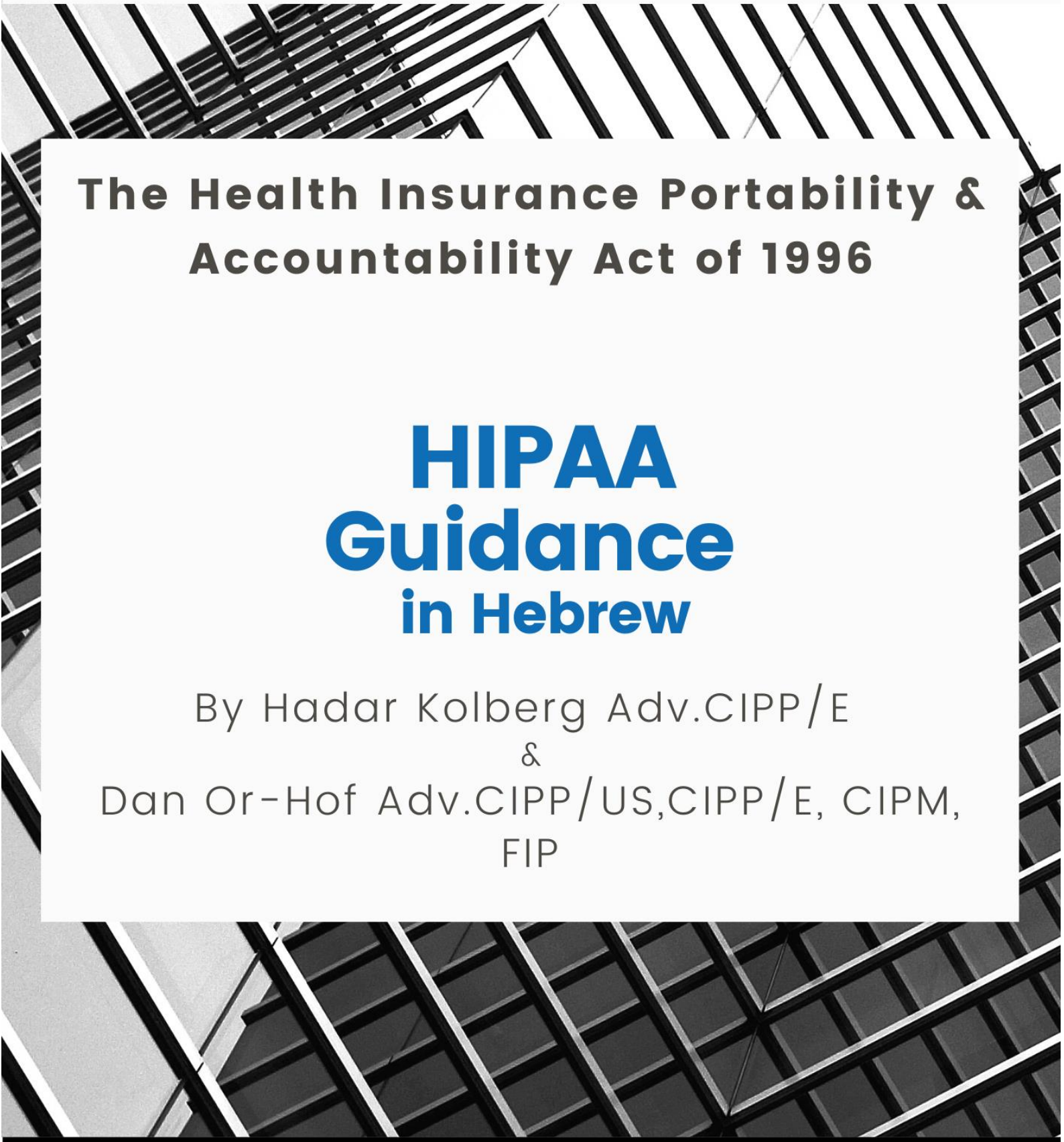
Or-Hof



The Health Insurance Portability & Accountability Act of 1996

HIPAA Guidance in Hebrew

By Hadar Kolberg Adv.CIPP/E
&
Dan Or-Hof Adv.CIPP/US,CIPP/E, CIPM, FIP

We will be happy to be at your service.

Dan Or-Hof

מדריך HIPAA

תוכן עניינים

III.1.6.1.2. ליחידים

III.2.6.1.2. לתקשורת

III.3.6.1.2. למזכירות משרד הבריאות

IV. אישור בכתב של יחידים לשימוש במידע לצרכים שיווקיים

6.1.3. מסמכים והליכים פנים - ארגוניים

I. מסמכי מדיניות ונהלים

II. תיעוד

6.1.4. זכויות יחידים

I. זכות הגישה למידע רפואי מוגן

II. זכות תיקון המידע

III. הזכות לקבלת דיווח אודות גילוי (שיתוף) המידע הרפואי המוגן

IV. הזכות לבקש את הגבלת השימוש במידע רפואי מוגן

V. הזכות לבקש אמצעים חלופיים או מיקום חלופי להתקשרות בנוגע למידע רפואי מוגן

VI. הזכות להסכים או לסרב לשימושים מסוימים במידע רפואי מוגן

VII. הזכות להגיש תלונה

6.1.5. נקיטת פעולות למזעור השפעות אירוע אבטחה העולה כדי פריצה (Breach Mitigation)

6.1.6. חובות אבטחת מידע

6.2. **חובות החלות על שותף עסקי**

6.2.1. עדכון מסכי מדיניות ונהלים

6.2.2. מינוי קצין אבטחת מידע

6.2.3. התקשרות עם ספקי משנה באמצעות הסכם שותף עסקי (BAA)

6.2.4. הודעה בדבר אירוע אבטחה לישות מכוסה או שותף עסקי אחר

6.2.5. חובות אבטחת מידע

6.3. **חובות אבטחת מידע החלות על יישויות מכוסות ושותפים עסקיים**

6.4. **חובות תיעוד החלות על יישויות מכוסות ושותפים עסקיים**

7. סנקציות והשלכות נוספות להפרת החוק

8. סיכום

1. <u>פתיח</u>

The Health Insurance Portability and Accountability Act of 1996 (HIPAA), הינו החוק הפדרלי העיקרי בארה"ב המסדיר את פרטיותו וביטחונו של מידע רפואי מוגן (PHI) ("**החוק**").

הוראות החוק הפכו במשך השנים לסטנדרט פרטיות ואבטחת מידע מקובל ונדרש בשוק, ועל כן חברות שבוחרות לציית לחוק, אף אם אינן מחויבות לעשות כן על פי דין, נהנות מיתרון איכותי ותחרותי משמעותי על פני מתחרותיהן.

מטרת מדריך זה היא לסייע לחברות הנדרשות לציית לחוק, בין אם מתוקף תחולתו על פי דין ובין אם מכוח דרישה מסחרית שמקורה בלקוחות החברה.

המדריך אינו תרגום של החוק ואינו ממצה את כלל הוראותיו, בין היתר, כיוון שהוא מתייחס בעיקרו להוראות מתוך כלל הפרטיות (כפי שמונח זה מבואר בהמשך), שלדעתנו הן המשמעותיות ביותר לחברות הישראליות שבקהל לקוחותינו.

<u>לתשומת הלב</u>: המדריך אינו חוות דעת משפטית ואינו תחליף ליעוץ מקצועי בנוגע לחוק. תפקידו לשמש כמורה נבוכים למושגים ולעקרונות מרכזיים בחוק ולסייע בהבנת יישום הוראותיו.

אנו מקווים שמדריך זה יועיל לכם.

