משרד המשפטים
MINISTRY OF JUSTICE | وزارة العدل
הרשות להגנת הפרטיות
THE PRIVACY PROTECTION AUTHORITY
سلطة حماية الخصوصية

דו"ח פיקוח רוחב

ממצאי הליך פיקוח הרוחב בקרב מגזר מרפאות בריאות הנפש בישראל



טבת תשפ"א
דצמבר 2020

תוכן עניינים

1. תקציר מנהלים 3
1.1. מגזר מרפאות בריאות הנפש 3
1.2. תהליך העבודה 4
1.3. ליקויים, מסקנות והמלצות עיקריות 4
2. מרפאות בריאות הנפש - תמונת מצב 6
2.1. כללי 6
2.2. רקע על המגזר 6
2.3. תהליך העבודה 6
2.4. הקריטריונים הנבדקים ואופן חישוב רמת העמידה בהוראות חוק הגנת הפרטיות והתקנות מכוחו 7
3. ממצאים – ליקויים מרכזיים 8
3.1. בקרה ארגונית וממשל תאגידי 8
3.2. ניהול מאגרי מידע 9
3.3. העברת מידע בין גופים ציבוריים 9
3.4. אבטחת המידע 10
3.5. עיבוד מידע אישי במיקור חוץ 10
4. מסקנות/תמונת מצב והמלצות 11
4.1. בקרה ארגונית וממשל תאגידי 11
4.2. ניהול מאגרי מידע 11
4.3. העברת מידע בין גופים ציבוריים 12
4.4. אבטחת מידע 12
4.5. עיבוד מידע אישי במיקור חוץ 13
5. סיכום 13
נספח א' - ליקויים מרכזיים שנמצאו במגזר והתיקון הנדרש בגינם 15

1. תקציר מנהלים

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

1.1. מגזר מרפאות בריאות הנפש

מגזר מרפאות בריאות הנפש בישראל כולל יחידות אשר מעניקות שירותים של טיפולים נפשיים בבתי חולים כלליים, בתי חולים לבריאות הנפש ומרכזים ייעודיים לבריאות הנפש.

מגזר זה מאופיין ככזה המנהל מידע רפואי רגיש מאוד על מצבם הנפשי של המטופלים ובהיקפים רבים, וביחס מיוחד בין הגופים המטפלים לבין המטופלים אשר לעיתים, במקרים דוגמת אשפוז כפוי, לא יכולים בשל מצבם הרפואי להעניק את הסכמתם למסירת מידע רגיש כהגדרתו בחוק, אודות מצבם הבריאותי והנפשי או שמידע מסוג זה אודותיהם נאסף תוך כדי הטיפול בהם.

מאפייניו של מגזר זה עלולים להביאו להוות יעד תקיפה אטרקטיבי לאירועי אבטחת מידע, בין אם בידי בעלי הרשאה ובין עם על ידי פצחנים (האקרים) העלולים לבצע שימוש לרעה במידע ואף להשתמש במידע זה כאמצעי סחיטה. דוגמה לאירוע כזה התרחש לאחרונה בפינלנד, כאשר האקרים פרצו למחשבים של רשת מרפאות פסיכיאטריות "וסטאמו", המעניקה שירותים למערכת הבריאות הפינית כספקית משנה, הורידו לרשת האפלה עשרות אלפי רשומות אודות מטופלים לרבות רשומות רפואיות ופרטי מטפלים, והשתמשו במידע זה לדרישת כופר מהמטופלים בסך של בין 200 ל-500 אירו במטבעות ביטקוין ומהמרכז הרפואי כופר בסך 450,000 אירו במטבעות ביטקוין. נכון למועד זה, משטרת פינלנד דיווחה כי קיבלה כ-25 אלף דיווחים אודות הפריצה, ולשכת החקירות הממשלתית פתחה בחקירת האירוע אשר קיבל עדיפות לאומית ונדון בסדר היום של הממשלה.

הגופים שנבדקו במגזר זה כוללים, בין היתר, מרפאות בבתי חולים המתמחים במתן טיפול נפשי למטופלים, יחידות אשר מעניקות שירותים של טיפולים נפשיים בבתי חולים כלליים ומרכזים ייעודיים לבריאות הנפש. אופן הניהול ואחזקת המידע אודות מצבם הבריאותי של המטופלים משתנה ומתבצע באופן שונה בין הגופים, כגון ניהול המידע באופן ישיר, ניהול המידע באמצעות מיקור חוץ או ניהול המידע באופן ישיר. כמו כן, מדובר בגופים המחזיקים בהיקפי מידע גדולים ורמת רגישות גבוהה.

לאור כל אלה הרשות להגנת הפרטיות הגדירה מגזר זה כיעד פיקוח רוחב משמעותי.

1.2. תהליך העבודה

כחלק מפעילות הליך פיקוח הרוחב פנתה הרשות בדרישה למילוי שאלוני ביקורת ל-30 גופים המנהלים מרפאות לבריאות הנפש. הליך הפיקוח התמקד ב- 18 גופים זאת מאחר וחלק מהגופים העבירו מענה מרוכז אחד בשל פעילות מאוחדת ו/או ניהול משותף של מאגר מידע או עקב קיומה של תשתית טכנולוגית משותפת

שאלוני הביקורת בחנו חמישה קריטריונים עיקריים בתחום הגנת הפרטיות: בקרה ארגונית וממשל תאגידי, ניהול מאגרי מידע, העברת מידע בין גופים ציבוריים, אבטחת מידע ושימוש בשירותי מיקור חוץ. הציונים ניתנו לגופים בהתאם למענה ולמסמכים שסופקו על ידם ואשר נבחנו על ידי הרשות, בהתאם לרמת עמידתם בהוראות חוק הגנת הפרטיות והתקנות מכוחו.

1.3. ליקויים, מסקנות והמלצות עיקריות

במגזר המרפאות לבריאות הנפש נמצאה רמת עמידה בינונית-גבוהה בהוראות החוק. עם זאת, הליקוי העיקרי בו נמצאה רמת עמידה נמוכה תחת קטגוריית "עיבוד מידע אישי ומיקור חוץ", מעלה את החשש מדליפת מידע דרך מתן גישה למידע לגופים שלישיים (ספקי מיקור החוץ או עובדי קופ"ח בעלי נגישות שוטפת למידע רפואי במאגרי המידע של המרפאות).

מצד אחד, מרבית הגופים שנבדקו במסגרת פיקוח הרוחב עושים שימוש בשירותי המחשוב של המוסד הרפואי אליו הם משויכים ולמעשה מהווים חלק אירגוני של אותו מוסד, מה שמאפשר להם לעמוד בדרישות החוק ברמה גבוהה יותר. מאידך, במרפאות שמקבלות שירותי מחשוב במיקור חוץ, נמצא כי רמת העמידה בהוראות החוק בקשר להפעלתו של ספק מיקור החוץ נמוכה (בהיבטים של אי עמידה מספקת בכל הנוגע להסכמים, היבטי אבטחת מידע, דיווח שנתי על אירועים וכד' מול הספקים).

בנוסף, נמצאה רמת עמידה נמוכה בכל הנוגע לקבלת הרשאת המטופלים לאיסוף ושמירת מידע רפואי שלהם במאגר, ולא נשמר תיעוד כלשהו לגבי קבלת הסכמה ויידוע המטופלים במקרים בהם מתאפשרת הסכמה, בדבר זכויותיהם לפי החוק בנושא מאגר המידע הרפואי בו נשמרים פרטיהם.

