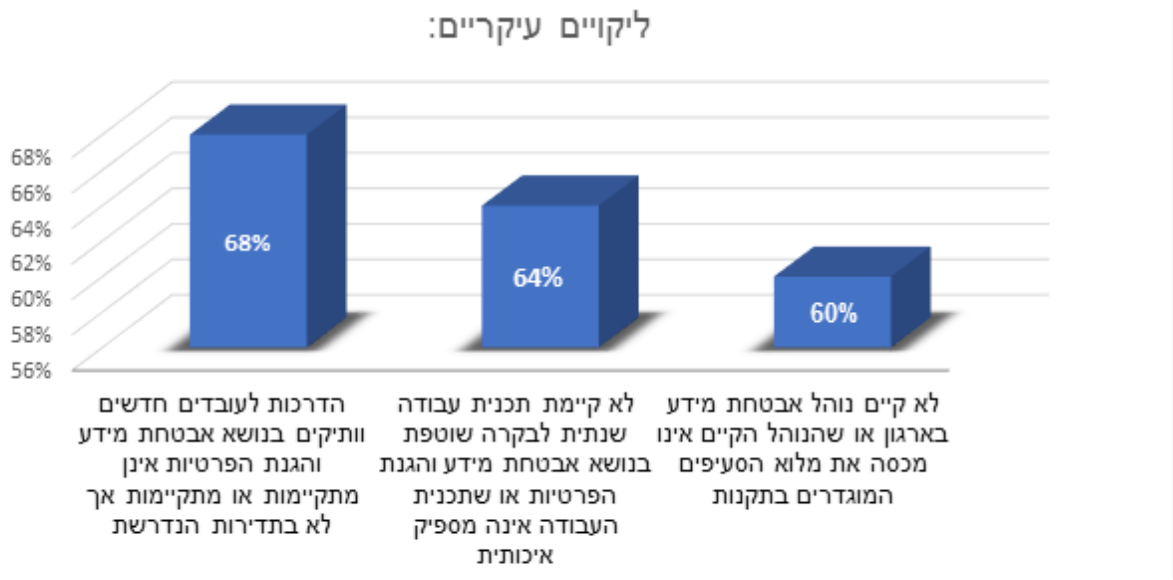
בתחום בקרה ארגונית וממשל תאגידי, נמצא כי 50% מהגופים נמצאים ברמה נמוכה ובינונית בהוראות החוק.

בתחום העברת מידע בין גופים ציבוריים, נמצא כי 30% מהגופים נמצאים ברמה נמוכה בעמידה בהוראות החוק.