2. מושגי יסוד

2.1. **יישות מכוסה (Covered Entity)** סעיף 160.103

יישות מכוסה הינה יחיד או ארגון המספק שירותים רפואיים (Healthcare Provider), שירותי תשלום עבור שירותים רפואיים או שירותי סליקה לשירותים רפואיים, והמעביר מידע רפואי מוגן באופן אלקטרוני.

ספקי שירותים רפואיים הם גופים המספקים שירות רפואי ומעבירים מידע באופן אלקטרוני בקשר לעסקה שמשרד הבריאות האמריקאי אימץ תקן לגביה. לדוגמה, רופאים, מרפאות, פסיכולוגים, רופאי שיניים, כירופרקטים, בתי אבות ובתי מרקחת.

ספקי שירותי תשלום עבור שירותים רפואיים (Health Plans) הם גופים המנהלים תוכניות בריאות המשתתפות במימון שירותים רפואיים. לדוגמה, חברות ביטוח רפואי, תוכניות בריאות פרטיות מטעם חברות ותוכניות ממשלתיות המסבסדות שירותי בריאות.

ספקי שירותי סליקה לשירותים רפואיים (Healthcare Clearinghouse) הם גורמים המתווכים בין ספקי השירותים הרפואיים לבין ספקי שירותי התשלום. ספקים אלו "מתרגמים" נתונים שהוזנו בצד אחד של התקשורת בין הגורמים הללו, מפורמט שאינו תקני לפורמט תקני, על מנת שהנתונים יוכלו להיקלט במערכות הצד השני.

2.2. **שותף עסקי (Business Associate)** סעיף 160.103

שותף עסקי הינו יחיד או ארגון המבצע פעולה הכרוכה בשימוש במידע רפואי מוגן או בחשיפתו, בשם יישות מכוסה, או יחיד או ארגון המעניק שירות ליישות מכוסה הכרוך בשימוש במידע רפואי מוגן או בחשיפתו.

יישות מכוסה יכולה על פי הגדרות החוק להוות שותף עסקי של יישות מכוסה אחרת.

נבהיר, כי אין הכוונה לעובדים של יישות מכוסה, הפועלים בשמה או כזרועה הארוכה. עובדים של יישות מכוסה אינם שותפים עסקיים שלה.

החוק מפרט מספר חריגים להגדרת שותף עסקי. לדוגמה, אם ישות מכוסה חושפת מידע רפואי מוגן לספק שירותי בריאות למטרות טיפול בלבד, ספק שירותי הבריאות הנחשף למידע לא מהווה שותף עסקי.

כך למשל, אם בית חולים מסתייע בשירותיו של רופא שאיננו עובד בית החולים לצורך טיפול חירום, ולשם כך חושף בית החולים מידע רפואי מוגן לאותו רופא, הרופא שנחשף למידע לא מהווה שותף עסקי לצורך החוק.

חריגים נוספים המפורטים בחוק הינם, לדוגמה, תוכניות בריאות קבוצתיות ונותני החסות שלהן, ארגונים ממשלתיים ועוד.

משרד הבריאות האמריקאי פרסם הבהרה לפיה, יחידים או ארגונים המשמשים רק כ"צינור" לניוד מידע רפואי מוגן, אך לא ניגשים למידע זה, אלא באופן אקראי או נדיר לשם ביצוע ניוד המידע או כנדרש על פי החוק, אינם שותפים עסקיים. כך לדוגמה, ספקי שירותי דיוור, אינם שותפים עסקיים כאמור בחוק.[1]

[1] https://www.hhs.gov/hipaa/for-professionals/faq/245/are-entities-business-associates/index.html

משרד הבריאות מדגיש כי חריג זה חל רק ככל שניוד המידע לא כרוך באחסון ארוך יותר מאחסון רגעי הדרוש לשם ביצוע הניוד. על כן, מבהיר משרד הבריאות כי ספקי שירותי אחסון בענן אינם נכנסים בגדר החריג, ומהווים למעשה שותפים עסקיים כאמור בחוק.[2]

2.3. **מידע אישי רפואי מזהה (Individually Identifiable Health Information)** סעיף 160.103

מידע רפואי הכולל נתונים מזהים אודות יחיד. לדוגמה, כתובת, תאריך לידה, מספר בביטוח לאומי (Social Security Number) אשר:

2.3.1. נוצר על ידי או מתקבל מאת ספק שירותי בריאות (healthcare provider), תוכנית בריאות (health plan), עובד (employer), או מסלקת שירותי בריאות (healthcare clearinghouse) כהגדרת מונחים אלו תחת סעיף 160.103 לחוק;

2.3.2. קשור למצב פיזיולוגי או מנטלי של יחיד בעבר, בהווה או בעתיד; או לתשלום בגין שירותי בריאות;

2.3.3. ושמזהה את היחיד או שניתן להניח כי באמצעותו ניתן לזהות את היחיד.

2.4. **מידע רפואי מוגן (PHI)** סעיף 160.103

הינו מידע אישי רפואי מזהה (Individually Identifiable Health Information) המועבר או נשמר במדיה אלקטרונית או בכל צורה או אמצעי אחר, אך אינו כולל מידע:

2.4.1. מרשומות חינוך המכוסות תחת החוק הפדרלי Family Educational Rights and Privacy Act of 1974 ('FERPA');

2.4.2. מרשומות מסוימות של בתי ספר תיכוניים המוחזקות על ידי ספקי שירותי בריאות;

2.4.3. מרשומות העסקה המוחזקות על ידי יישות מכסה במסגרת תפקידה כמעסיק;

2.4.4. אודות אדם שנפטר לפני למעלה מ – 50 שנים.

2.5. **מידע רפואי מוגן בלתי מאובטח (Unsecured Protected Health Information)** סעיף 164.402

זהו מידע רפואי מוגן, שלא עבר התמרה (טרנספורמציה) באמצעות טכנולוגיה ושיטות המפורטות בהנחיות מזכירות משרד הבריאות,[3] על מנת שיהא בלתי שמיש, בלתי קריא או בלתי ניתן לפענוח למי שאינו מורשה לגשת אליו. הנחיות המזכירות מתייחסות לשיטות הצפנת המידע או השמדת המדיה עליה היה שמור המידע.

2.6. **שימוש במידע רפואי מוגן (Use)** סעיף 160.103

החוק כולל תחת הגדרת המונח "שימוש" שיתוף, יישום, ייעול, בחינה או ניתוח של מידע אישי רפואי מזהה על ידי היישות המחזיקה במידע זה.

2.7. **חשיפת מידע (Disclosure)** סעיף 160.103

מתן גישה למידע או העברת מידע אל מחוץ ליישות המחזיקה במידע בכל צורה ודרך.

---

[2] https://www.hhs.gov/hipaa/for-professionals/special-topics/health-information-technology/cloud-computing/index.html#_ftn14

[3] https://portal.ct.gov/-/media/Departments-and-Agencies/DSS/HIPAA-Information/GuidanceToRender.pdf?la=en

2.8. **התממה (De-identification) של מידע רפואי מוגן**

מידע רפואי מוגן שעבר תהליך התממה הינו מידע רפואי שאינו מזהה יחיד ואין בסיס סביר להניח כי ניתן להשתמש בו כדי לזהות יחיד. הוראות החוק לא חלות עוד על מידע זה. החוק מפרט שתי דרכים להתממה: [4]

2.8.1. באמצעות קביעת מומחה בעל ידע וניסיון מתאים, לפיה הסיכון שהמידע, לבדו או בצירוף מידע נוסף, יוכל לשמש לזיהוי יחיד, נמוך מאוד; או

2.8.2. באמצעות הסרה של 18 נתונים מזהים על אודות היחיד, קרוביו, מעסיקו או בני ביתו. לדוגמה, שמות, כתובת, תמונות פנים, מזהים ביומטריים, לרבות טביעת אצבע וקול וכיו"ב נתונים מזהים.