כמו כן, נמצאה רמת עמידה בינונית בנושא ניהול מאגרי המידע, אשר מצביעה על חוסר בידע ובטיפול מוסדי בנושאי זכויות המטופלים בקשר למידע הנאגר עליהם במרפאות בריאות הנפש.

לאור הממצאים שעלו מהליך פיקוח הרוחב, הועברו ל-18 הגופים שנבדקו הנחיות ספציפיות לתיקון הליקויים שנמצאו אצלם. לאור בחינת כשלי המגזר, דו"ח זה כולל ריכוז של ההנחיות העיקריות לתיקון הליקויים שנשלחו לגופים.

משרד המשפטים
MINISTRY OF JUSTICE | وزارة العدل
הרשות להגנת הפרטיות
THE PRIVACY PROTECTION AUTHORITY
سلطة حماية الخصوصية

דו"ח פיקוח רוחב

ממצאי הליך פיקוח הרוחב בקרב מגזר מרפאות בריאות הנפש

אתגרים ומאפיינים ייחודיים של מגזר מרפאות בריאות הנפש

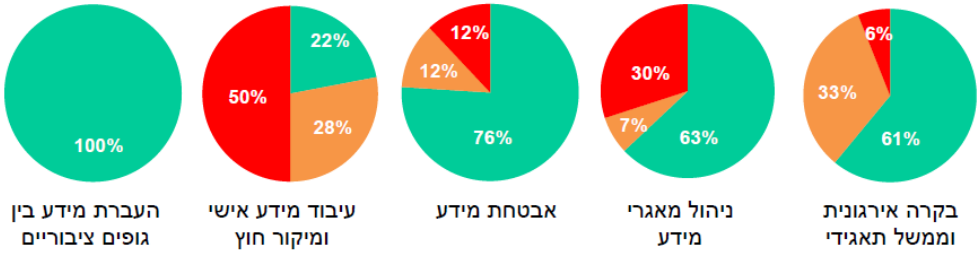
יחסים ייחודיים בין הגוף המטפל למטופלים.

ניהול מידע רגיש הכולל מידע דמוגרפי, רפואי, גנטי ומידע על מצב נפשי.

ניהול ואחזקת מידע באופן ישיר ובאמצעות מיקור חוץ בהיקפי מידע גדולים וברמת רגישות גבוהה.

התהליך שבוצע במספרים







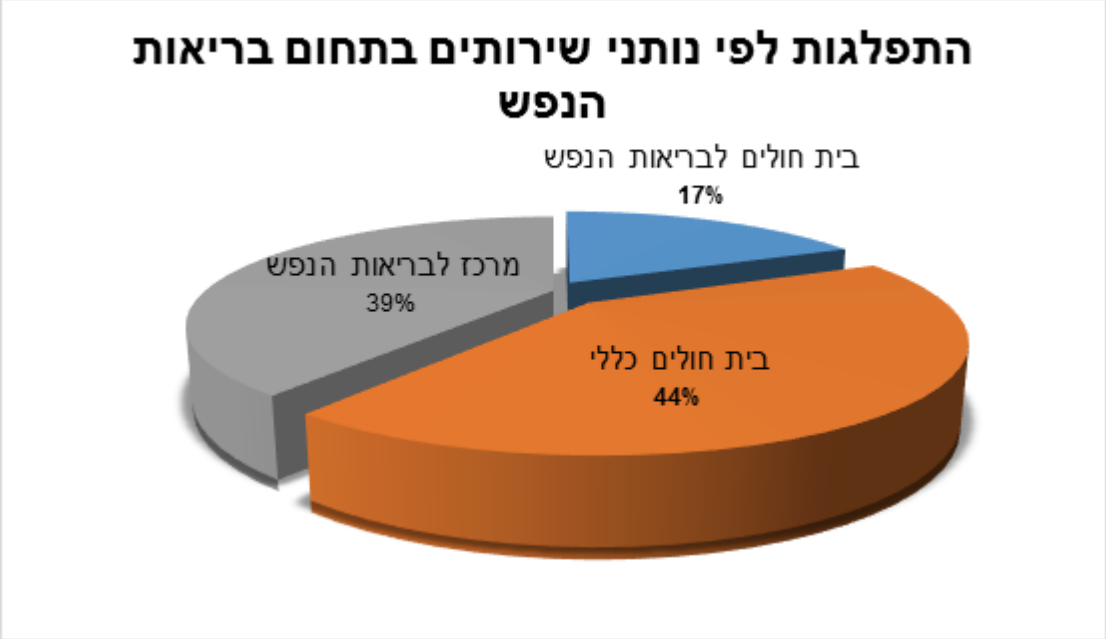
2. מרפאות בריאות הנפש - תמונת מצב

2.1. כללי

הדו"ח מתייחס לפיקוחי הרוחב שביצעה הרשות להגנת הפרטיות בתקופה שבין החודשים יולי 2018 לאוגוסט 2019 במגזר מרפאות לבריאות הנפש.

2.2. רקע על המגזר

במסגרת סקר הבוחן את סיכוני הפרטיות במגזרים השונים, נמצא מגזר מרפאות בריאות הנפש, הכולל יחידות המעניקות שירותי טיפול נפשי בבתי חולים כלליים, בתי חולים לבריאות הנפש ומרכזים ייעודיים לבריאות הנפש, כיעד פיקוח רוחב משמעותי וזאת בשל מספר מאפיינים ייחודיים למגזר. מרפאות לבריאות הנפש מחזיקות במידע רגיש אודות מטופלים אשר לעיתים כלל אינם נותנים את הסכמתם למסירת המידע (כגון במקרה של אשפוז כפוי). סוג המידע במגזר זה כולל, בין היתר, מידע דמוגרפי, רפואי, גנטי ומידע על מצב נפשי. מספרם הרב של האנשים עליהם מוחזק המידע, דורש הקפדה יתרה על אבטחת המידע, קיום חובת השקיפות וחובות נוספות המבטיחות את קיום הוראות החוק והתקנות בהיבטים של ניהול והחזקת מידע רגיש כאמור.



2.3. תהליך העבודה

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. התכנית נבנית בהתחשב בקריטריונים הבאים: כמות והיקף המידע במגזר, רמת רגישות המידע, מידע שהצטבר ברשות בנוגע למגזר או נושא מסוים, תלונות ספציפיות שהתקבלו ברשות והצורך בבחינה

מגזרית והבאת הגופים המשתייכים למגזר לרמת עמידה התואמת את דרישות החוק והתקנות.

הרשות פנתה במסגרת פיקוח הרוחב ל-30 גופים המנהלים מרפאות לבריאות הנפש, כאשר בניכוי גופים אשר סיימו פעילותם, שינו את תחום הפעילות או דיווחו על פעילות שאינה רלוונטית למגזר הנבדק, הופצו לבסוף 21 שאלוני ביקורת. לאחר שחלק מהגופים השיבו באופן מאוחד בשל פעילות או תשתית טכנולוגית משותפת, התמקד הליך הפיקוח ב-18 גופים אשר נבדקו במסגרת הפיקוח במגזר זה. מתוך 18 הגופים 4 נדרשו לספק לרשות מידע נוסף לרבות מסמכים והבהרות נוספות. גוף אחד מאותם הגופים נדרש לספק ידיעות ומסמכים באמצעות פיקוח במשרדי הגופים המפוקחים. בסיום ההליך נמצאו אצל כל 18 הגופים המפוקחים, ליקויים הדורשים תיקון. בהתאם לכך, הפיצה הרשות לאותם גופים מכתבי הנחייה שכללו דרישה לתקן את הליקויים שנמצאו ולספק תכנית מפורטת לתיקונם בליווי הצהרת נושא משרה לביצוע והשלמת התיקונים, כאשר כחלק מההליך תבדוק הרשות באמצעות ביקורת חוזרת את השלמת התיקונים בגופים נבחרים.