## בקרה ארגונית

## ממצאים:



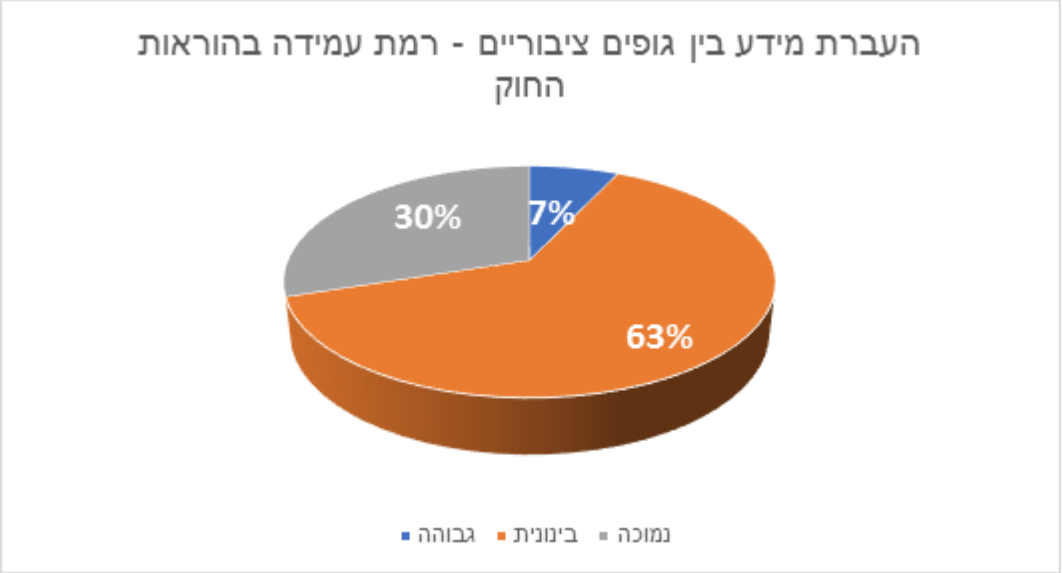

*הנתונים מוצגים כאחוז מסה"כ הגופים שנבדקו

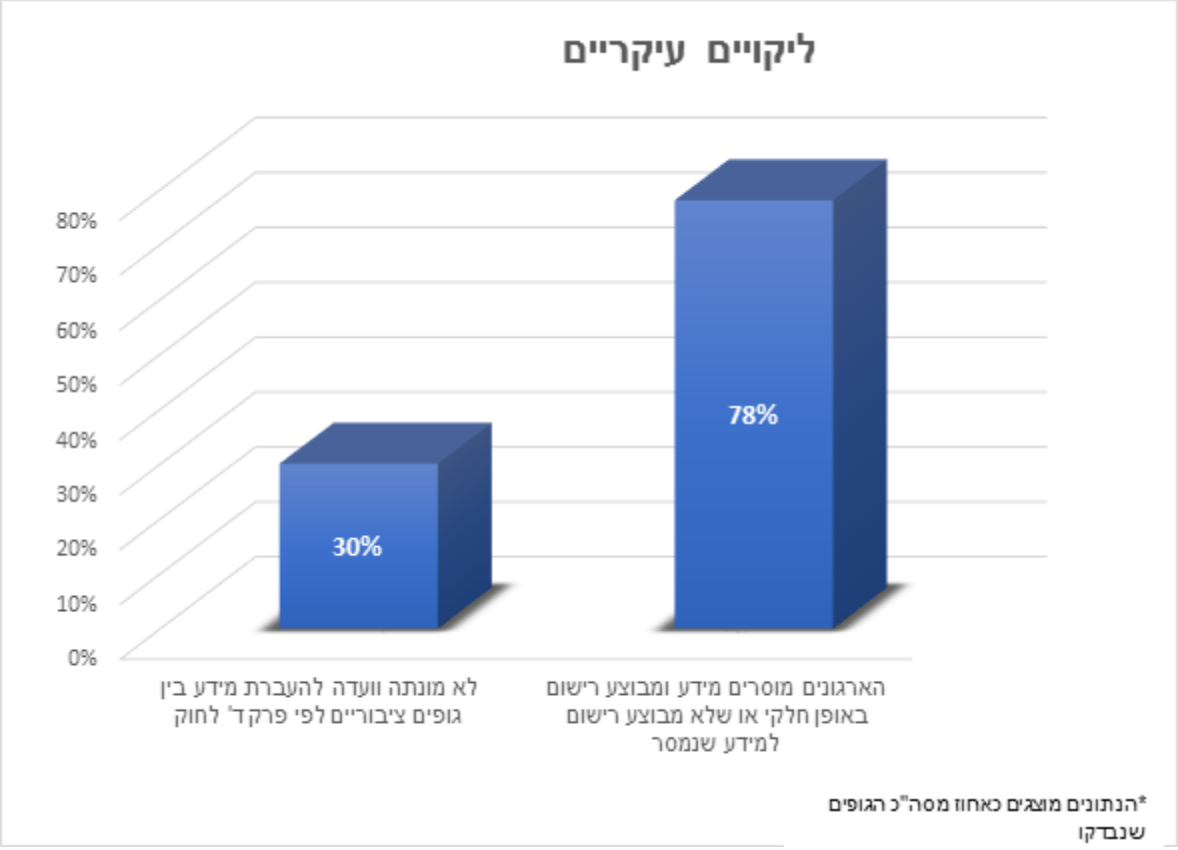
**המלצות:**

- כחלק ממכלול התיקונים הנדרשים כדי לעמוד בהוראות החוק והתקנות, נדרשים הגופים, בין היתר, לוודא את רישום כלל מאגרי המידע שבבעלותם בהתאם להוראות החוק, תוך התאמה בין זהות מנהל המאגר במסמכי החברה לבין הרשום אצל רשם מאגרי המידע.
- על הגופים לוודא כי מונו כדין הגורמים הנדרשים בחוק ובתקנות, לרבות הוצאת כתבי מינוי רשמיים למנהל המאגר ולממונה אבטחת המידע היכן שמינויו נדרש, וכן לוודא שכתבי המינוי כוללים את כל הפרטים הנדרשים בהתאם לסעיף 7 לחוק ולתקנה 4 לתקנות.