2.9. **אירוע אבטחה העולה כדי פריצה (Breach)** סעיף 164.402

רכישה, מתן גישה, שימוש או חשיפה ללא הרשאה למידע רפואי מוגן, המסכנים את אבטחת המידע או את ההגנה על פרטיות המידע, אלא אם היישות המכוסה או השותף העסקי מוכיחים כי ישנה סבירות נמוכה שהמידע הרפואי נפגע, בהתבסס על הערכת סיכון, במסגרתה נשקלו לכל הפחות השיקולים הבאים:

2.9.1. טבעו והיקפו של המידע הרפואי המוגן הרלבנטי, לרבות סוגי הנתונים המזהים שבו והסבירות שפרטים מזהים שהוסרו מהמידע ישוחזרו;

2.9.2. זהות הגורמים הבלתי מורשים שנחשפו למידע או השתמשו בו;

2.9.3. האם הלכה למעשה צפו במידע או שנעשה בו שימוש;

2.9.4. עד כמה הופחת הסיכון לחשיפת המידע.

2.10. **אירוע אבטחה שאינו עולה כדי פריצה (Security Incident)** סעיף 164.304

כל ניסיון גישה, שימוש, חשיפה, שינוי או אובדן מידע בלתי מורשים או הפרעה לפעילות מערכת מידע, בין אם ניסיון זה צלח ובין אם כשל.

2.11. **מזכירות משרד הבריאות האמריקאי The secretary of the U.S. Department of Health and Human Services (HHS)-** סעיף 160.103

מזכירות משרד הבריאות וכן כל משרד ממשלתי או עובד משרד ממשלתי שמשרד הבריאות האמריקאי האציל לו מסמכויותיו.

2.12. **המשרד לזכויות האזרח במשרד הבריאות האמריקאי The U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR)**

המשרד לזכויות אזרח הוא הגורם האמון על אכיפת החוק, והוא מבצע, הלכה למעשה, פעולות אכיפה, כמפורט תחת הפרק: "סנקציות והשלכות נוספות להפרת החוק".

3. <u>מידע כללי על החוק</u>

3.1. **רקע**

HIPAA הינו חוק פדרלי שנועד ליצור סטנדרטיים לאומיים להגנה על פרטיות מידע רפואי ואבטחתו ולמניעת גילויו של מידע זה ללא ידיעתו והסכמתו של היחיד אודותיו המידע כאמור.

החוק מורכב מחמישה כללים עיקריים:

[4] בסעיף 164.514(b)

3.1.1. **כלל הפרטיות (The Privacy Rule)** – כלל הפרטיות מסדיר את השימוש והחשיפה של מידע רפואי מוגן על ידי יישויות מכוסות ושותפים עסקיים. הכלל מגביל את השימוש במידע רפואי מוגן וחשיפתו, תוך קביעת זכותם של היחידים על אודותיהם המידע כאמור לשלוט בשימוש בו ובחשיפתו.

3.1.2. **כלל האבטחה (The Security Rule)** – קובע סט של אמצעי אבטחה אדמיניסטרטיביים, טכניים ופיזיים שמטרתם להגן על סודיות מידע רפואי מוגן, תקינותו וזמינותו.

3.1.3. **כלל האכיפה (The Enforcement Rule)** – העדר רמת ציות מספקת מצד יישויות מכוסות ושותפים עסקיים, הביאה לידי חקיקת כלל האכיפה, המקנה למשרד הבריאות האמריקאי (HHS), ובפרט למשרד זכויות האזרח שבו (OCR) סמכויות חקירה והטלת קנסות בגין אי ציות להוראות החוק.

3.1.4. **כלל הדיווח על אודות אירוע אבטחה העולה כדי פריצה (The Breach Notification Rule)** – קובע הוראות בדבר מתן הודעות ליחידים ולממשלה בעקבות אירוע אבטחה.

3.1.5. **הכלל המקיף (The Omnibus Rule)** – מכיל הוראות מהחוק המכונה חוק ההייטק (The Health Information Technology for Economic and Clinical Health Act, **HITECH**)) במטרה להקשיח את ההגנה על מידע רפואי מוגן.

3.2. **מועד תחילה / חקיקה**

מרכיביו השונים של החוק נחקקו ונכנסו לתוקף במועדים שונים. כך בעוד החוק עצמו נחקק כבר בשנת 1996, כלל הפרטיות התווסף בשנת 2000, כלל האבטחה בשנת 2003 והכלל המקיף נחקק בשנת 2013, כאשר הוא כולל בחובו הוראות מחוק ההייטק שנחקק בשנת 2009.

4. <u>תחולה</u>

4.1. החוק חל על יישויות מכוסות (כהגדרת מונח זה לעיל), לדוגמה, רופאים, אחיות, בתי חולים, בתי מרקחת, חברות ביטוח רפואי וכיוצ"ב ארגונים האוספים ומעבדים מידע רפואי מוגן דרך קבע וכחלק מליבת עבודתם.

4.2. בנוסף, החוק חל על שותפים עסקיים שהינם ארגונים או יחידים המבצעים פעולות ושירותים הכרוכים באיסוף מידע רפואי מוגן, בשימוש בו או בחשיפתו, בשם יישות מכוסה. כלומר, ספקי מיקור חוץ, גם אם אינם אמריקאים, אך הם מספקים שירות הכרוך באיסוף, עיבוד, אחסון או חשיפה של מידע רפואי מוגן, בשם היישות המכוסה, נדרשים לציית לדין כשותפים עסקיים.

5. <u>ציות – שימוש מותר במידע רפואי מוגן</u>

5.1. כלל הפרטיות קובע איסור כללי על שימוש במידע רפואי מוגן או חשיפתו ללא קבלת הסכמתו של היחיד על אודותיו המידע (או מיופה כוחו) מראש ובכתב. בכלל זאת, נאסר בפרט שימוש במידע רפואי מוגן ביחס לפעולות הקשורות בגיוס כספים, פרסום ושיווק ומחקר, אלא בכפוף לקבלת ההסכמה כאמור.

5.2. על אף האיסור הגורף לעיל, יישות מכוסה רשאית (ולעיתים אף מחויבת) להשתמש במידע רפואי מוגן או לחשוף אותו, אף ללא הסכמתו של היחיד, לדוגמה, על מנת לאפשר או להקל על הליך או טיפול רפואי ולצורך תשלום בגינם (כהגדרתם בסעיף 164.501), כאשר שימוש או חשיפה אלו אגביים לשימוש או לחשיפה המותרים על פי החוק, או במענה לדרישה של מזכירות משרד הבריאות האמריקאי ובכפוף לתנאים המפורטים בחוק (להרחבה ראו סעיף 164.502(a)).

5.3. שותף עסקי מורשה להשתמש במידע הרפואי המוגן או לחשוף אותו, אך ורק על פי הנחיות היישות המכוסה, כפי שהן מנוסחות בהסכם השותף העסקי (Business Associate Agreement (BAA)) או על פי דין (להרחבה ראו סעיפים (164.502(a)(3)-(4)).

5.4. גילוי מועט ככל הניתן – יישות מכוסה או שותף עסקי מחויבים לנקוט מאמץ סביר לחשוף או לשתף את חלקו המינימאלי של המידע הרפואי המוגן ההכרחי לצורך השגת המטרה לשמה מתבצעת חשיפתו.

6. <u>חובות החלות על ישות מכוסה ושותף עסקי</u>

החוק מטיל על הכפופים לו סט של חובות בתחום הגנת פרטיות ואבטחת מידע. פרק זה מתמקד בחובות העיקריות בתחום הגנת פרטיות החלות על יישויות מכוסות ושותפים עסקיים מכוח כלל הפרטיות.