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

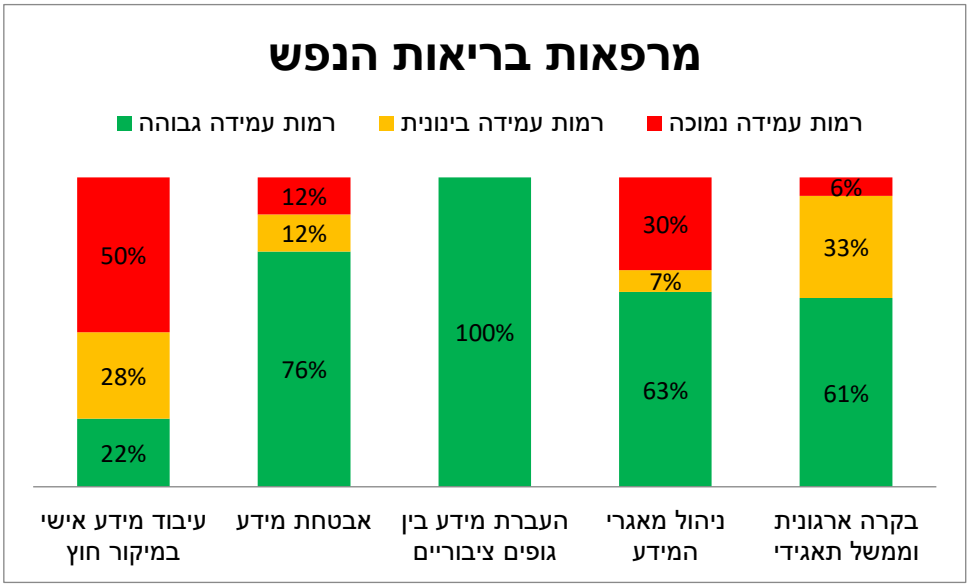
במטרה לבחון את רמת העמידה המגזרית בהוראות החוק והתקנות, פנתה הרשות כאמור בדרישה למילוי שאלוני ביקורת המתייחסים לקריטריונים שונים ובהם:

- **בקרה ארגונית וממשל תאגידי** - קריטריון זה בוחן קיומה של תכנית שנתית בתחום אבטחת המידע והגנת הפרטיות ואת מינויים של גורמים בעלי אחריות בתחום;
- **ניהול מאגרי מידע** - קריטריון זה בוחן את אופן קבלת ההסכמה לשימוש במידע אישי, רמת התאמת השימוש במידע למטרה שלשמה נאסף, מתן זכות העיון במידע, ועמידה בהוראות החוק בעניין דיוור ישיר;
- **אבטחת מידע** - בחינת עמידת הגופים בהוראות תקנות הגנת הפרטיות (אבטחת מידע), בהתייחס לניהול המידע האישי שבבעלותם ובהחזקתם;
- **שירותי מיקור חוץ** - בחינת ההתקשרויות של בעלי מאגרי המידע עם צדדים שלישיים המחזיקים במידע ומעבדים אותו, והאופן בו הם מבטיחים הגנה על המידע.
- **העברת מידע אישי בין גופים ציבוריים** - בחינת קיומן של ועדות הבוחנות את הצורך במידע במרפאות המשתייכות לגופים ציבוריים, אי העברת מידע עודף והסמכות להעברה וקבלת מידע מגופים ציבוריים ואליהם.

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 במסגרת ההליך:

- 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



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

3.1. בקרה ארגונית וממשל תאגידי

- במסגרת בחינת קריטריון זה, נמצא כי 61% מהגופים עמדו ברמה גבוהה בהוראות החוק בנוגע לבקרה ארגונית וממשל תאגידי.
- עמידה גבוהה זו מיוחסת בחלקה לכפיפות הגופים המפוקחים לבתי חולים כלליים או בתי חולים לבריאות הנפש, אשר משמעותה כי גופים אלה מקבלים את שירותי המחשוב מבתי החולים ואינם מנהלים את מערכות המידע ומאגרי המידע בעצמם. בתי החולים כפופים לרגולציה של גופים רגולטוריים אחרים בכל הנוגע למערכות מחשב והגנת מידע רפואי, וזו מסדירה את העמידה בהוראות הנוגעות לממשל התאגידי, אבטחת המידע והשמירה על פרטיות המידע.

- עם זאת, בגופים בהם נמצאה רמת עמידה בינונית (33%), וביתר שאת בגופים בהם נמצאה רמת עמידה נמוכה (6%), נמצאו פערים אשר נבעו בין היתר מאופן ההתנהלות של מערך המחשוב של בית החולים לו כפופה המרפאה.
- בהיבט זה, נמצאו ליקויים בנושא ביצוע בדיקת התאמה לעובדים חדשים בעלי גישה למאגר אשר נועדה לוודא שאין חשש כי בעל ההרשאה אינו מתאים לקבלת גישה למידע המצוי במאגר.
- נמצאו גופים בהם תפקידים ותחומי אחריות היו מרוכזים אצל גורם יחיד באופן אשר עלול להעמידו בחשש לניגוד עניינים, בניגוד לדרישות תקנות הגנת הפרטיות (אבטחת מידע).
- חלק מהגופים לא מינו מנהל מאגר או שכתב המינוי לא תאם את דרישות רשם מאגרי המידע.
- נמצאו גופים אשר לא צרפו תיעוד לנהלי אבטחת מידע ולתכנית עבודה שנתית או שהנהלים היו חלקיים בלבד, וכן נמצאו גופים בהם לא הייתה הקפדה על תכנית עבודה שנתית סדורה.

3.2. ניהול מאגרי מידע

- במסגרת בחינת קריטריון זה, נמצא כי 63% מהגופים עמדו ברמה גבוהה בהוראות החוק בנוגע לניהול מאגרי מידע, בעוד שב-37% מהגופים המפוקחים נמצאו ליקויים באופן יישום הוראות החוק והתקנות.
- כן נמצא כי הגופים אינם מקפידים על שקיפות בדבר מקור הסמכות לאיסוף המידע האישי ויידוע האנשים עליהם מוחזק המידע בדבר זכויותיהם בנוגע למאגר המידע הרפואי בו נשמרים פרטיהם, בהתאם לסעיף 11 לחוק, בכל פניה לקבלת מידע.
- עוד נמצא כי חלק מגופים אלו אינם שומרים או מתעדים את אופן קבלת הסכמת נושאי המידע למסירת מידע ויידועם בדבר הזכויות המוקנות להם מכוח החוק.
- נמצאו גופים אשר לא אפשרו לנושאי המידע לשנות או לתקן את המידע המוחזק אודותיהם כנדרש בחוק.[1]

3.3. העברת מידע בין גופים ציבוריים

- בקריטריון זה נמצאה רמת עמידה גבוהה,[2] כאשר עיקר הפערים שנמצאו ושלא באו לידי ביטוי בציון המשוקלל בקטגוריה זו, נבעו מחוסר בהירות של הגופים המעבירים מידע בנוגע לחובתם בהקמת ועדה להעברת מידע בין גופים ציבוריים.
- עמידה גבוהה זו מיוחסת בחלקה לדרישות המוטלות על גופים הפועלים במגזר זה כחלק ממערכת החובות המוטלות על ידי משרד הבריאות והרגולציה הפרטנית הנוגעת למתן שירותים רפואיים.

