מידעון חמישי: סוגיות משפטיות בתחום מאגרי מידע רפואי - חלק א' - במסגרת סדרת מידעונים בנושא נתוני עתק (ביג דאטה) במערכת הבריאות

נובמבר 4 , 2018

במסגרת סדרת המידעונים "נתוני עתק במערכת הבריאות", הצגנו מידע כללי אודות מערכת הבריאות בישראל, המבוססת על שילוב אלמנטים של כמות המטופלים[1] ,איכות מידע הבריאות הנצבר[2] וקישוריות בשרשרת הטיפול הרפואי[3]. הסברנו כיצד המדינה פועלת להגברת השימושים המשניים במידע בריאות ולקידום שיתופי פעולה בין ארגוני בריאות לבין גופי מחקר וחברות הזנק, כמו גם סקרנו את התוכנית הלאומית לבריאות דיגיטלית.

אל מול המהפכה שקורמת עור וגידים כיום בתחום הבריאות הדיגיטלית, נראה כי המסגרת הנורמטיבית והמעטפת החקיקתית בתחום הבריאות הדיגיטלית עדיין לוקה בחסר ואינה מדביקה את קצב ההתפתחות המהיר של התחום. לא בכדי נאמר בעבר על ידי המשנה לשעבר לנשיא בית המשפט העליון, השופט ד"ר מישאל חשין ז"ל, כי: "*המשפט והטכנולוגיה הם יצורים שונים, שבאים מעולמות שונים - והם הפכים... המשפט עניינו הסדר החברתי, מוסר צדק ויושר, ואילו ההתקדמות הטכנולוגית - מקורה בסקרנות והישגיות. המשפט מפגר אחר הטכנולוגיה, לעיתים במרחק ובזמן רבים מאוד* "[4].

במידעון זה נסקור את המצב החקיקתי בתחום הבריאות הדיגיטלית ושימושים במידע אישי ורפואי בארה"ב ובאירופה לאחריו נסקור את הדין הרלוונטי, הקיים כיום בישראל.

ארה"ב[5]

בשנת 1996 נחקק בארצות הברית חוק בשם Health Insurance Portability and Accountability Act הידוע בכינויו HIPAA. חוק זה ביסס לראשונה את הסטנדרט והדרישות להגנה על מידע רפואי והוא חל באופן כללי על כל מטפל רפואי וספק שירותי רפואה אשר עושה שימוש במידע בריאות בתצורה אלקטרונית.

חוק זה נחקק נוכח ההתפתחות של יישומיים טכנולוגיים ברפואה[6], אשר הביאו להתייעלות והנגשה של מערכות הבריאות, אך העלו את הצורך לחזק את אבטחת המידע הרגיש. מטרת הHIPAA- היא להגן על המידע הרפואי האישי של מטופלים בד בבד עם אימוץ טכנולוגיות חדשות לשיפור היעילות והאיכות של הטיפול הרפואי.

לפיכך, הHIPAA- מונחה מהעיקרון הכללי לפיו יש להגדיר ולהפחית את המצבים בהם נעשה שימוש במידע רפואי אישי, **הניתן לזיהוי** (בשפת החוק, protected health information, PHI – "**מידע בריאות מוגן**").

בהתאם להסדר שנקבע, הגופים הרלוונטיים[7] אינם רשאים לעשות שימוש במידע בריאות מוגן אלא **בהתאם לחוק** או אם **נושא המידע הסכים לכך בכתב**. יצוין כי החוק אינו מגביל את השימוש או החשיפה של מידע בריאות מותמם, דהיינו, שאינו מאפשר זיהוי או שאינו מספק בסיס סביר לזיהוי של פרט מסוים.

למעשה, הגופים הרלוונטיים יכולים לחשוף מידע בריאות מוגן במספר מצבים, כגון: (1) למטופל עצמו; (2) טיפול, תשלום, פעילויות הכרוכות בניהול מוסד רפואי; (3) מקרים בהם המטופל נותן הסכמה בלתי רשמית לגילוי המידע[8]; (4) גילוי ו/או שימוש של מידע בריאות מוגן המתרחש כתוצאה, או כתוצר לוואי משני, של שימוש מותר[9]; (5) מידע בריאות מוגן ממנו נגרעו משתנים אשר היו יכולים להביא לזיהויו של נושא המידע.