6.1. <u>חובות החלות על יישויות מכוסות</u>

6.1.1. <u>מינוי נושאי תפקיד</u>

כל יישות מכוסה נדרשת למנות שני נושאי תפקיד – קצין הגנת פרטיות ואיש קשר.

קצין הגנת הפרטיות אחראי על גיבוש והטמעת מסמכי מדיניות, נהלים והליכים פנימיים בקשר עם הגנת פרטיות.

קצין הגנת הפרטיות נדרש להדריך את עובדי היישות המכוסה בנוגע להגנה על פרטיות מידע רפואי מוגן ואבטחתו, לרבות בקשר לאפשרות לשתף מידע רפואי מוגן, עם מי ניתן לשתף מידע זה ובאילו נסיבות.

איש הקשר אמון על קבלת תלונות בקשר עם פגיעה בפרטיות ועל אספקת מידע ומענה לשאלות בקשר להודעת הפרטיות המפורסמת על ידי היישות המכוסה.

6.1.2. <u>הסכמים והודעות חוץ - ארגוניים</u>

6.1.2.1. **הסכם שותף עסקי (Business Associate Agreement (BAA)) (סעיף 164.504(e)(2))** –

ישות מכוסה המתקשרת עם שותף עסקי, דהיינו, ספק שירותים שיוצר או מקבל מידע רפואי מוגן בשמה, נדרשת להסדיר את חובותיו ביחס להגנה על מידע רפואי מוגן ואבטחתו, בהתאם לחוק באמצעות הסכם שותף עסקי. הסכם זה כולל התייחסות לכל הפחות לנושאים הבאים:

6.1.2.1.1. הגדרת פעולות שימוש וחשיפה מותרים במידע הרפואי המוגן על ידי השותף העסקי.

6.1.2.1.2. איסור שימוש במידע הרפואי המוגן למטרות עצמאיות של השותף העסקי, למעט לצורכי ניהול ואדמיניסטרציה של עסקו של השותף העסקי.

6.1.2.1.3. היתר ליישות המכוסה לסיים את ההתקשרות עם השותף העסקי, אם יימצא כי השותף העסקי הפר מהותית תנאי מתנאי הסכם השותף העסקי.

6.1.2.1.4. התחייבות השותף העסקי כי:

6.1.2.1.4.1. לא יעשה שימוש או יחשוף את המידע הרפואי המוגן, אלא בהתאם להרשאה שניתנה לו תחת הסכם השותף העסקי או הדין.

6.1.2.1.4.2. ינקוט באמצעי הגנה מתאימים על מנת למנוע שימוש או חשיפה של המידע הרפואי המוגן שלא בהתאם להסכם השותף העסקי.

6.1.2.1.4.3. ידווח ליישות המכוסה על כל שימוש או חשיפה של מידע רפואי מוגן, שאינו בהתאם להסכם השותף העסקי מיד עם גילויים.

6.1.2.1.4.4. יחתים כל ספק משנה מטעמו, היוצר, מקבל, מחזיק או מעביר מידע רפואי מוגן בשם השותף העסקי, על הסכם הכולל את ההוראות החלות על השותף העסקי ביחס למידע רפואי מוגן זה.

6.1.2.1.4.5. יעמיד לרשות היישות המכוסה מידע רפואי מוגן למטרות מימוש זכויות על ידי יחידים (כדוגמת זכות העיון, הזכות לקבלת דיווח על שיתוף המידע וזכות תיקון המידע).

6.1.2.1.4.6. יציית להוראות החוק החלות על היישות המכוסה, בעת ביצוע התחייבויות בשמה.

6.1.2.1.4.7. יעמיד לרשות מזכירות משרד הבריאות האמריקאי את מסמכיו ונהליו הפנימיים בקשר עם שימוש או חשיפה של מידע רפואי מוגן בשם יישות מכוסה, לצורך בחינת ציות היישות המכוסה לחוק.

6.1.2.1.4.8. בעת סיום ההתקשרות, ישיב ליישות המכוסה את המידע הרפואי המוגן או ישמיד אותו. אם השבה או השמדה כאמור אינם ברי ביצוע, יותיר על כנם את אמצעי ההגנה על המידע בהתאם להסכם השותף העסקי ויגביל את השימוש במידע או שיתופו רק למטרות בגינן לא מתאפשרת השמדת המידע או השבתו.

6.1.2.2. **הודעת פרטיות** (סעיף 164.520) –

6.1.2.2.1. יישות מכוסה נדרשת ליידע את היחידים שהיישות המכוסה מחזיקה מידע רפואי מוגן אודותיהם, בדבר נוהגי הפרטיות שלה ביחס למידע זה. החוק מפרט הוראות בדבר פרסום ההודעה ותוכנה, ובכלל זאת:

6.1.2.2.1.1. יישות מכוסה המפעילה אתר אינטרנט, במסגרתו מפורסם מידע אודות שירות הלקוחות של היישות המכוסה או הטבות ללקוחות נדרשת לפרסם את הודעת הפרטיות שלה באתר.

6.1.2.2.1.2. יישות מכוסה נדרשת לשלוח את ההודעה באופן אלקטרוני (לדוגמה, באמצעות דוא"ל) בתגובה לבקשה הראשונה של יחיד לקבל שירות.

6.1.2.2.1.3. ליחיד המקבל את הודעת הפרטיות באופן אלקטרוני שמורה הזכות לקבל את ההודעה אף בעותק קשיח.

6.1.2.2.2. **יישות מכוסה המתקשרת באופן ישיר עם יחיד –**

יישות מכוסה המתקשרת באופן ישיר עם יחיד, נדרשת ליידעו אודות נוהגי הפרטיות שלה באינטראקציה הראשונה עם היחיד, כלקוח שלה, בין אם פנים מול פנים, בין אם בדיוור אלקטרוני ובין אם בשיחת טלפון.

למעט במקרי חירום, יישות מכוסה המקיימת יחסי טיפול, ישירות עם יחידים, נדרשת על פי החוק לעשות מאמץ כן להשיג אישור בכתב מהמטופל על שקיבל את הודעת הפרטיות (acknowledgment of receipt).

חריג להוראה זו, הינו במקרים בהם נדרש טיפול חירום, אז היישות המכוסה מחויבת למסור את הודעת הפרטיות מטעמה בהקדם האפשרי בחלוף בהילות החירום.

היישות המכוסה אף נדרשת לפרסם את הודעת הפרטיות בכל אתר אינטרנט במסגרתו היא מציעה את שירותיה, במקום בו סביר להניח כי יחיד המעוניין בשירות יוכל לקרוא את ההודעה.

החוק כולל הוראה דומה ביחס לאתרים פיזיים, אשר גם בהם נדרשת היישות המכוסה לפרסם את הודעת הפרטיות מטעמה, במקום בו סביר להניח כי יחיד המעוניין בשירות יוכל לקרוא את ההודעה.

ההודעה צריכה להיכתב בשפה פשוטה, ברורה וקלה לקריאה.

על הודעת הפרטיות להיות מעודכנת, והיישות המכוסה נדרשת לערוך אותה ולבצע בה את ההתאמות הנדרשות לאור שינויים בשימוש ובחשיפה של מידע רפואי מוגן, בזכויות יחידים, בחובות חוקיות החלות על היישות המכוסה או בנוהגי פרטיות אחרים המפורטים בהודעה.

אין להטמיע שינוי כאמור, אלא לאחר מועד תחילת ההודעה המעודכנת, למעט בכפוף להיתר לעשות כן על פי חוק.