[1] ההתייחסות לסעיף זה מתייחסת רק לעמידה בס' 13 לחוק, ללא התייחסות לחובות ודרישות אחרות בנוגע לתיקון מידע לפי חוק טיפול בחולי נפש, התשנ"א-1981 או חקיקה אחרת.
[2] לרבות חוזר מינהל מידע ומחשוב בנושא "הוועדה של משרד הבריאות להעברת מידע בין גופים ציבוריים".

- העמידה בדרישות אלו הייתה גבוהה בקרב גופים המוגדרים כגופים ציבוריים, בכל הנוגע לאופן העברות המידע כנדרש בחוק, אך כאמור, העמידה בהיבטי הממשל הארגוני ובאופן ניהול מאגרי המידע ואבטחת המידע, הייתה נמוכה לרבות ביחס לאופן ההתקשרות של גופים אלו עם גורמי מיקור חוץ לצורכי עיבוד ואחסון המידע.

3.4. אבטחת המידע

- בקריטריון זה נמצאה רמת עמידה גבוהה של 76% מהגופים, בעוד שב-24% מהגופים, נמצאו רמות עמידה בינונית ונמוכה.
- בין היתר, נמצאו ליקויים בניהול הרשאות הגישה למאגרים, בין אם בהעדר תהליכים נאותים לניהול ההרשאות ובין אם בהעדר יישום הפרדת תפקידים ויישום מתן ההרשאה לפי עקרון הצורך לדעת בלבד (בעל הרשאה המורשה לכך בלבד, לפי רשימת ההרשאות התקפות).
- אותרו גופים, בהם פרקי הזמן לשמירת תיעוד אוטומטי המאפשרים ביקורת על הגישה למערכות המאגר היו קצרים מפרקי הזמן הנדרשים.
- בנוסף, נמצאו גופים אשר לא נקטו באמצעים מספקים בכדי למנוע חדירה למיקום הפיזי בו נשמרים השרתים והתשתיות המחזיקים את מאגרי המידע או המאפשרים גישה אליהם. כן נמצאו גופים אשר בכניסה לאתריהם לא נעשה שימוש באמצעי פיזי הנתון לשליטתו הבלעדית של המורשה אלא בשם משתמש וסיסמה בלבד.
- עבור גופים מסוימים כלל לא מתבצע ניתוק אוטומטי של המערכת לאחר פרק זמן של אי-פעילות.
- כמו כן, קיימים גופים אשר לא הקפידו על ביצוע מבחני חדירה/סקרי סיכונים בתדירות הנדרשת ע"פ התקנות.
- בקרב גופים רבים אף לא גובש נוהל עבודה סדור לטיפול באירועי אבטחת מידע.

3.5. עיבוד מידע אישי במיקור חוץ

- **הליקוי המרכזי שנמצא במגזר זה** מתייחס לקריטריון עיבוד מידע אישי במיקור חוץ בו 50% מהגופים נמצאו ברמת עמידה נמוכה, ו-28% ברמת עמידה בינונית.
- ניכר כי גם במקרים בהם הגופים שנבדקו הטמיעו מנגנוני בקרה נאותים בארגון עצמו, קיים עדיין ליקוי ביישום הדרישות מחברות צד ג' המעניקות שירותי עיבוד מידע אישי במיקור חוץ. ליקוי זה מתבטא בכך שחלק מהגופים לא נקטו צעדים מספקים מבעוד מועד על מנת להעריך את מידת הסיכון הנשקפת למידע ולפגיעה אגב כך בזכותם לפרטיות של נושאי המידע, הנובעת משימוש במיקור חוץ.
- מהממצאים עולה כי מחצית מהגופים אינם מבצעים התקשרות עם ספקי מיקור חוץ בהתאם לדרישות הקבועות בתקנות, לא בוחנים את איכות ניהול אבטחת המידע ואת אופן תפעול מאגרי המידע אצל ספקי מיקור החוץ ולא מבצעים פעולות פיקוח כנדרש.

4. מסקנות/תמונת מצב והמלצות

מממצאי הליך פיקוח הרוחב עולה כי הגם שמרבית הגופים במגזר מרפאות בריאות הנפש הינם בעלי היכרות עם דרישות החוק והתקנות, והטמיעו או מצויים בשלבי הטמעה של עיקרי הדרישות, **עדיין נמצאו ליקויים משמעותיים באופן יישום הוראות החוק והתקנות, והנחיית הרשות היא כי על הגופים המשתייכים למגזר זה ליישם את הנקודות הבאות**:

4.1. בקרה ארגונית וממשל תאגידי

נוכח הליקויים שנמצאו בקריטריון זה, וכחלק ממכלול התיקונים הנדרשים בכדי לעמוד בהוראות החוק והתקנות, נדרשים הגופים, בין היתר, לוודא את רישום כלל מאגרי המידע שבבעלותם בהתאם להוראות החוק, וקיום 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 כתב מינוי רשמי למנהל המאגר ולממונה אבטחת המידע היכן שנדרש למנות כזה, וכן לוודא שכתבי המינוי כוללים את כל הפרטים הנדרשים בהתאם לסעיף 7 לחוק ולתקנה 4 לתקנות אבטחת מידע.

כמו כן, 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, יש לעדכן את נוהל אבטחת המידע ולבחון את עדכניותו אחת לשנה, כנדרש בתקנות אבטחת מידע (תקנה 4).

כמו כן, על הגופים להכין תכנית עבודה לנושא אבטחת מידע והגנת הפרטיות לרבות התייחסות לנושא גורם אחראי ולו"ז לביצוע, שתעמוד בדרישות תקנות אבטחת מידע (תקנה 3 (3)). ככל שמדובר בגוף החייב במבדקי חדירות, עליו לוודא כי אכן נעשו כאלה העומדים בדרישות תקנות אבטחת מידע (תקנה 16).

בנוסף, בהתאם לנדרש בתקנות אבטחת מידע (תקנה 7), על הגופים לערוך הליך מיון (בדיקת התאמה) עבור עובדים חדשים או כל גורם אחר שמקבל גישה למאגר/מערכת הכוללת מספר מאגרים.

4.2. ניהול מאגרי מידע

מכוח החובה המוטלת על פי החוק על הגופים המנהלים רשימות מטופלים הכוללות אפיון של נושאי המידע לרבות מידע עליהם, כהגדרתו בחוק, נדרשים אלה לבצע מיפוי לכל מאגרי המידע הקיימים אצלם, ועל בסיס מיפוי זה לרשום מאגרי מידע שאינם רשומים, או לעדכן את מאגרי המידע הקיימים בפנקס מאגרי המידע.

על הגופים לקבל את הסכמת נושא המידע כנדרש בחוק עבור שמירת פרטיו במערכת הארגון, תוך מתן הודעה בעת איסוף המידע, הכוללת התייחסות לשאלה האם חלה חובה

חוקית למסור את המידע, או שמסירת המידע תלויה ברצונו ובהסכמתו, וכן ציון המטרה אשר לשמה מבוקש המידע, למי יימסר המידע ומטרות המסירה.