בעוד שחשיפת מידע בריאות מוגן מוגבלת למצבים מסוימים, לא קיימת הגבלה לגבי חשיפת מידע מותמם. החוק מתייחס גם לאפשרות זו ומציע שתי שיטות להתממת מידע בריאות (1) :(de-identification) קביעה על ידי מומחה מוסמך, בהתבסס על שיטות ועקרונות מדעיים, כי המידע בריאות אינו ניתן לזיהוי או שקיים סיכון מאוד נמוך לשימוש במידע בריאות לבדו או בשילוב עם מידע אחר לזיהוי נושא המידע; (2) הסרת פרטי זיהוי מסוימים (כגון שם מלא, תאריכים, מספרי טלפון ופקס, תמונות פנים, כתובות דוא"ל ועוד) כאשר גם שילוב המידע הנותר עם מידע אחר לא יוביל לזיהוי נושא המידע[10]. יצוין כי הוראות החוק אינן חלות על מידע מותמם, משום שהמידע כאמור אינו נחשב יותר למידע בריאות מוגן לאחר התממתו.

החוק קובע סנקציות כספיות ופליליות במקרים של אי ציות, ובמקרים מסוימים אף מאפשר עונש של 10 שנות מאסר .(!)

אירופה[11]

בשנת 2016 התקבלה באירופה אסדרה כללית של נושא הגנת הפרטיות במסגרת General Data Protection Regulation, המכונה GDPR, המחליפה דירקטיבה קודמת משנת 1995[12]. הGDPR - נחקק על מנת ליצור בין היתר, הרמוניזציה בחוקי פרטיות מידע באירופה וכן לחזק את ההגנה על פרטיות המידע. בדומה לתקנות הגנת הפרטיות (אבטחת המידע), התשע"ז-2017, גם הGDPR- נכנסו לתוקפן בחודש מאי האחרון.

הGDPR- קובע אסדרה של "שימוש" בכל "**מידע אישי** "**הנוגע לפרט באירופה**, אשר חלה על כל הארגונים האוספים, המשתמשים והמאחסנים מידע אישי אודות תושבי האיחוד האירופי, בין אם למשל, הארגון העושה שימוש במידע של הפרט מצוי באירופה ובין אם לאו.

ההגדרה של "**מידע אישי**" רחבה ונוגעת ל"כל מידע המתייחס לאדם מזוהה או הניתן לזיהוי"[13]. כך, בגדר "מידע אישי" נכלל גם מידע שניתן לזיהוי אותו באמצעות איסוף של מספר מקורות מידע או מידע שהותמם אך ניתן לאחזר אותו. לעומת זאת, מידע אנונימי, מספר רישום של חברה או כתובת מייל גנרית לא ייחשבו למשל כמידע אישי.

מטרת הGDPR- להגן על מידע אישי, ללא קשר לסוג הטכנולוגיה בה נעשה, וה- "**שימוש**" במידע כולל פעילויות מסוגים שונים, לרבות באופן ידני או אוטומטי, לרבות, איסוף, הקלטה, ארגון, אחסון, שידור, שימוש, ייעוץ, שילוב, השמדה ועוד. לפיכך, בהתאם ל,GDPR- שליחת הודעת דוא"ל שיווקית נופלת תחת הוראות החוק. לעומת זאת, שימוש הנעשה במסגרת פעילות של פרט למטרות פרטיות לחלוטין, הנעשות בביתו של אותו פרט, ובלבד שאין לה כל קשר לפעילות מקצועית או מסחרית, מוחרגת מהחוק.

לפי הGDPR- נדרשת שקיפות גדולה יותר כלפי נושאי המידע, והשימוש במידע האישי מותר רק אם הוא עומד באחד מהתנאים הבאים למשל: (1) נושא המידע נתן הסכמה חיובית מפורשת לכך; (2) עיבוד המידע נחוץ לביצועו של חוזה שנושא המידע הינו צד לו; (3) עיבוד המידע נחוץ כדי לציית לצורך עמידה במחויבות חוקית[14].

יתרה מכך, הGDPR- מטיל חובות מוגברות על גורמים המעבדים "מידע הקשור לבריאות" "מידע גנטי" ו"מידע ביומטרי", ושימוש במידע כזה יתאפשר רק כאשר: (1) נושא המידע נתן את הסכמתו המפורשת; (2) הדבר נחוץ למטרות של רפואה מונעת או תעסוקתית, עבור הערכת כשירות לעבודה של עובד, אבחון רפואי, מתן שירותי בריאות, טיפול או טיפול סוציאלי או ניהול של מערכות ושירותי בריאות או מערכות ושירותים סוציאליים; או (3) כאשר קיים עניין לציבור בתחום בריאות הציבור[15].