6.1.2.2.3. **תוכן ההודעה –**

6.1.2.2.3.1. ההודעה צריכה לפרט ולהסביר את נוהגי הפרטיות של היישות המכוסה בקשר עם המידע הרפואי המוגן, ובכלל זאת, לכלול תיאורים והצהרות אודות סוגי השימושים במידע הרפואי המוגן; מטרות השימוש; תיאור השימושים במידע וגילויו המחייבים את הסכמת היחיד על אודותיו המידע; הצהרה בדבר זכויות יחידים על אודותיהם המידע והסבר על דרכי מימוש זכויות אלו; הצהרת היישות המכוסה בדבר חובתה להגן על המידע הרפואי המוגן ולציית לכללים ולהוראות המפורטים בהודעתה.

6.1.2.2.3.2. כותרת ההודעה צריכה לכלול את הנוסח האחיד הבא:

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

6.1.2.3. **הודעה בדבר אירוע אבטחה העולה כדי פריצה (Breach)** –

יישות מכוסה נדרשת ליידע את היחידים על אודותיהם המידע הרפואי המוגן בדבר אירוע אבטחה חמור. בקרות אירוע אבטחה חמור רחב היקף (כמפורט בהמשך) היישות המכוסה מחויבת ליידע גם את התקשורת ואת מזכירות משרד הבריאות.

שותפים עסקיים נדרשים ליידע אודות אירוע אבטחה חמור רק את היישות המכוסה בשמה הם פועלים.

6.1.2.3.1. **מתן הודעה ליחידים** (סעיף 164.404) –

במקרה של אירוע אבטחה העולה כדי פריצה, היישות המכוסה מחויבת ליידע את היחידים אודותיהם המידע הרפואי המוגן ללא דיחוי, ובכל מקרה בתוך 60 ימים מרגע גילוי האירוע.

יש לספק את ההודעה בדואר או בדוא"ל (אם היחיד אישר קבלת הודעות בדוא"ל), במקרים חריגים תתאפשר מסירת ההודעה בדרכים חלופיות כדוגמת טלפון או פרסום באתר האינטרנט של היישות המכוסה.

ההודעה תכלול פרטים בדבר האירוע והשלכותיו, לרבות תיאור של סוגי המידע הרפואי הבלתי מאובטח (כהגדרת מונח זה בפרק ההגדרות) המעורב באירוע, צעדים שעל היחידים לנקוט על מנת להגן על עצמם מפני נזק פוטנציאלי שמקורו באירוע, פרטי קשר עם היישות המכוסה לשאלות מטעם היחידים בקשר עם האירוע ופירוט הצעדים שנקטה היישות המכוסה בעקבות גילוי האירוע.

6.1.2.3.2. **מתן הודעה לתקשורת** (סעיף 164.406) –

בעת אירוע אבטחה העולה כדי פריצה, בקשר עם מידע רפואי בלתי מאובטח על אודות למעלה מחמש מאות תושבים של תחום שיפוט מסוים או מדינה, על היישות המכוסה להודיע על האירוע לכלי תקשורת בולט בתחום שיפוט זה או במדינה כאמור.

ההודעה תכלול את הפרטים הנדרשים בקשר עם הודעה ליחידים ותינתן בהתאם ללוחות הזמנים של מתן הודעה ליחידים (כמפורט לעיל).

6.1.2.3.3. **הודעה למזכירות משרד הבריאות** (סעיף 164.408) –

בקרות אירוע אבטחה העולה כדי פריצה, בקשר עם מידע רפואי לא מאובטח על אודות חמש מאות יחידים או יותר, היישות המכוסה נדרשת לדווח למזכירות משרד הבריאות באמצעות מילוי טופס אינטרנטי והגשתו באתר משרד הבריאות.

יישות מכוסה נדרשת לדווח למזכירות משרד הבריאות על אירועי אבטחה בקשר עם מידע רפואי לא מאובטח על אודות פחות מחמש מאות יחידים, שהתגלו במהלך אותה שנה קלנדרית, תוך 60 ימים מתום אותה שנה קלנדרית.

גם דיווחים אלו יוגשו באופן אלקטרוני על ידי מילוי טופס אינטרנטי באתר משרד הבריאות.

6.1.2.4. **אישור בכתב של יחידים לשימוש במידע רפואי מוגן לצרכים שיווקיים (סעיף 164.508) –**

תקשורת "שיווקית" באופייה מותרת תחת החוק בכפוף לאישור מראש ובכתב של היחיד. יישות מכוסה אינה רשאית למכור מידע רפואי מוגן לשותפים עסקיים או לצדדים שלישיים.

בנוסף, יישות מכוסה רשאית למכור רשימות של שמות של יחידים אך ורק בכפוף לאישור מראש ובכתב של היחידים. חריג לחובת קבלת האישור כאמור, הינו בעת תקשורת ישירה בין יישות מכוסה ויחיד, המתבצעת פנים מול פנים. תקשורת זו, אף אם היא בעלת אופי שיווקי, לא דורשת את אישור היחיד.

6.1.3. <u>מסמכים והליכים פנים - ארגוניים</u>

6.1.3.1. **מסמכי מדיניות ונהלים**

יישות מכוסה נדרשת לגבש ולהחיל מסמכי מדיניות, נהלים והליכים פנימיים על מנת להטמיע את עקרונות החוק שלהלן:

6.1.3.1.1. הגבלת שימושים וגילוי מידע רפואי מוגן למינימום ההכרחי הנדרש על מנת להשיג את המטרה לשמה נערך השימוש במידע או גילויו (סעיפים 164.502(b) ו-164.5014(d)).

6.1.3.1.2. הגבלת גישה ושימוש במידע רפואי מוגן, אך ורק לעובדי היישות המכוסה עם צורך לדעת את המידע, לשם ביצוע תפקידם (סעיף 164.308).

6.1.3.1.3. יישות מכוסה נדרשת להטמיע נהלים על מנת להסדיר את אפשרותם של יחידים להגיש תלונה בגין נוהגי הפרטיות ואבטחת המידע הרפואי המוגן על ידי היישות המכוסה. היישות המכוסה נדרשת לפרסם הסבר אודות נהלים אלו בהודעת הפרטיות מטעמה.

6.1.3.1.4. נקיטת צעדי תיקון (mitigation) – יישות מכוסה נדרשת, כלל הניתן, לנקוט בצעדים על מנת להקל ולמזער תוצאות אפשריות של שימוש במידע רפואי בלתי מוגן או גילויו, על ידי עובד ביישות המכוסה או שותף עסקי, המפרים את הוראות הודעת הפרטיות מטעם היישות המכוסה, את נהליה הפנימיים או את כלל האבטחה.

6.1.3.2. **תיעוד** –

יישות מכוסה כפופה לחובות תיעוד, בהן החובה לתעד באופן רציף כל גילוי של המידע הרפואי המוגן וכן את ההליכים והמסמכים הפנימיים בקשר עם נוהגי הפרטיות של היישות המכוסה (ראו בהמשך פרק הדן בחובות התיעוד החלות על יישות מכוסה ושותפים עסקיים).

6.1.4. <u>זכויות יחידים</u>

בדומה לדיני פרטיות אחרים ברחבי העולם, החוק מקנה ליחידים, זכויות בקשר עם המידע הרפואי המוגן אודותיהם, כמפורט להלן:

6.1.4.1. **זכות הגישה למידע רפואי מוגן (סעיף 164.524) –**

תחת החוק, ליחידים הזכות לעיין במידע הרפואי המוגן אודותיהם, לקבל עותק ממנו (או שניהם) או להורות ליישות מכוסה להעביר את המידע כאמור לצד שלישי, בכפוף לחריגים, אשר בהתקיימם יכולה היישות המכוסה לדחות את בקשת היחיד לגשת למידע אודותיו.