בנוסף, על הגופים להקפיד לאפשר לנושאי המידע לעיין במידע על אודותיהם, המוחזק במאגר מידע בהתאם לסעיף 13 לחוק. לעניין זה, יודגש כי זכות העיון חלה גם כאשר מדובר במידע כגון שיחות טלפוניות מוקלטות, תכתובות צ'ט, שיחות המצולמות בווידאו וכיו"ב, אשר נשמרות באופן דיגיטלי על ידי בתי עסק או גוף אחר הנותן שירות לציבור.[3] כמו כן, יש להקפיד ליידע ולאפשר לנושאי המידע לתקן או לשנות את המידע אודותיהם המוחזק במאגר מידע בהתאם לסעיף 14 לחוק.

4.3. העברת מידע בין גופים ציבוריים

על הגופים לקבוע מדיניות ולהגדיר הנחיות ספציפיות לתחום העברת המידע הרפואי בין מרפאות בריאות הנפש לבין גופים אחרים, ולבצע פעולות פיקוח ובקרה בגופים עצמם בכל הנוגע לשימוש במידע הרפואי המוזן אצלם. מוצע כי נהלי משרד הבריאות בנושא זה ייבחנו ויעודכנו מעת לעת.

על הגופים הפועלים במגזר זה, לבצע בחינה עצמית בנוגע לתחולת פרק ד' לחוק, ולבחון האם הם מוגדרים כגופים ציבוריים בהתאם לחוק או לצו הגנת הפרטיות (קביעת גופים ציבוריים), התשמ"ו-1986, וככל שכן, לפעול בהתאם לקבוע בפרק ד' לחוק ובתקנות הרלוונטיות.[4]

4.4. אבטחת מידע

נוכח הליקויים בנושא ניהול ההרשאות, על הגופים לוודא בניית מנגנוני הרשאות במאגרי המידע של הארגון בהתאם לתקנות 8 ו -9 (א) לתקנות אבטחת מידע, אשר יבטיחו הפרדת סמכויות ויאפשרו גישה לנתוני המאגר אך ורק במידה הנדרשת לביצוע התפקיד של העובדים בעלי הגישה למידע.

בנוסף, על הגופים לנקוט באמצעים מספקים בכדי למנוע חדירה למיקום הפיזי בו נשמרים השרתים והתשתיות המחזיקים או המאפשרים גישה אל מאגרי המידע. כמו כן, עליהם לוודא שבכניסה לאתר מאגר המידע נעשה שימוש באמצעי פיזי הנתון לשליטתו הבלעדית של המורשה על פי תקנות אבטחת מידע (תקנה 9(ב)(2)).

במאגרים בעלי רמת אבטחה גבוהה, יש לבצע מבדקי חדירה אחת ל- 18 חודשים, בהתאם לתקנה 5 (ד) לתקנות אבטחת מידע.

---

[3] לקריאה נוספת ראו הנחיית רשם מאגרי המידע 1/2017 - תחולת הוראות חוק הגנת הפרטיות על זכות העיון בהקלטות קול, וידאו ומידע דיגיטלי נוסף - https://www.gov.il/BlobFolder/policy/right_of_access/he/video.pdf

[4] תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), התשמ"ו–1986.

יש לוודא כי תיעוד של אירועי אבטחת מידע יישמר ויגובש נוהל עבודה סדור בנושא, בהתאם לתקנה 11 לתקנות אבטחת מידע.

כמו כן, על הגופים לוודא כי פרק הזמן לשמירת תיעוד שמאפשר ביקורת על הגישה למערכות המאגר הינו לפחות 24 חודשים כנדרש בתקנה 10 לתקנות אבטחת מידע.

בנוסף, על הגופים לוודא כי מתבצע ניתוק אוטומטי לאחר פרק זמן של אי-פעילות על פי תקנות הגנת הפרטיות (תקנה 9(ב)(2)).

4.5. עיבוד מידע אישי במיקור חוץ

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 בעלי המאגר לוודא עריכת הסכם מול כל גורם חיצוני שמחזיק במאגר, בו ייקבעו במפורש כל הוראות תקנה 15(א)(2) לתקנות אבטחת מידע, 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.

עוד דורשות התקנות מן הגופים לנקוט אמצעי בקרה ופיקוח נאותים על עמידת הגורם החיצוני בהוראות ההסכם והתקנות. הוראות דומות לעניין החובות המוטלות על בעל מאגר המסתייע במיקור חוץ של עיבוד מידע, מפורטות בהנחיית רשם מאגרי המידע מס' 2/2011 "שימוש בשירותי מיקור חוץ (Outsourcing) לעיבוד מידע אישי"[5] ובאופן ספציפי לעניין מידע רפואי בהנחיית רשם מאגרי המידע מס' 1/2009 "תחולת החובות מכוח החוק במאגרי מידע רפואי שבשימוש קופות חולים ונותני שירותים רפואיים".[6]

5. סיכום

כאמור, מגזר מרפאות לבריאות הנפש מעלה סיכונים לא מעטים לפרטיות המטופלים, אשר נובעים מניהול מידע רב, מזוהה ורגיש, וניהול קשר בדיוור ישיר עם ציבור המטופלים באמצעות הגופים ובאמצעות מיקור חוץ. כל אלה דורשים הקפדה יתרה על קיום הוראות תקנות אבטחת מידע, שקיפות מול המטופל, ומילוי החובות החלות מכח פרק הדיוור הישיר ושירותי הדיוור הישיר בחוק הגנת הפרטיות.

ממסקנות פיקוח הרוחב ניתן לומר כי מגזר מרפאות בריאות הנפש אינו אחיד ונחלק לשתי קבוצות עיקריות - קבוצה אחת כוללת מרפאות עצמאיות וקטנות והקבוצה השנייה כוללת מרפאות המסונפות לבתי החולים הציבוריים וכפופות לניהולם. במסגרת הליך פיקוח

[5] לקריאה נוספת ר' הנחיית רשם מאגרי המידע 2/2011 – שימוש בשירותי מיקור חוץ (outsourcing) לעיבוד מידע אישי - לקריאה נוספת
[6] לקריאה נוספת ר' הנחיית רשם מאגרי מידע מס' 1/2009 תחולת החובות מכוח החוק במאגרי מידע רפואי שבשימוש קופות חולים ונותני שירותים רפואיים - לקריאה נוספת

הרוחב נמצא כי בקבוצה השנייה קיימת היכרות רבה יותר של הוראות הרגולציה השונות ומודעות להטמעת ויישום הוראות החוק והתקנות מאשר בקבוצה הראשונה, וזאת בין היתר עקב ציות קפדני יותר לחוזרי ונהלי משרד הבריאות (כגון נהלי אבטחת מידע וחוזרי משרד הבריאות) וכן עקב אימוץ תקן אבטחת מידע רלוונטי (תקן אבטחת מידע רפואי ISO 27799).

ממצאי הליך פיקוח הרוחב במגזר מרפאות לבריאות הנפש העלה ממצאים מדאיגים המצביעים על ליקויים בעיקר בנוגע לעמידה בהוראות החוק בתחום עיבוד המידע האישי באמצעות מיקור חוץ, היעדר ועדה להעברת מידע בין גופים ציבוריים על אף שבפועל מועבר מידע, עמידה חלקית בהוראות החוק בכל הנוגע למינויים של ממונה אבטחת מידע ופערים ברמת האבטחה הקיימת ביחס לניהול הרשאות גישה למאגרי המידע. בנוסף, נמצא כי חלק מהגופים המשתייכים למגזר זה אינם מקפידים דיים ליידע את ציבור המטופלים בדבר זכויותיהם על פי חוק הגנת הפרטיות, הכוללות בין היתר את החובה להציג את מקור המידע ואת הזכות לעיין במידע.