הרגולציה של הGDPR- קובעת סנקציות כספיות כבדות במקרים של אי ציות, והקנסות עשויים להאמיר עד ל20- מיליון אירו או 4% מהמחזור העולמי השנתי, הגדול מביניהם.

ישראל

כפי שנבהיר להלן, החקיקה בישראל מסדירה בעיקר את נושא הגנת הפרטיות באופן כללי[16].

למעשה, טרם הוגדר הסדר כולל, בתחום של מידע רפואי או בריאות דיגיטלית, לפיו יוכלו לפעול באופן אחיד ומוסדר ארגוני הבריאות, גופי המחקר, חברות ההזנק והחוקרים העצמאיים, בבואם לעשות שימוש במידע בריאות ציבורי או לשתף פעולה עם מערכת הבריאות.

בהתאם לחוק הגנת הפרטיות, תשמ"א-1981, מאגר מידע הינו אוסף של נתוני מידע, המוחזק באמצעי מגנטי או אופטי והמיועד לעיבוד ממוחשב, למעט אוסף לשימוש אישי או שאינו למטרות עסק או אוסף הכולל רק שם, מען ודרכי התקשרות[17]. בהתאם לחוק, אין לנהל או להחזיק מאגר מידע בעל "מידע רגיש"[18] אלא אם המאגר נרשם בפנקס, והוא עומד בתנאי החוק

והתקנות.

לאחרונה הותקנו תקנות הגנת הפרטיות (אבטחת מידע), התשע"ז,2017- הנוגעות לאבטחת מידע במאגרי מידע, עליהן דיווחנו בסמוך לכניסתן לתוקף[19]. תקנות אלו חלות באופן גורף ומחייב על כל מאגר מידע המוגדר בחוק, הן במגזר הציבורי והן במגזר הפרטי, בין אם מאגר המידע רשום ובין אם לאו.

התקנות מגדירות שלוש רמות אבטחה אשר יש ליישם על מאגרי מידע בהתאם לסוג המאגר, תוכנו או היקפו – רמת אבטחה בסיסית, רמת אבטחה בינונית ורמת אבטחה גבוהה. התוספת הראשונה לתקנות קובעת כי מאגרי מידע הכוללים "מידע רפואי או מידע על מצבו הנפשי של אדם", "מידע גנטי כהגדרתו בחוק מידע גנטי, התשס"א"2000- או "מידע ביומטרי" הינם מאגרי מידע שחלה עליהם רמת האבטחה הבינונית, ועל כן על המנהלים את המאגרים הללו חלה חובת אבטחה מוגברת יחסית לרמת האבטחה הבסיסית.

נכון למועד כתיבת מידעון זה, לא נחקקה עדיין בישראל חקיקה ראשית המאסדרת את תחום העיסוק בנתוני עתק בתעשיית הבריאות, מעבר לאסדרה שמתחום דיני הגנת הפרטיות אותה סקרנו לעיל. את החלל החקיקתי הזה ממלאים, במידה חלקית, הנהלים של משרד הבריאות המתווים את גבולות הגזרה בשימוש משני במידע בריאות ושיתופי פעולה[20]. השילוב של חוזרים אלה, ביחד עם דיני הגנת הפרטיות, מהווה נקודת המוצא לבחינה האסדרה הכוללת בתחום השימוש במאגרי מידע הכוללים מידע אישי ואו רפואי בישראל.

מעבר לכך, סוגיות משפטיות רבות עשויות להתעורר בעת שימוש משני במידע בריאות כמו גם בעת יצירת שיתופי פעולה המבוססים על שימושים משניים, ונוגעות בין היתר, לתחום הקניין הרוחני או האתיקה. כך למשל, שאלות מורכבות עולות באשר לבעלות על מידע הבריאות, התמורה שניתן לקבל בגין מתן גישה למידע, אם בכלל, האופנים להעברת המידע והגורמים אליהם מותר להעביר את המידע, האופן בו ייעשה שימוש נוסף במידע על ידי אותם גורמים נעברים וכיוצ"ב. כל אלה אינם מוסדרים בחקיקה או בכלל והדבר יוצר אי וודאות הן במגזר הפרטי והן במגזר הציבורי.

במידעון הבא נסקור מספר סוגיות משפטיות מרכזיות אלו.