זכות הגישה מוקנית ליחיד כל עוד המידע בקשר אליו נשמר על ידי היישות המכוסה או השותף העסקי, ללא תלות במועד איסוף או יצירת המידע, אופן שמירתו (אלקטרונית או פיזית) או מקורו.

זכות הגישה למידע תחת החוק חלה על "סט מידע ייעודי" (designated record set). סט מידע ייעודי כאמור הוא קבוצת רשומות הכוללת, לדוגמה, תיעוד רפואי, רישומי חיוב ותשלום ופרטים נוספים המשמשים את היישות המכוסה לשם קבלת החלטות בקשר ליחיד על אודותיו המידע.

בעת מענה לבקשת יחיד לגישה למידע אודותיו, היישות המכוסה לא נדרשת לייצר מידע חדש, כדוגמת פירוט או הסברים שאינם מצויים בסט המידע הייעודי.

כאשר יחיד מבקש גישה למידע שאינו נכלל תחת סט מידע ייעודי, היישות המכוסה יכולה לדחות את בקשתו לקבל גישה למידע.

קבלה או דחייה של בקשת יחיד לגישה למידע אודותיו, תימסר ליחיד בתוך 30 ימים מיום קבלת הבקשה (עם אפשרות להארכת מועד זה ב-30 ימים נוספים, בכפוף לעמידה בהוראות החוק בקשר להארכה כאמור).

הגישה למידע תתאפשר בדרך ובפורמט המבוקשים על ידי היחיד, אלא אם אלו אינם ניתנים לייצור בקלות. אז הגישה תינתן באמצעות עותק קשיח או בדרך ובפורמט אחר עליו יסכימו היישות המכוסה והיחיד.

אם היחיד מבקש עותק מהמידע או מוכן לקבל לידיו סיכום או הסבר של המידע, היישות המכוסה זכאית לדרוש תשלום סביר בשווי עלות יצירת מסמכים אלו.

אם היישות המכוסה דוחה את בקשתו של היחיד לגישה למידע רפואי מוגן מסוים, עליה לאפשר, ככל הניתן, גישה למידע רפואי מוגן אחר שמתבקש, ולספק הודעה אודות הדחייה בכתב ובזמן כמפורט לעיל.

6.1.4.2. **זכות תיקון המידע הרפואי המוגן (סעיף 164.526) –**

ליחיד הזכות לתיקון מידע רפואי מוגן אודותיו, השמור בסט מידע ייעודי, אם המידע אינו מעודכן או בלתי שלם.

יישות מכוסה נדרשת לתקן את המידע כאמור בתוך 60 ימים מיום קבלת בקשתו של היחיד (עם אפשרות להארכת מועד זה ב-30 ימים נוספים, בכפוף לעמידה בהוראות החוק בקשר להארכה כאמור).

היישות המכוסה נדרשת לידע את היחיד בדבר קבלת בקשתו או דחייתה, ובמקרה של קבלת הבקשה ליידע אף כל גורם (לרבות שותף עסקי) שמסרה לו את המידע על הצורך לתקנו.

היישות המכוסה נדרשת לתעד את בקשת התיקון והתהליכים והפעולות שננקטו בעקבותיה, בסט המידע הייעודי בו מצוי המידע שתיקונו מבוקש.

6.1.4.3. **הזכות לקבלת דיווח אודות גילוי (שיתוף) המידע הרפואי המוגן (סעיף 164.528) –**

ליחידים קנויה הזכות לבקש דיווח על גילוי המידע הרפואי המוגן אודותיהם, על ידי היישות המכוסה או השותפים העסקיים הפועלים מטעמה. תקופת הגילוי המירבית הינה ביחס לשש שנים טרם מועד הגשת בקשת הדיווח. יישות מכוסה אינה מחוייבת לדווח על גילוי שביצעה בטרם מועד תחילת ציותה לכלל הפרטיות.

יישות מכוסה נדרשת להשיב לבקשת הדיווח בתוך 60 ימים מיום קבלת בקשתו של היחיד (עם אפשרות להארכת מועד זה ב-30 ימים נוספים, בכפוף לעמידה בהוראות החוק בקשר להארכה כאמור).

יחיד זכאי לקבלת דיווח בודד ללא עלות אחת ל-12 חודשים. החל מבקשתו השנייה של היחיד בתוך אותם 12 חודשים, זכאית היישות המכוסה לדרוש תשלום סביר בשווי עלות הבקשה, ובלבד שהיישות המכוסה יידעה את היחיד מראש לגבי העמלה ואפשרה לו לחזור בו מבקשתו או לשנותה על מנת להימנע מתשלום העמלה או להפחיתה.

הדיווח יכלול את הפרטים הבאים:

6.1.4.3.1. מועד הגילוי;

6.1.4.3.2. שם המוסד או האדם להם גולה המידע הרפואי המוגן וכתובתם (ככל שכתובתם ידועה);

6.1.4.3.3. תיאור קצר של המידע הרפואי המוגן שגולה;

6.1.4.3.4. הצהרה קצרה בדבר מטרת גילוי המידע.

6.1.4.4. **הזכות לבקש את הגבלת השימוש במידע רפואי מוגן (סעיף 164.522(a)(1) –**

ליחידים הזכות לבקש את הגבלת השימוש במידע הרפואי המוגן אודותיהם וחשיפתו לצרכים מוגדרים, כדוגמת ביצוע טיפול רפואי או תשלום בגינו. היישות המכוסה אינה מחויבת לקבל את הבקשה, אך אם קיבלה את הבקשה, היישות המכוסה מחויבת לכבדה, ולגלות את המידע שלא בהתאם לבקשה, רק במקרים חריגים, כדוגמת צורך בטיפול חירום.

6.1.4.5. **הזכות לבקש אמצעים חלופיים או מיקום חלופי להתקשרות בנוגע למידע רפואי מוגן (סעיף 164.522(b)(1) –**

ספק שירותים רפואיים מחויב לאפשר ליחידים לקבל מידע בקשר למידע הרפואי המוגן אודותיהם מספקי שירותי בריאות, על ידי אמצעים אחרים או במקום אחר מדרך ההתקשרות הרגילה על מנת לשמור על סודיות המידע. כך לדוגמה, אדם יכול לבקש מהרופא המטפל שלו להתקשר אליו למשרדו ולא לביתו. ספק שירותי הבריאות חייב להיענות לבקשות מסוג זה אם היחיד מצהיר בבירור כי אי היענות לבקשתו עלולה לסכן אותו.[5]

6.1.4.6. **הזכות להסכים או לסרב לשימושים מסוימים במידע רפואי מוגן (סעיף 164.510 –**

[5] https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/disclosures-treatment-payment-health-care-operations/index.html

יישות מכוסה מחויבת לתת ליחיד אפשרות להסכים או להתנגד למטרות מסוימות לשימוש במידע הרפואי המוגן או לגילויו.

6.1.4.7. **הזכות להגיש תלונה (סעיף 160.306) –**

יחידים הסבורים כי יישות מכוסה או שותף עסקי אינם מקיימים את הוראות החוק, רשאים להגיש תלונה למשרד לזכויות האזרח במשרד הבריאות (OCR). ניתן לעשות זאת באמצעות משלוח התלונה בדואר, בפקסימיליה, בדוא"ל לכתובת (OCRComplaint@hhs.gov) או דרך הפורטל של ה-OCR (OCR Complaint Portal).