ניכר, כי עצם קיום הליך פיקוח הרוחב עורר אצל הגופים שנבדקו תהליך בחינה עצמית והנעה לשיפור עצמי באופן הציות לחוק ולתקנות, כאשר בסיום ההליך כאמור, הגופים שבהתנהלותם נתגלו ליקויים, נדרשו להציג לרשות התחייבות נושא משרה ותכנית מסודרת לתיקונם.

הרשות להגנת הפרטיות תמשיך לפעול לאכיפת מדיניותה בקרב בעלים ומחזיקים במאגרי מידע אישי 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 זכות הציבור 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 מרפאות בריאות הנפש, על ידי בחינת גופים נוספים ואחרים במגזר זה, במועד שייקבע לאחר פרסום הדו"ח המגזרי.

נספח א' - ליקויים מרכזיים שנמצאו במגזר והתיקון הנדרש בגינם

הליקוי/פער	פעילות מתקנת נדרשת	הפניה לחוק/תקנה/הנחיה	נושא
בקרה ארגונית וממשל תאגידי	בקרה ארגונית וממשל תאגידי	בקרה ארגונית וממשל תאגידי	בקרה ארגונית וממשל תאגידי
לא בוצעה ביקורת אבטחת מידע.	עריכת ביקורות בנושא אבטחת מידע/הגנת הפרטיות מידי 24 חודשים במאגר ברמת אבטחה בינונית ומעלה, לחילופין במאגר ברמת אבטחה גבוהה - עריכת סקר סיכונים מידי 18 חודשים הכולל את דרישות הביקורת.	ביקורות תקופתיות תקנות הגנת הפרטיות (אבטחת מידע), תשע"ז-2017, תקנה 16	**ביקורות תקופתיות**
עובדים חדשים לא עוברים הליך מיון/בדיקת התאמה.	הטמעת תהליך מיון של עובדים חדשים שבוחן היבטים הרלבנטיים לפרטיות ולאבטחת מידע.	אבטחת מידע בניהול כוח אדם –קליטת עובדים תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 7	**מיון עובדים חדשים**
בגוף המחויב במינוי ממונה אבטחת מידע על פי החוק, לא מונה ממונה אבטחת מידע.	בגופים הנדרשים במינוי ממונה אבטחת מידע 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.	פרטי הממונה על אבטחת המידע חוק הגנת פרטיות, תשמ"א-1981 סעיף 17ב. תקנות הגנת פרטיות (אבטחת מידע) תשע"ז-2017, תקנה 3	**מינוי ממונה אבטחת מידע**
לא מונה מנהל מאגר.	יש למנות מנהל למאגר המידע. ולעדכן את רשם מאגרי המידע בהתאם.	פרטי מנהל המאגר	**מינוי מנהל מאגר**
לא מונה מנהל מאגר.	יש למנות מנהל למאגר המידע. ולעדכן את רשם מאגרי המידע בהתאם.	חוק הגנת פרטיות, תשמ"א-1981 סעיף 7, הגדרות	**מינוי מנהל מאגר**
נוהל אבטחת המידע שנקבע, אינו מכסה את כלל הסעיפים המנויים בתקנות	קביעת נוהל אבטחת מידע ובו מענה לכל הנושאים המנויים בתקנה 4, בהתאם לרמת האבטחה הנדרשת במאגר.	נוהל אבטחת מידע תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 4	**נהלי אבטחת מידע**
לא קיימים נהלי אבטחת מידע.	כתיבת נהלי אבטחת מידע אשר יכללו את כל הנושאים המפורטים בתקנה 4.	נוהל אבטחת מידע	**נהלי אבטחת מידע**
לא קיימים נהלי אבטחת מידע.	כתיבת נהלי אבטחת מידע אשר יכללו את כל הנושאים המפורטים בתקנה 4.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 4 (ה)	**נהלי אבטחת מידע**
לא הוגדר בנוהל אבטחת מידע הצורך לבחינת עדכניותו אחת לשנה.	בחינת הצורך בעדכון מדיניות אבטחת המידע ועדכנה בהתאם.	נוהל אבטחת מידע. תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 4	**נהלי אבטחת מידע**

לא קיימת תכנית עבודה שנתית לבקרה שוטפת בנושא אבטחת מידע.	בניית תכנית עבודה שנתית לבקרה שוטפת בנושא אבטחת מידע והגנת הפרטיות המפרטת את הגורם האחראי ואבני דרך ברורות.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 3 (3)	**תכנית עבודה**
תכנית העבודה השנתית לבקרה שוטפת בנושא אבטחת מידע אינה מפורטת מספיק ואיננה כוללת את כל הרכיבים הנדרשים מתוכנית עבודה	עדכון תכנית עבודה שנתית לבקרה שוטפת בנושא אבטחת מידע כך שתכסה בצורה טובה את נושאי אבטחת מידע והגנה על הפרטיות ותפרט את הגורם האחראי ואבני דרך ברורות.	תכנית עבודה שנתית לבקרה שוטפת	**תכנית עבודה**
תכנית העבודה השנתית לבקרה שוטפת בנושא אבטחת מידע אינה מפורטת מספיק ואיננה כוללת את כל הרכיבים הנדרשים מתוכנית עבודה	עדכון תכנית עבודה שנתית לבקרה שוטפת בנושא אבטחת מידע כך שתכסה בצורה טובה את נושאי אבטחת מידע והגנה על הפרטיות ותפרט את הגורם האחראי ואבני דרך ברורות.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז 2017, תקנה 3 (3)	**תכנית עבודה**
ניהול מאגרי מידע	**ניהול מאגרי מידע**	**ניהול מאגרי מידע**	**ניהול מאגרי מידע**
לא נמסרת למטופלים הודעה המפרטת לשם מה מבוקש המידע, למי יימסר המידע ומטרות המסירה.	מתן הודעה לנושא המידע בעת איסוף המידע, נוסח ההודעה לכלול את כל המוגדר בסעיף 11 לחוק, ובכלל זה התייחסות לשאלה האם חלה על אותו אדם חובה חוקית למסור את המידע, או שמסירת המידע תלויה ברצונו ובהסכמתו; המטרה אשר לשמה מבוקש המידע; ולמי יימסר המידע ומטרות המסירה.	חובת מבקש המידע	**מקור סמכות לאיסוף המידע**
לא נמסרת למטופלים הודעה המפרטת לשם מה מבוקש המידע, למי יימסר המידע ומטרות המסירה.	מתן הודעה לנושא המידע בעת איסוף המידע, נוסח ההודעה לכלול את כל המוגדר בסעיף 11 לחוק, ובכלל זה התייחסות לשאלה האם חלה על אותו אדם חובה חוקית למסור את המידע, או שמסירת המידע תלויה ברצונו ובהסכמתו; המטרה אשר לשמה מבוקש המידע; ולמי יימסר המידע ומטרות המסירה.	חוק הגנת הפרטיות, תשמ"א-1981 - סעיף 11	**מקור סמכות לאיסוף המידע**
אין התאמה בין המאגרים המנוהלים לבין רישומם בפנקס המאגרים.	יש לפעול להסדרת רישום מאגרי המידע בפנקס המאגרים.	חוק הגנת הפרטיות תשמ"א – 1981, סעיף 8	**רישום המאגר אצל רשם**
העברת מידע בין גופים ציבוריים	**העברת מידע בין גופים ציבוריים**	**העברת מידע בין גופים ציבוריים**	**העברת מידע בין גופים ציבוריים**