- על הגופים לוודא כי קיימים נהלי אבטחת מידע בארגון הכוללים התייחסות לנושאים כגון :אבטחה פיזית, הרשאות גישה, תיאור אמצעי ההגנה, הוראות למורשי גישה, ניהול סיכונים ,התמודדות עם אירועי אבטחת מידע, התקנים ניידים וכו'. בנוסף, על הארגונים לגבש נוהל אבטחת מידע ולבחון את הצורך לעדכנו אחת לשנה, כנדרש בתקנות (תקנה 4).
- בהתאם להוראות התקנות, יש לבצע הדרכות לכלל בעלי הרשאות הגישה בטרם יקבלו גישה למאגר המידע, ובמאגרי מידע בעלי רמת אבטחה בינונית או גבוהה יש לקיים הדרכה כזו לפחות אחת לשנתיים. הדרכות אלו יבוצעו באמצעות חומרי הדרכה סדורים. יש לשמור את תיעוד החומרים שהועברו וכן את התיעוד לביצוע ההדרכות.
- בנוסף, בהתאם לנדרש בתקנות אבטחת מידע (תקנה 7), על הגופים לערוך הליך מיון (בדיקת התאמה) עבור עובדים חדשים או בעלי הרשאת גישה אחרים למאגר המידע, על מנת לברר שאין חשש כי בעל ההרשאה אינו מתאים לקבלת גישה למידע המצוי במאגרים. זאת, בהתאם לרגישות המידע הנכלל במאגר, ולהיקף ההרשאה שצפוי להינתן.

## העברת מידע בין גופים ציבוריים

**ממצאים:**



**המלצות**:

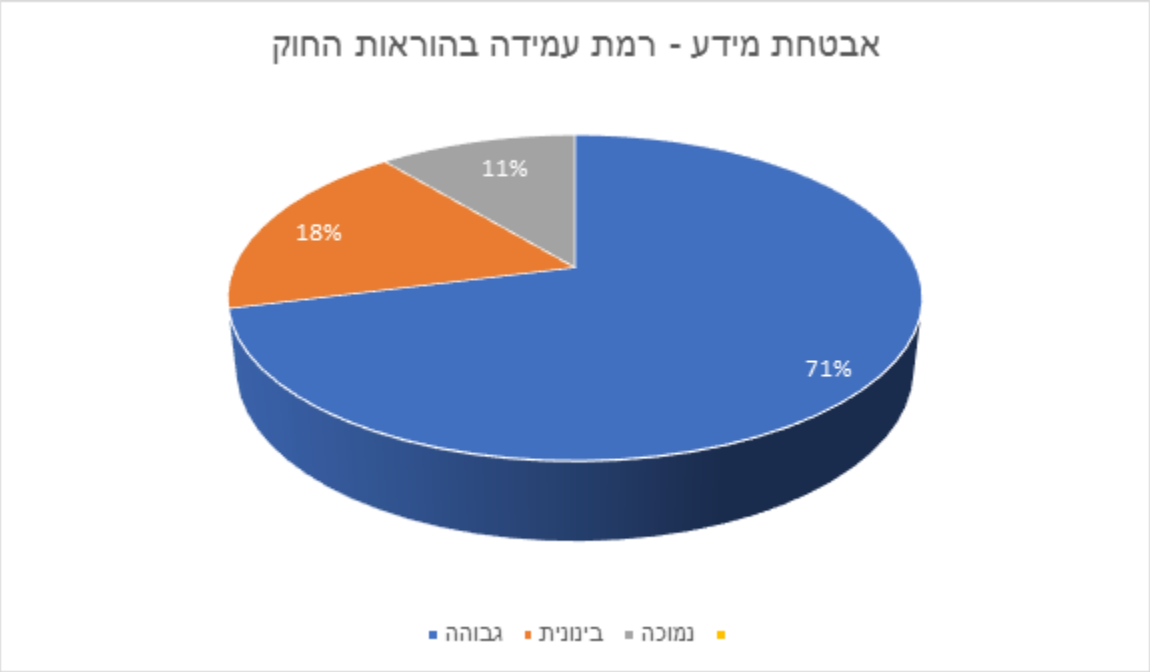
נוכח הפערים שנמצאו בקריטריון זה, נמצא כי על הגופים המפוקחים לחזק את תחום העברת מידע בין גופים ציבוריים בהיבטים הבאים:

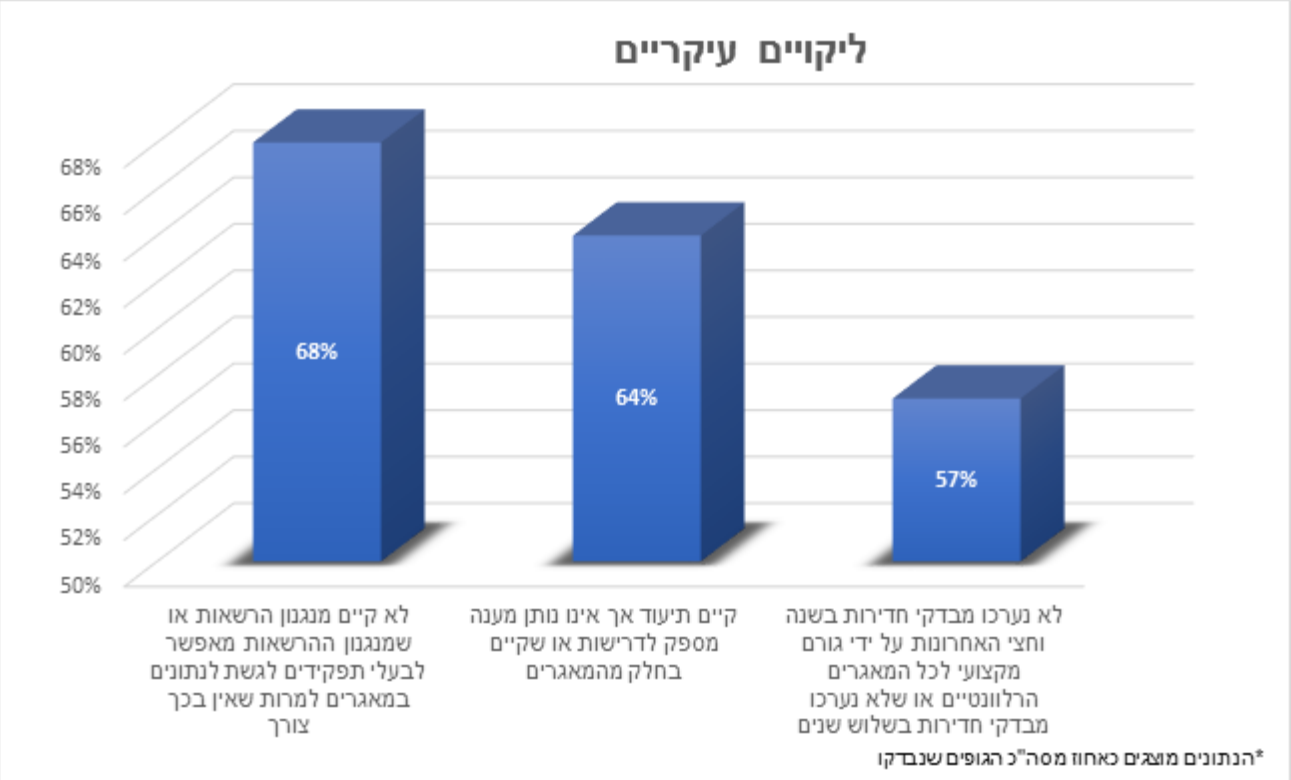
הגופים נדרשים לוודא כי הוקמה ועדה להעברת מידע בין גופים ציבוריים והיא מתכנסת לצורך דיון בבקשות להעברת מידע מידי הגוף הציבורי או לקבלת מידע על-ידו (בהתאם להוראות פרק ד' לחוק, ובהתאם ל–הוראות הקבועות בתקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו-1986).