6.1.5. נקיטת פעולות למזעור השפעות אירוע אבטחה העולה כדי פריצה (Breach Mitigation) (סעיף 164.504(e)(1)) –

החוק מטיל חובה על יישות מכוסה לנקוט בצעדים הדרושים על מנת למתן כל השפעה מזיקה של אירוע אבטחה העולה כדי פריצה. צעדים אלו עשויים לכלול: אחזור, מחיקה או השמדה של מידע רפואי מוגן שנחשף באופן בלתי מורשה; הפסקת גישה או שינוי סיסמאות; שינוי מסמכי מדיניות ונהלים וכו'.

עם היוודע ליישות המכוסה כי שותף עסקי מפר את הוראות החוק, עליה לנקוט בצעדים הדרושים כדי לתקן את ההפרה או לסיים את ההתקשרות עם השותף העסקי.

6.1.6. חובות אבטחת מידע –

יישות מכוסה (וכן שותף עסקי) כפופים לחובות אבטחת מידע, תחת כלל האבטחה. ראו בהמשך פירוט בדבר חובות אלו תחת פרק 5.9.

6.2. **חובות החלות על שותף עסקי**

בעוד בעבר הטיל החוק חובות רק על יישויות מכוסות, בשנת 2013, שונו הוראות בכללים המרכיבים את ה – HIPAA, תוך יצירת תחולה ישירה של חלק מהוראותיו של "חוק ההייטק" (The Health Information Technology for Economic and Clinical Health Act, (**HITECH**)), על שותפים עסקיים ולא רק על יישויות מכוסות.

לאור שינויים אלו, שותפים עסקיים אחראים היום באחריות ישירה ונתונים לפעולות אכיפה ביחס להפרת הוראות החוק, כדלקמן:

- אי דיווח והגשת מסמכי ציות נדרשים למזכירות משרד הבריאות; שיתוף פעולה עם חקירות בעקבות תלונות וחקירות לבחינת עמידה בהוראות החוק; מתן גישה למזכירות משרד הבריאות, לרבות למידע רפואי מוגן לצורך קביעת עמידה בהוראות החוק (סעיפים: 160.310, 164.502(a)(4)(i)).

- נקיטת פעולת תגמול כנגד יחיד בגין הגשת תלונה בקשר עם ציות להוראות החוק, השתתפותו בחקירה או בהליך אכיפה אחר או בשל התנגדותו למעשה או נוהג שאינם חוקיים תחת החוק (סעיף 160.316).

- העדר ציות לכלל האבטחה (סעיפים 42 USC § 17931, 13401 § בחוק ההייטק מחילים באופן ישיר את הוראות סעיפים 164.308, 164.310, 164.312, ו-164.316 על שותפים עסקיים; וכן סעיפים 164.306, 164.308, 164.310, 164.312, 164.314, 164.316).

- אי דיווח על אירוע אבטחה ליישות מכוסה או לשותף עסקי אחר (סעיפים 164.410 ו-164.412).

- שימוש במידע רפואי מוגן או חשיפתו ללא הרשאה (סעיף 164.502(a)(3)).

- אי העברת מידע רפואי מוגן ליישות מכוסה, ליחיד או למיופה כוחו (בהתאם להוראות הסכם השותף העסקי) על מנת לסייע ליישות המכוסה בציות לחובותיה בקשר עם זכות העיון (סעיפים 164.524(c)(2)(ii)ו-(3)(ii)).

- העדר צמצום שימוש או חשיפה של מידע רפואי מוגן למינימום ההכרחי לצורך הגשמת מטרת השימוש בו (סעיף 164.502(b)).

- אי העברת תיעוד חשיפת המידע הרפואי המוגן בנסיבות מסוימות (סעיפים 42 U.S.C. § 17935(c)(3), 13405(c)(3) 13405(c)(2) לחוק ההייטק).

- התקשרות עם ספק משנה, שיוצר או מקבל מידע רפואי מוגן בשם השותף העסקי שלא באמצעות הסכם שותף עסקי, או העדר הטמעה של הוראות הסכם השותף העסקי (סעיפים 164.504(e)(5), 164.502(e)(1)(ii)).

- אי נקיטת צעדים סבירים בקשר עם אירוע אבטחה או הפרה של הסכם שותף עסקי על ידי ספק משנה (164.504(e)(1)(iii)).

בהתאם לשינוי כאמור, והחלת תחולה ישירה של חלק מהוראות החוק על שותפים עסקיים, להלן הפעולות הנדרשות משותף עסקי לצורך עמידתו בעיקרי הוראות החוק:

6.2.1. **עדכון מסכי מדיניות ונהלים –**

שותפים עסקיים נדרשים לעדכן את מסמכי המדיניות, הנהלים הפנימיים ונוהגי הפרטיות ואבטחת המידע כך שיהלמו את הוראות החוק.

6.2.2. **מינוי קצין אבטחת מידע (Security Official) (סעיף 164.308(a)(2)) –**

שותפים עסקיים נדרשים למנות קצין אבטחה האמון על פיתוח והטמעת נוהגי פרטיות מידע רפואי מוגן ואבטחתו והליכי ציות לחוק.

6.2.3. **התקשרות עם ספקי משנה באמצעות הסכם שותף עסקי (סעיף 164.504(e)(5)) –**

כאמור לעיל, שותף עסקי נדרש להתקשר עם כל ספק משנה שלו, שיוצר או מקבל מידע רפואי מוגן בשמו, באמצעות הסכם שותף עסקי.

הסכם השותף העסקי עם ספק משנה יכלול את כל ההוראות הנדרשות במסגרת הסכם שותף עסקי בין יישות מכוסה לבין שותף עסקי, בשינויים המחוייבים.

6.2.4. **הודעה בדבר אירוע אבטחה ליישות מכוסה או לשותף עסקי אחר (סעיף 164.410) –**

שותף עסקי נדרש להודיע ליישות מכוסה על אירוע אבטחה, עם גילוי קרות האירוע. מועד הגילוי הינו ביום בו התגלה האירוע בפועל או ביום הראשון בו היה על השותף העסקי לדעת על אירוע זו, לו הפעיל מאמץ סביר לגלותו.

יראו שותף עסקי כמי שידע על אירוע אבטחה, אם אירוע זה ידוע או במאמץ סביר היה ידוע, לאדם אחר, שאיננו הגורם לאירוע האבטחה או עובד או נושא תפקיד אחר בשותף העסקי.

6.2.4.1. **מועד הדיווח על אירוע אבטחה –**

בכפוף לחריגים הקבועים בחוק, שותף עסקי ידווח על אירוע אבטחה ללא שיהוי בלתי סביר, ובכל מקרה בתוך 60 ימים קלנדריים מיום גילוי האירוע.

6.2.4.2. **תוכן הדיווח על אירוע אבטחה –**

הדיווח יכלול, ככל הניתן, את זהות היחידים שהשותף העסקי יודע או מניח באופן סביר, כי מידע רפואי מוגן בלתי מאובטח (unsecured PHI כהגדרתו מעלה) על אודותיהם נחשף.

השותף העסקי יספק ליישות המכוסה כל מידע נגיש נוסף, שהיישות המכוסה נדרשת לכלול בדיווחה ליחידים על אודות אירוע האבטחה.

6.2.5. **חובות אבטחת מידע –**

שותף עסקי (וכן יישות מכוסה) כפופים לחובות אבטחת מידע, תחת כלל האבטחה. פירוט בדבר חובות אלו ניתן למצוא בהמשך תחת פרק מס' 6.3.

6.3. **חובות אבטחת מידע החלות הן על יישויות מכוסות והן על שותפים עסקיים**

כלל האבטחה מחייב יישויות מכוסות ושותפים עסקיים להטמיע ולשמר אמצעים ובקרות אבטחת מידע ניהוליים, טכניים ופיזיים סבירים ומתאימים להגנה על המידע הרפואי המוגן.