לא הוקמה וועדה להעברת מידע בין גופים ציבוריים.	יש להקים ועדה לנושא העברת מידע בין גופים ציבוריים כנדרש בתקנות. המנהל הכללי או סגנו יהיה יושב ראש הוועדה בין חברי הוועדה יהיו לכל הפחות היועץ המשפטי או נציגו וממונה אבטחת המידע. כנדרש בתקנות.	חוק הגנת הפרטיות תשמ"א – 1981, פרק ד'	**וועדה להעברת מידע בין גופים ציבוריים**
לא הוקמה וועדה להעברת מידע בין גופים ציבוריים.	יש להקים ועדה לנושא העברת מידע בין גופים ציבוריים כנדרש בתקנות. המנהל הכללי או סגנו יהיה יושב ראש הוועדה בין חברי הוועדה יהיו לכל הפחות היועץ המשפטי או נציגו וממונה אבטחת המידע. כנדרש בתקנות.	נוהל ביצוע העברת מידע - תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים, תשמ"ו - 1986 - פרק ג'	**וועדה להעברת מידע בין גופים ציבוריים**
העברות מידע בין גופים ציבוריים לא בוצעו בהתאם לנהלי ביצוע העברת מידע בין גופים ציבוריים	יש לוודא כי פעילות הוועדה להעברת מידע בין גופים ציבוריים תואמת לחוק ולתקנות	חוק הגנת הפרטיות תשמ"א – 1981, פרק ד'	**וועדה להעברת מידע בין גופים ציבוריים**
העברות מידע בין גופים ציבוריים לא בוצעו בהתאם לנהלי ביצוע העברת מידע בין גופים ציבוריים	יש לוודא כי פעילות הוועדה להעברת מידע בין גופים ציבוריים תואמת לחוק ולתקנות	תקנות הגנת הפרטיות (תנאי החזקת מידע ושמירתו וסדרי העברת מידע בין גופים ציבוריים), תשמ"ו - 1986 - פרק ג'	**וועדה להעברת מידע בין גופים ציבוריים**
אבטחת מידע	**אבטחת מידע**	**אבטחת מידע**	**אבטחת מידע**
לא קיימת אבטחה פיזית וסביבתית למערכות.	יש להבטיח כי המערכות 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 ושל כל הכנסה והוצאה אל מערכות המאגר ומהן.	תקנות הגנת פרטיות (אבטחת מידע) תשע"ז-2017,תקנה 6	**אבטחה פיזית**
לא קיימים אמצעי הגנה מספקים אשר נותנים מענה לחדירה לא מורשית במאגרי המידע מחוברים לרשת האינטרנט או לרשת ציבורית אחרת, בהתאם לדרישה בתקנות.	יש לוודא 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.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 14 (א)	**אבטחת תקשורת**

התיעוד האוטומטי שמאפשר ביקורת על הגישה למאגר מטופלים נשמר לזמן קצר יותר מהדרוש בתקנות.	יש לנהל מנגנון תיעוד אוטומטי שיאפשר ביקורת על הגישה למאגרי מידע אשר יכלול את הנתונים הבאים: זהות המשתמש, התאריך והשעה של הניסיון הגישה, רכיב המערכת שאליו בוצע ניסיון הגישה, סוג הגישה, היקפה, ואם הגישה אושרה או נדחתה.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 10	**בקרה ותיעוד גישה**
התיעוד האוטומטי שמאפשר ביקורת על הגישה למאגר מטופלים נשמר לזמן קצר יותר מהדרוש בתקנות.	נתוני התיעוד של המנגנון יישמרו למשך 24 חודשים לפחות	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 10	**בקרה ותיעוד גישה**
בכניסה מרחוק למאגר ברמה הבינונית והגבוהה על ידי עובד הארגון לא נעשה שימוש באמצעי פיזי הנתון לשליטתו המלאה של המורשה.	אופן הזיהוי בעת הכניסה מרחוק למאגר על ידי עובד הארגון, יעשה באמצעות אמצעי פיזי הנתון לשליטתו המלאה של המורשה.	אבטחת תקשורת	**גישה מרחוק**
בכניסה מרחוק למאגר ברמה הבינונית והגבוהה על ידי עובד הארגון לא נעשה שימוש באמצעי פיזי הנתון לשליטתו המלאה של המורשה.	אופן הזיהוי בעת הכניסה מרחוק למאגר על ידי עובד הארגון, יעשה באמצעות אמצעי פיזי הנתון לשליטתו המלאה של המורשה.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 14 (ג).	**גישה מרחוק**
בכניסה מרחוק למאגר ברמה הבינונית והגבוהה על ידי עובד הארגון לא נעשה שימוש באמצעי פיזי הנתון לשליטתו המלאה של המורשה.	אופן הזיהוי בעת הכניסה מרחוק למאגר על ידי עובד הארגון, יעשה באמצעות אמצעי פיזי הנתון לשליטתו המלאה של המורשה.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 9 (ב)(2).	**גישה מרחוק**
לא קיימת הפרדה בין סביבת הנתונים של המאגר לבין יתר הנתונים של הארגון.	יש לקיים הפרדה בין מערכות המאגר אשר ניתן לגשת מהן למידע, לבין מערכות מחשוב אחרות המשמשות את בעל המאגר בהתאם לתקנות.	ניהול מאובטח ומעודכן של מערכות המאגר	**הפרדה בין מאגרים**
לא קיימת הפרדה בין סביבת הנתונים של המאגר לבין יתר הנתונים של הארגון.	יש לקיים הפרדה בין מערכות המאגר אשר ניתן לגשת מהן למידע, לבין מערכות מחשוב אחרות המשמשות את בעל המאגר בהתאם לתקנות.	תקנות הגנת פרטיות (אבטחת מידע) תשע"ז-2017, תקנה 13 (ב)	**הפרדה בין מאגרים**