כמו-כן, גוף ציבורי המוסר מידע בהתאם לסעיף 23ג יקיים רישום של המידע שנמסר. בנוסף, גוף ציבורי המקבל דרך קבע מידע בהתאם לסעיף 23, והמידע נאגר במאגר מידע, יודיע על כך לרשם ועובדה זו תיכלל בפרטי רשימת מאגרי המידע לפי סעיף 12.

## אבטחת מידע

**ממצאים:**



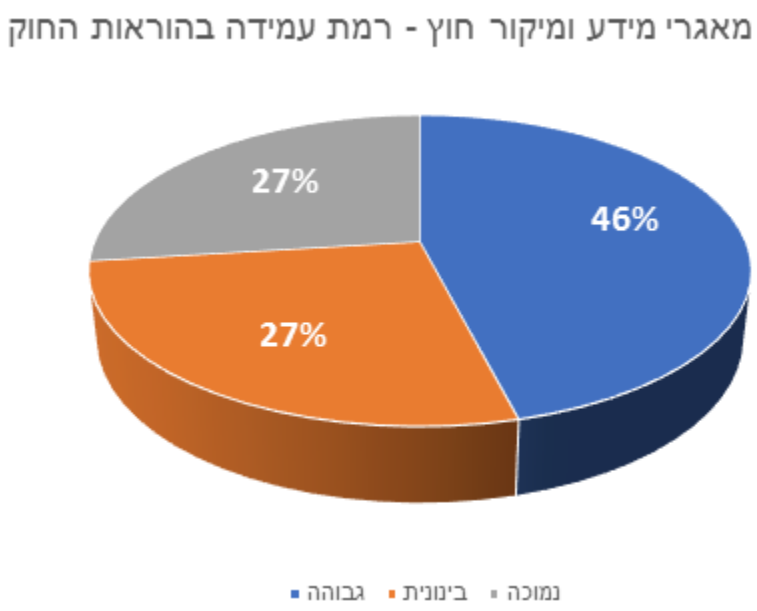
**המלצות:**

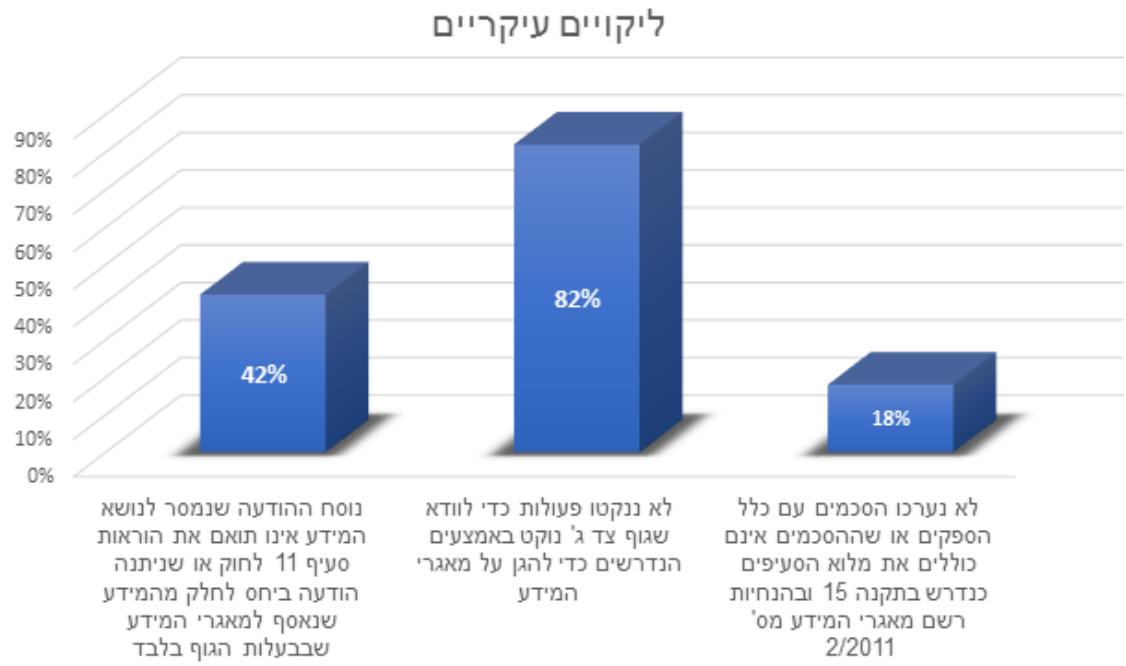
- על הגופים לבצע בחינה עצמית לצורך סיווג רמת אבטחת המידע של מאגרי המידע שבבעלותם בהתאם לקבוע בתוספת השנייה לתקנות אבטחת מידע. בעניין זה, על הגופים לבדוק את סוגי המידע האישי שהם אוספים, ואת המטרות והשימושים שנעשים במידע. יודגש, כי עמדת הרשות היא כי רמת אבטחת המידע הנדרשת של מאגרי המידע לא משתנה, גם אם מאגרי המידע מנוהלים או מעובדים בצורה מפוצלת על גבי מספר מערכות טכנולוגיות שונות בעלות מספר בעלי הרשאה שונה, שכן הבחינה לצורך סיווג רמת האבטחה היא מהותית, ואינה תלויה בהיבטים הטכניים של אופן ניהול המידע. בהתאם לכך, מספר בעלי ההרשאה לצורך קביעת רמת האבטחה של המאגר הוא 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 האבטחה 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 מידע שחלה עליו רמת האבטחה הבינונית או הגבוהה נעשה שימוש באמצעי פיזי הנתון לשליטתו הבלעדית של המורשה, בהתאם לתקנה 9(ב)(1) לתקנות.
- על הגופים 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 האבטחה כנדרש בתקנה 9(ב)(2) 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.
- במאגרים בעלי רמת אבטחה בינונית ומעלה, יש לפעול להטמעת תהליכי גיבוי ללוג אבטחת מידע, ולקביעת נהלים וביצוע גיבויים ללוג נתוני האבטחה במאגר, באופן שיבטיח כי ניתן יהיה לשחזר את הנתונים האמורים למצבם המקורי, כנדרש בתקנה 17 ותקנה 18 לתקנות. בהתאם לתקנה 2(ג) לתקנות אבטחת מידע, על הגופים לערוך, לפחות אחת לשנה, בחינה האם קיים במאגר מידע עודף, קרי – מידע רב מן הנדרש למטרות המאגר, ולתעד בחינה זו.

## 3.1. 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. יש לציין את 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 והתקנות, כנדרש בתקנה 15 ובהנחיית רשם מאגרי המידע מס' 2/2011.