באופן כללי, יישויות מכוסות ושותפים עסקיים נדרשים להגן על סודיות, אמינות וזמינות המידע הרפואי המוגן האלקטרוני שהם יוצרים, מקבלים, שומרים או משתפים; לזהות ולהגן מפני איומי אבטחת מידע שניתן לצפותם באופן סביר; להגן מפני שימושים או גילויים בלתי מורשים שניתן לצפותם באופן סביר; ולהבטיח ציות מצד כוח האדם שלהם.

כלל האבטחה מונה סט של דרישות ובקרות אבטחת מידע המחולקות לבקרות הכרחיות (required), ולבקרות שהיישות המכוסה או השותף העסקי נדרשים להטמיע, בכפוף לשיקול דעתם, אם אותה בקרה מהווה אמצעי אבטחה סביר ומתאים ליישום, בקשר עם אותה יישות מכוסה או שותף עסקי (addressable).

באופן ספציפי, מרבית בקרות אבטחת המידע המפורטות בכלל האבטחה מהוות בקרות מוכרות ונפוצות בדינים אחרים העוסקים באבטחת מידע. כך לדוגמה, החובה לבצע הערכת סיכונים פוטנציאליים לסודיות, אמינות וזמינות המידע הרפואי המוגן האלקטרוני; להטמיע אמצעים מספקים להפחתת סיכונים אלו, לרבות אמצעי אבטחה פיזיים וטכניים; למנות גורם האמון על פיתוח והטמעת נהלים ומסמכים דרושים לשם מימוש הוראות כלל האבטחה; להטמיע בקרות בדבר הרשאות גישה למורשי גישה מטעם היישות המכוסה או השותף העסקי; לבצע הדרכות ורענונים למורשי גישה כאמור; להטמיע תוכנית התאוששות מאסון, וכו'.

עם זאת, כלל האבטחה מונה גם הוראות שאינן נפוצות בהכרח בדינים אחרים, כדוגמת החובה להטמיע נהלים המסדירים את הרשאות הגישה למידע הרפואי המוגן בעתות חירום; או החובה לנקוט בסנקציות מתאימות נגד חברי כוח אדם, שאינם מצייתים למסמכי המדיניות ולנהלי אבטחת המידע של היישות המכוסה או השותף העסקי.

6.4. **חובות תיעוד החלות על יישויות מכוסות ועל שותפים עסקיים (סעיפים 164.530 ו- 164.316)**

תחת כלל האבטחה, יישויות מכוסות ושותפים עסקיים נדרשים לתעד בכתב נהלים ומסמכי מדיניות, פעולות נדרשות (לדוגמה, מינוי קצין אבטחת מידע, תקשורת עם יחידים על אודותיהם המידע הרפואי המוגן, תלונות מטעם יחידים ופעולות בקשר עם מימוש זכות הגישה למידע) והערכות סיכונים שבוצעו בקשר עם כלל האבטחה. יש לשמור את התיעוד כאמור למשך שש שנים.

תיעוד של נהלים ומסמכי מדיניות יישמר למשך שש שנים ממועד יצירתם או ממועד כניסתם לתוקף, על פי המאוחר מבניהם (סעיף 164.316).

יישויות מכוסות ושותפים עסקיים נדרשים לעדכן את התיעוד כאמור, בתגובה לשינויים סביבתיים או ארגוניים המשפיעים על אבטחת המידע הרפואי המוגן (סעיף 164.316(b)(2)(iii)).

7. <u>סנקציות והשלכות נוספות להפרת החוק</u>

7.1. מלבד החשש לנזק תדמיתי, הפרה של החוק עלולה לעלות כדי הפרה חוזית, לדוגמה, עקב אי עמידה בהתחייבויות שותף עסקי תחת הסכם השותף העסקי עליו הוא חתום, וכן לגרור סנקציות כספיות ואף מאסרים, כמפורט להלן.

7.2. הטלת קנסות על יישויות מכוסות ושותפים עסקיים – משרד זכויות האזרח האמריקאי (OCR), אמון על אכיפת הוראות החוק, ובסמכותו להטיל קנסות בסכומים משתנים על יישויות מכוסות ושותפים עסקיים וכן על עובדיהם, בהתאם לחומרת ההפרה.

ישנן ארבע קטגוריות לענישה כספית כאמור:

7.2.1. הפרה שהיישות המכוסה או השותף העסקי לא היו מודעים לה, ולא יכלו להימנע ממנה באמצעות הליך בדיקת נאותות סביר. היקף הקנסות תחת קטגוריה זו הינו -$100 50,000 פר הפרה ועד $25,000 לשנה.

7.2.2. הפרה שהיישות המכוסה או השותף העסקי היו צריכים להיות מודעים לה, לו נקטו בהליך בדיקת נאותות סביר, אך לא ניתן היה להימנע מקרות ההפרה, אף בנקיטת טיפול סביר. היקף הקנסות תחת קטגוריה זו הינו $1,000-50,000 פר הפרה ועד $100,000 לשנה.

7.2.3. הפרה שמקורה ברשלנות מכוונת של כללי החוק, כאשר ההפרה תוקנה בתוך 30 ימים ממועד גילויה. היקף הקנסות תחת קטגוריה זו הינו $10,000-50,000 פר הפרה ועד $250,000 לשנה.

7.2.4. הפרה שמקורה ברשלנות מכוונת של כללי החוק, כאשר לא נעשה כל ניסיון לתקן את ההפרה. היקף הקנסות תחת קטגוריה זו הינו $50,000 פר הפרה ועד $1,500,000 לשנה.

7.3. בנוסף, עובדי יישויות מכוסות ושותפים עסקיים עשויים להימצא אחראים באחריות פלילית, ולשאת בקנסות ותקופות מאסר כדלקמן:

7.3.1. קנס עד לסך של $50,000 ו/או עד שנת מאסר אחת, בשל הפרה שמקורה ברמת מודעות נמוכה להפרת החוק.

7.3.2. קנס עד לסך של $100,000 ו/או עד 5 שנות מאסר, בשל הפרה שבוצעה תוך מרמה.

7.3.3. קנס עד לסך של $250,000 ו/או עד 10 שנות מאסר, בשל גניבת מידע רפואי מוגן בכוונה למכור אותו, להעביר אותו או להשתמש בו למטרות הפקת רווח אישי, יתרון מסחרי או גרימת נזק בזדון.

7.3.4. אם במסגרת ההפרה בוצעה גניבת זהות, ניתן להחמיר את העונש הנקוב לעיל בשתי שנות מאסר נוספות.

8. <u>סיכום</u> –

8.1. אנו ממליצים לחברות ישראליות המתקשרות עם חברות אמריקאיות או שהינן בעלות גישה למידע רפואי על אודות אזרחי ארה"ב לבצע בדיקת תחולה של החוק, בין מכח דרישות הדין ובין מכח דרישה עסקית מצד הלקוחות שלהן.

8.2. אם החוק אכן חל על החברה, אנו ממליצים לבצע ניתוח פערים בין המצב השורר בחברה לבין החובות החלות עליהן מכוח החוק.

8.3. ציות לחוק ידרוש יישום של הנושאים הבאים:

8.3.1. עדכון מסמכי מדיניות ונהלים פנימיים והטמעת בקרות אבטחת מידע נוספות נדרשות;

8.3.2. מינוי נושאי תפקיד;

8.3.3. הסדרת התקשרויות חוזיות עם שותפים עסקיים או יישויות מכוסות תחת הסכם שותף עסקי;

8.3.4. מיסוד הליכי טיפול בתלונות יחידים ובבקשות למימוש זכויותיהם.