לקריאת המידעון הראשון: מבנה מערכת הבריאות בישראל ומידע כללי לגבי מאגרי מידע
לקריאת המידעון השני: שימושים (ראשוניים ומשניים) במידע בריאות
לקריאת המידעון השלישי: שיתופי פעולה בהעברה של מידע בריאות
לקריאת המידעון רביעי: התוכנית הלאומית לקידום שימושים ושיתופי פעולה בהעברת מידע בריאות

ערן ברקת
עורך דין, שותף בכיר

ערן ברקת הינו שותף בכיר
בגילת, ברקת ושות'

חן בן דורי - אלקן
עורכת דין, שותפה

חן בן דורי- אלקן הינה שותפה
בגילת, ברקת ושות'

אלכסנדרה כהן
עורכת דין

אלכסנדרה כהן הינה עורכת דין
בגילת, ברקת ושות'

[1] כלל תושבי מדינת ישראל מבוטחים, ולכן השירותים ניתנים על ידי כמות מצומצמת של ספקים.

[2] תיעוד המידע הרפואי הנאגר במאגרי המידע של ארגוני הבריאות מאפשר עומק ורצף טיפולי.

[3] מספר תעודת הזהות מקשר בין כל הנתונים הרפואיים של אדם מסוים.

[4] הדברים נאמרו במסגרת כנס בנושא משפט וטכנולוגיה באוניברסיטת תל אביב בשנת 2006: http://www.news1.co.il/Archive/001-D-369673-00.html

[5] ר' אתר HHS.GOV, של שירותי בריאות ארה"ב (U.S. Department of Health & Human Services) https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/summary/privacysummary.pdf

[6] לרבות העברות מידע ממחושב, ושימוש במידע ממוחשב ובמאגרי מידע בריאות.

[7] עליהם חל החוק HIPAA.

[8] בין אם התבקש לתת הסכמתו ישירות, או שמדובר בנסיבות בהן ברור כי המטופל יכול היה להסכים או לא להסכים לגילוי. במקרים בהם לא ניתן לתקשר עם המטופל (כגון מצבי חירום, מקרים בהם המטופל הינו נכה או לא מסוגל לתקשר מסיבה אחרת) ניתן לגלות ו/או להשתמש במידע לפי שיקול הדעת, אם ברור כי השימוש הוא למען אינטרס המטופל.

[9] כל עוד הגוף המגלה נקט באמצעי הגנה מתאימים ושהמידע שגולה היה המינימום שנדרש לגלות.

[10] להרחבה, ר' https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html

[11] https://ec.europa.eu/commission/priorities/justice-and-fundamental-rights/data-protection/2018-reform--u-data-protection-rules_en

[12] Regulation וDirective- הן שניהם מעשי חקיקה של האיחוד האירופי. ההבדל ביניהן הוא הRegulation- חלה במישרין במדינות החברות, כחוק של אותה מדינה ואילו דירקטיבה אינה חלה במישרין, אלא מקימה חובה למדינות החברות ליישמה בחקיקה מקומית.

[13] באופן ישיר או עקיף על ידי מאפיין מסוים כגון, שם, מספר זהות, מידע הנוגע למיקום, מזהה מקוון או מאפיין כלשהו הקשור לזהותו פיזית, פסיכולוגית, גנטית/נפשית, כלכלית, תרבותית, חברתית של אותו אדם.

[14] ר' https://gdpr-info.eu/art-7-gdpr/

[15] כגון הגנה נגד סכנות בריאותיות חוצות גבולות או הבטחה של סטנדרטים גבוהים של איכות ובטיחות של טיפול רפואי ותרופות. ר' סעיף 9 ל-GDPR
https://gdpr-info.eu/art-9-gdpr/

[16] ר' למשל נספח לחוזר מנכ"ל משרד הבריאות בנושא "שימושים משניים במידע בריאות".

[17] כאשר האוסף שכשלעצמו אינו יוצר איפיון שיש בו פגיעה בפרטיות לגבי בני האדם ששמותיהם כלולים בו, ובלבד שלבעל האוסף או לתאגיד בשליטתו אין אוסף נוסף.

[18] מידע רגיש מוגדר בסעיף 7 לחוק כנתונים על אישיותו של אדם, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, דעותיו ואמונתו.

[19] ר' מידעון מיום 6 במאי 2018: https://bit.ly/2OoUzI9

[20] ר' מידעון שני ושלישי לסדרת מידעונים זו.