לא בוצעו מבחני חדירה בגוף המנהל מאגרים בעלי סיווג רמת אבטחה גבוהה.	במאגר מידע שחלה עליו רמת האבטחה הגבוהה יש לבצע מבדקי חדירה מידי אחת לשנה וחצי, בחינת הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה בעקבותיהן, ותיקון הליקויים שהתגלו במסגרת המבדקים.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 5(ד).	**מבדקי חדירה**
במערכת לא מוטמעת מדיניות סיסמאות או לא קיימת מדיניות סיסמאות חזקה.	במאגרים בעלי רמת אבטחה בינונית ומעלה, קביעה בנוהל האבטחה את אופן הגישה למערכות מאגרי המידע באמצעות שימוש במדיניות סיסמאות חזקה הכוללת בין היתר: סיסמאות מורכבות, החלפות תקופתיות של הסיסמה וכד'	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 9 (ב-2)	**מדיניות סיסמאות**
לא קיים תהליך לביטול הרשאות לבעל הרשאה שסיים את תפקידו או מנגנון לעדכון הרשאות לבעל הרשאה שעבר לתפקיד חדש, או שאינו מתקיים בסמוך לשינוי סטטוס העובד.	אפיון ויישום תהליך בו מיד בעת סיום תפקיד או עזיבת עובד הארגון, הרשאותיו של העובד יבוטלו או יעודכנו בהתאם לצורך.	תקנות הגנת פרטיות (אבטחת מידע) תשע"ז 2017, תקנה 8, תקנה 9 (א)	**ניהול הרשאות**
אי ביצוע ניתוק אוטומטי לאחר פרק זמן או ביצוע ניתוק אוטומטי לאחר פרק זמן לא סביר של אי פעילות.	ברמת אבטחה בינונית ומעלה, נדרשת הגדרת ניתוק אוטומטי במערכות מאגרי המידע לאחר פרק זמן סביר של אי פעילות במערכת	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 9 (ב-2)	**ניתוק אוטומטי**
לא בוצע סקר סיכוני מערכות מידע.	במאגר מידע שחלה עליו רמת האבטחה הגבוהה יש לבצע סקר סיכונים מידי אחת לשנה וחצי, בחינה את הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה בעקבותיהן, ותיקון הליקויים שהתגלו במסגרת הסקר.	סקר סיכונים	**סקר סיכונים**
לא בוצע סקר סיכוני מערכות מידע.	במאגר מידע שחלה עליו רמת האבטחה הגבוהה יש לבצע סקר סיכונים מידי אחת לשנה וחצי, בחינה את הצורך בעדכון מסמך הגדרות המאגר או נוהל האבטחה בעקבותיהן, ותיקון הליקויים שהתגלו במסגרת הסקר.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 5(ג)	**סקר סיכונים**
לא קיים הליך סדור לתיעוד וקביעת הוראות התמודדות עם אירועי אבטחת מידע	יש לתעד כל אירוע המעלה חשש לאירוע אבטחה, בנוסף נוהל העבודה יכלול התייחסות לפעולות הנדרשות לביצוע, מנגנוני הדיווח, אופן הדיווח והליך הפקת לקחים במקרה של אירוע אבטחה מידע.	תיעוד של אירועי אבטחה	**תיעוד אירועי אבטחה**

לא קיים הליך סדור לתיעוד וקביעת הוראות התמודדות עם אירועי אבטחת מידע	במאגר מידע ברמת אבטחה גבוהה יש לקיים דיון רבעוני (וברמה בינונית אחת לשנה) באירועי האבטחה ולבחון את הצורך בעדכון הנוהל.	תקנות הגנת פרטיות (אבטחת מידע) תשע"ז-2017, תקנה 11	**תיעוד אירועי אבטחה**
מיקור חוץ	**מיקור חוץ**	**מיקור חוץ**	**מיקור חוץ**
אי בחינה וקביעה בהסכם מול גורם חיצוני הנותן שירותי עיבוד מידע אישי בחברה, כי הוא פועל בהתאם לתקנה 15 ולהנחיות רשם מאגרי המידע מס' 2/2011.	ביצוע בחינה וכלל הפעולות הנדרשות בהתאם לתקנה 15 הנחיות רשם מאגרי המידע מס' 2/2011 עבור כל גורם חיצוני אשר נותן שירותי עיבוד מידע אישי בחברה, לרבות נקיטת אמצעי בקרה ופיקוח נאותים על עמידת הגורם החיצוני בהוראות ההסכם והתקנות.	מיקור חוץ	**מיקור חוץ**
אי בחינה וקביעה בהסכם מול גורם חיצוני הנותן שירותי עיבוד מידע אישי בחברה, כי הוא פועל בהתאם לתקנה 15 ולהנחיות רשם מאגרי המידע מס' 2/2011.	ביצוע בחינה וכלל הפעולות הנדרשות בהתאם לתקנה 15 הנחיות רשם מאגרי המידע מס' 2/2011 עבור כל גורם חיצוני אשר נותן שירותי עיבוד מידע אישי בחברה, לרבות נקיטת אמצעי בקרה ופיקוח נאותים על עמידת הגורם החיצוני בהוראות ההסכם והתקנות.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 15.	**מיקור חוץ**
אי בחינה וקביעה בהסכם מול גורם חיצוני הנותן שירותי עיבוד מידע אישי בחברה, כי הוא פועל בהתאם לתקנה 15 ולהנחיות רשם מאגרי המידע מס' 2/2011.	ביצוע בחינה וכלל הפעולות הנדרשות בהתאם לתקנה 15 הנחיות רשם מאגרי המידע מס' 2/2011 עבור כל גורם חיצוני אשר נותן שירותי עיבוד מידע אישי בחברה, לרבות נקיטת אמצעי בקרה ופיקוח נאותים על עמידת הגורם החיצוני בהוראות ההסכם והתקנות.	הנחיית רשם מאגרי מידע מס' 2/2011 - שימוש בשירותי מיקור חוץ (Outsourcing) לעיבוד מידע אישי.	**מיקור חוץ**
ההסכם המתייחס לאופן עיבוד המידע האישי במיקור חוץ אינו כולל את כל הנושאים המנויים בתקנות	יש לפעול לעיגון במסמך ההתקשרות התייחסות לחובותיו ואחריותו של הספק, בהתאם להוראות התקנות, לרבות:	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 15.	**מיקור חוץ**
ההסכם המתייחס לאופן עיבוד המידע האישי במיקור חוץ אינו כולל את כל הנושאים המנויים בתקנות	1. דיווח אודות אירועי אבטחת מידע.	הנחיית רשם מאגרי מידע מס' 2/2011 - שימוש בשירותי מיקור חוץ (Outsourcing) לעיבוד מידע אישי.	**מיקור חוץ**

ההסכם המתייחס לאופן עיבוד המידע האישי במיקור חוץ אינו כולל את כל הנושאים המנויים בתקנות	2. מנגנוני אבטחת המידע הנדרשים.		**מיקור חוץ**
ההסכם המתייחס לאופן עיבוד המידע האישי במיקור חוץ אינו כולל את כל הנושאים המנויים בתקנות	3. שמירת המידע לאחר סיום תקופת ההתקשרות.		**מיקור חוץ**
ההסכם המתייחס לאופן עיבוד המידע האישי במיקור חוץ אינו כולל את כל הנושאים המנויים בתקנות	4. חובות צד ג' בהעברת מידע לאחר.		**מיקור חוץ**
אי נקיטת פעולות בכדי לוודא שהגוף החיצוני נוקט בהוראות ההסכם ובהוראות התקנות המפרטות את האמצעים הנדרשים להגנת המידע	ווידוא כי כל גוף חיצוני אשר נותן שרותי מיקור חוץ בתחום מאגרי המידע נוקט באמצעים הנדרשים בהוראות ההסכם עמו ובהוראות תקנה 15, תוך נקיטה באמצעי בקרה ופיקוח.	תקנות הגנת הפרטיות (אבטחת מידע) תשע"ז-2017, תקנה 15.	**מיקור חוץ**
אי נקיטת פעולות בכדי לוודא שהגוף החיצוני נוקט בהוראות ההסכם ובהוראות התקנות המפרטות את האמצעים הנדרשים להגנת המידע	ווידוא כי כל גוף חיצוני אשר נותן שרותי מיקור חוץ בתחום מאגרי המידע נוקט באמצעים הנדרשים בהוראות ההסכם עמו ובהוראות תקנה 15, תוך נקיטה באמצעי בקרה ופיקוח.	הנחיית רשם מאגרי מידע מס' 2/2011 - שימוש בשירותי מיקור חוץ (Outsourcing) לעיבוד מידע אישי.	**מיקור חוץ**