## 4. מסקנות/ תמונת מצב

להלן התובנות המרכזיות בנוגע ליעד פיקוח הרוחב:

- מגזר בתי החולים אוסף מידע הנוגע למצבם הרפואי של המטופלים בהם, וכן נתונים הנוגעים לצוות רפואי המועסק בבתי החולים. בהתחשב ברגישותו הרבה של המידע, ישנו משקל רב לעובדה שבתחום אבטחת מידע כ-29% מן הגופים מצויים ברמת עמידה בינונית ונמוכה, ונדרשת הגברת המודעות להפעלת המנגנונים שנבנו במסגרת הבקרה הארגונית באופן מלא ויעיל על מנת שיבטיחו עמידה מלאה בדרישות אבטחת המידע.

- בתחום העמידה בתקנות אבטחת מידע נמצאו במצטבר סוגי ליקויים רבים במגזר, בנושאים בעלי חשיבות רבה לאבטחת מידע. בחלק מן הגופים נמצאו ליקויים כגון היעדר מדיניות סיסמאות חזקה, אי קיום מבדקי חדירות וסקרי סיכונים בתדירות הנדרשת, תיעוד גישה חלקי ועוד. כאמור, במגזר בעל שימוש נרחב באיסוף מידע, אנו מצפים להקפדה יתירה על אבטחת המידע ושמירה על פרטיות המטופלים, וכן גם על פרטיות הצוות הרפואי.

- בתחום ניהול מאגרי מידע כשליש מן הגופים מצויים, כאמור, ברמת עמידה נמוכה בלבד. הגורם המרכזי בתחום זה הינו עמידה חלקית בדרישות התקנות והנחיות הרשם בהתקשרות עם צד ג' לצורך עיבוד או ניהול מידע.

## 5. מעקב תיקון ליקויים - שיפור ותיקון ליקויים בעקבות הליך הפיקוח

במהלך שנת 2022, נערך מעקב תיקון ליקויים במגזר בתי חולים, 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, בין היתר תוך שקלול מספר הליקויים, סוג הליקוי והמסמכים אותם נדרשו הגופים להציג לרשות, על מנת לוודא את יישום דרישות הרשות לתיקון הליקויים. בעת פיקוח המעקב בחנה הרשות את אופן התקדמות תיקון הליקויים אצל הגופים ואת העמידה בלוחות הזמנים שהוגדרו ליישום התוכנית ולתיקון יתרת הליקויים שטרם תוקנו.

במסגרת ביקורת המעקב שנעשתה בקרב 43% מבתי חולים שקיבלו הנחיות לתיקון ליקויים, נמצא כי הגופים שיפרו את העמידה בתקנות הגנת הפרטיות באופן משמעותי וכי 57% מהליקויים יושמו וטופלו.

## 6. סיכום

כפי שעולה מהדוח, מאופי פעילותו של מגזר בתי החולים, מחזיקים בתי החולים בכמות גדולה של מידע אישי רגיש במיוחד על אודות מצבם הבריאותי של המטופלים בהם, וכן כמוסדות גדולים מחזיקים בתי החולים מידע אישי רב על עובדיהם – הצוותים הרפואיים והמנהליים במוסדות. נוכחנו כי מידת הטמעת התקנות, בראיה מגזרית, הייתה באופן כללי משביעת רצון.

עם זאת יצוין, כי למרות שחלק גדול מבתי החולים קיבלו ציון גבוה בתחום תקנות אבטחת המידע, עדיין נמצאו אצל חלק גדול מהם, ליקוים מהותיים בתחומים של אבטחת מידע, בהקשר של היעדר מערכי הרשאות מסודרים לעובדים, מנגנוני תיעוד אירועי אבטחת מידע (שיש בהם כדי להשפיע על מוכנות הארגון לאירוע אבטחת מידע) ואי-ביצוע מסודר של מבדקי חדירות. בהקשר למבדקי החדירות – חלק מבתי החולים, לא יזמו בעצמם מבדקי חדירות.

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 מודעותם לחובתם לעמוד 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 בתי חולים בישראל, על ידי בחינת גופים נוספים ואחרים במגזר זה, במועד שייקבע לאחר פרסום הדו"ח המגזרי.