ClinicAI

עודכן: אוקטובר 2026

צ'קליסט תיקון 13 למסגרות טיפוליות

מה לבדוק במסגרת שמחזיקה מידע רפואי ונפשי על מטופלים: בית מאזן, מרכז גמילה, הוסטל או מרפאה.

הכין: דויד סיני, ClinicAI

מידע רפואי ונפשי הוא "מידע בעל רגישות מיוחדת". לכן חלות על מסגרות טיפוליות רוב החובות שבתקנות אבטחת המידע, ותיקון 13 (בתוקף מאוגוסט 2025) מאפשר לרשות להגנת הפרטיות להטיל עליהן עיצומים כספיים.

מיפוי וחובות בסיס

- [ ] **רמת האבטחה של המאגר נקבעה ותועדה** — תקנה 1 ותוספות
  מאגר עם מידע רפואי או נפשי הוא ברמה בינונית. מעל 100 בעלי הרשאה או מידע על 100,000 איש ומעלה: רמה גבוהה. עד 10 בעלי הרשאה: רמה בסיסית.

- [ ] **נבדקה חובת רישום או הודעה לרשות** — סעיף 8א
  מסגרת פרטית בדרך כלל כבר לא חייבת ברישום. גוף ציבורי חייב. מאגר עם מידע רגיש על יותר מ-100,000 איש: הודעה לרשות תוך 30 יום.

- [ ] **נבדקה חובת מינוי ממונים** — סעיף 17ב, תקנה 3
  ממונה הגנת פרטיות (DPO) חובה למי שעיסוקו העיקרי כולל עיבוד מידע רגיש בהיקף ניכר, ואין סף מספרי. ממונה אבטחת מידע: בדקו את סעיף 17ב. ממונה שמונה כפוף ישירות להנהלה.

- [ ] **יש מסמך הגדרות מאגר ונוהל אבטחה כתובים** — תקנות 2, 4
  מה נאסף ולמה, מי מעבד, אילו סיכונים ואיך מטפלים בהם. בודקים ומעדכנים פעם בשנה.

גישה ואבטחה

- [ ] **הרשאות לפי תפקיד, ורשימת הרשאות מעודכנת** — תקנות 8, 9(ג)
  כל תפקיד רואה רק את מה שנדרש לו. עובד שסיים: ההרשאה מבוטלת מיד.

- [ ] **הזדהות חזקה וניתוק אוטומטי** — תקנות 9, 14(ג)
  ברמה בינונית ומעלה: הזדהות ככל האפשר באמצעי פיזי שרק לעובד יש שליטה עליו, וחובה בגישה מרחוק. סיסמאות מוחלפות לפחות כל שישה חודשים.

- [ ] **יומן גישה אוטומטי שנשמר 24 חודשים** — תקנה 10
  מי נכנס, מתי, לאיזה רכיב ואם הגישה אושרה. נבדק באופן שגרתי, והעובדים יודעים שהוא קיים.

- [ ] **הצפנה בהעברה ובהתקנים ניידים** — תקנות 12, 14
  מידע שעובר באינטרנט מוצפן. חיבור התקנים ניידים מוגבל, ומידע שמועתק אליהם מוצפן.

- [ ] **נתוני האבטחה נשמרים ומגובים** — תקנות 17, 18
  יומנים, הרשאות ותיעוד אירועים נשמרים 24 חודשים ומגובים, עם נוהל שחזור כתוב.

אנשים, ספקים ואירועים

- [ ] **יש נוהל לאירוע אבטחה** — תקנה 11
  כל אירוע מתועד. באירוע אבטחה חמור מודיעים לרשות להגנת הפרטיות באופן מיידי ומדווחים על הצעדים שננקטו.

- [ ] **הסכם אבטחה עם כל ספק שיש לו גישה למידע** — תקנה 15
  בדיקת סיכונים לפני ההתקשרות. בהסכם: מה מותר לעבד, אבטחה, סודיות, החזרת המידע ומחיקתו בסיום, ודיווח שנתי.

- [ ] **הדרכת צוות מתועדת** — תקנה 7
  הדרכה לפני קבלת גישה. ברמה בינונית ומעלה: הדרכה חוזרת לפחות פעם בשנתיים.

- [ ] **ביקורת אבטחה תקופתית** — תקנות 5, 16
  ברמה בינונית ומעלה: ביקורת פנימית או חיצונית לפחות פעם ב-24 חודשים. ברמה גבוהה גם סקר סיכונים ומבדק חדירות פעם ב-18 חודשים.

- [ ] **צמצום מידע והודעה למטופל** — תקנה 2(ג), סעיף 11
  פעם בשנה בודקים שלא נשמר מידע רב מהנדרש. טופס הקליטה מסביר למה המידע נאסף, אם חובה למסור אותו ולמי יועבר.

זה לא ייעוץ משפטי. החובות תלויות בגודל המאגר, במספר בעלי ההרשאה ובסוג הגוף. לבדיקת המסגרת שלכם פנו לעורך דין שמתמחה בהגנת פרטיות.

מקורות (נבדקו באוקטובר 2026):

הרשות להגנת הפרטיות, שאלות ותשובות על תיקון 13
gov.il/he/pages/tikun13_qa

הרשות להגנת הפרטיות, טופס דיווח על אירוע אבטחה
mojforms.justice.gov.il/mojaemprivacyprotectionauthority/databreachupdate.html

הרשות להגנת הפרטיות, גילוי דעת סופי על מינוי ממונה, 15.7.2026
gov.il/he/pages/amendment-13-26-07-26

תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז-2017, נבו
nevo.co.il/law_html/law00/144811.htm

הרשות להגנת הפרטיות, שאלות ותשובות על תקנות אבטחת מידע
gov.il/he/pages/data_security_fqa

חוק הגנת הפרטיות, נוסח מאוחד, אתר הכנסת
fs.knesset.gov.il/25/law/25_ls_bk_4326099.pdf