המכון הישראלי לדמוקרטיה

www.idi.org.il

מר אמיר אלשטיין
יו"ר הוועד המנהל
מר יוחנן פלסנר
נשיא
מר ברנרד מרכוס
יו"ר בינלאומי
פרופ' גרהרד קספר
יו"ר המועצה הבינלאומית
ד"ר ג'ורג' שולץ
יו"ר של כבוד

חברי הוועד המנהל
פרופ' ורד וניצקי-סרוסי
מר חן ליכטנשטיין
גב' מזל מועלם
מר סלי מרידור
עו"ד אבי פישר
מר אביעד פרידמן
ד"ר מיכל צור
מר יוסי קוצ'יק
מר עימאד תלחמי

המועצה הבינלאומית
השופטת רוזלי סילברמן אבלה, קנדה
מר אליוט אברמס, ארה"ב
ד"ר מרטין אינדיק, ארה"ב
גב' אן אפלבאום, ארה"ב
פרופ' ורנון בוגדנור, בריטניה
השופטת דורית בינישׁ, ישראל
השופט סטיבן ברייר, ארה"ב
השופט סלים ג'ובראן, ישראל
ד"ר איימי גוטמן, ארה"ב
ד"ר ג'וזף ג'וֹפה, גרמניה
פרופ' רונלד דניאלס, ארה"ב
פרופ' משה הלברטל, ישראל
פרופ' מייקל וולצר, ארה"ב
פרופ' רוברט מנוקין, ארה"ב
פרופ' כריסטוף מרקשיס, גרמניה
השופט אברהם סופר, ארה"ב
מר ברט סטפנס, ארה"ב
פרופ' ארווין קוטלר, קנדה
פרופ' יהודה ריינהרץ, ארה"ב
פרופ' גבריאלה שלו, ישראל

סגני נשיא
ד"ר ישי [ג'סי] פרס, אסטרטגיה
פרופ' קרנית פלוג, מחקר
פרופ' יובל שני, מחקר

עמיתים בכירים
פרופ' תמר הרמן
פרופ' מוסטפא כבהא
פרופ' עמיחי כהן
פרופ' יותם מרגלית
פרופ' עליה פישר
פרופ' יובל פלדמן
פרופ' מרדכי קרמניצר
פרופ' גדעון רהט
ד"ר תהילה שוורץ אלטשולר
פרופ' ידידיה צ' שטרן
פרופ' איתן ששינסקי

מייסד ונשיא לשעבר
ד"ר אריק כרמון

נספח לחוות הדעת : תזכיר טיוטת תקנות זכויות החולה (שימוש מחקרי במידע בריאות), התש"פ – 2019

עו"ד רחל ארידור הרשקוביץ

נספח א: התממה, זיהוי חוזר ומחקר בנתוני עתק

התממה בנתוני עתק ניצבת מול שני אתגרים מרכזיים ומנוגדים. האחד, הקושי להגדיר מהי רמת ההתממה הראויה, מתוך הבנה שהתממה המתמקדת רק בהסרת פרטי מידע מזהים ישירים של נשוא המידע כגון שם, מספר תעודת זהות וכתובת מגורים, מתעלמת מקיומם של פרטי מידע "כאילו מזהים" רבים. אלו הם נתונים על נושא המידע כמו למשל מידע דמוגרפי, תאריכים, ומשתנים סוציואקונומיים אשר מאפשרים זיהוי עקיף של נושא המידע באמצעות הצלבתם. האתגר השני נוגע לכך שהתממה שבמהלכה מסירים פרטי מידע רבים עלולה לפגוע ביעילות וחדשנות המחקר בנתוני עתק.[1]

1. טכניקות מקובלות להתממה:

(1) הסרת פרטי מידע: מחיקה מוחלטת של פרטי מידע מסויימים ממאגר המידע, בדרך כלל פרטי מידע מזהים. חסרונה של טכניקה זו נעוץ בחוסר התאמתה למאגרי המידע שאינם מובנים. כך, למשל, מאגרי מידע רפואיים נחשבים על פי רוב למאגרים לא מובנים שכן המידע הרפואי מפוזר בסיכומי הביקורים אצל הרופא, סיכומי אישפוז, בדיקות וכו' ויכול לעיתים להירשם בכתב יד או בפורמט לא אחיד. כתוצאה מכך קשה להבטיח את מחיקת כל הפרטים הדרושים ומציאתו של פרט שנשכח בטעות עלולה להוביל לזיהוי נושא המידע.[2]

---

[1] Jordi Soria-Comas & Josep Domingo-Ferrer, Big Data Privacy: Challenges to Privacy Principles and Models, 1(1) Data Sci. Eng. 21, 23 (2016); *Boris Lubarsky,* Re-Identification of Anonymized Data", 1 Geo. L. Tech. Rev. 202, 203 (2017).

[2] *Boris Lubarsky,* Re-Identification of Anonymized Data", 1 Geo. L. Tech. Rev. 202, 203 (2017).

(2) <u>החלפת פריט מידע בכינוי.</u> בטכניקה זו מוחלפים פרטי מידע מזהים בכינוי באופן רנדומלי או מכוון, כאשר הערך האמיתי נשמר באופן מאובטח וכך מתאפשר זיהוי חוזר במידת הצורך. חסרונה של טכניקה זו נעוץ גם כן בחוסר התאמתה למאגרי מידע שאינם מובנים, כדוגמת מאגרי מידע רפואיים. בנוסף, כאשר הכינוי נקבע על ידי אלגוריתם ואינו מחליף רנדומלית פריט מידע מזהה, די בהבנת האלגוריתם כדי להביא לזיהוי חוזר. כך למשל, בשנת 2014 נציב המוניות והלימוזינות בניו יורק פרסם דו"ח המפרט את כלל הנסיעות ברכבים אלו בניו יורק באותה השנה. מספר רישיון הנהיגה של הנהג ומספר המונית או הלימוזינה הוחלפו בכינוי. אולם בלוגרים הצליחו לבצע זיהוי מחדש של נתונים אלו לאחר שלמדו את אלגוריתם הקצאת הכינויים.[3]

(3) <u>הוספת רעש סטטיסטי:</u> בטכניקה זו נהוג להוסיף פרטי מידע פיקטיביים למאגר. יעילותה של טכניקה זו מוטלת כיום בספק נוכח קיומן של טכנולוגיות טובות למדי להסרת רעשים במאגרי מידע.[4]

(4) <u>רנדומיזציה</u>: התאמת שינוי רנדומלי זהה לכל נושאי המידע (למשל הוספה או הסרה של אותו מספר ימים מתקופות האישפוז).

(5) <u>ערבוב (Shuffling):</u> טכניקה זו מיושמת בשני אופנים. האחד, ערבוב הנתונים המזהים בין נושאי מידע שונים. כך נושא מידע יקושר במאגר למידע מזהה שאינו עליו; השני, ערבוב מאפיינים. כלומר, ארגון מחדש של הערכים בשדה אחד מחדש. למשל במקום שם משפחה סמית ירשם תמיס.

(6) <u>מיסוך מאפיינים:</u> החלפת אותיות או תווים בשדה ב"*". למשל החלפת שתי האותיות האחרונות בשם המשפחה בכוכביות.

(7) <u>קיצוץ (Truncation):</u> הסרת התווים האחרונים במילה (למשל 3 האותיות האחרונות בשם המשפחה).

---

[3] *Boris Lubarsky,* Re-Identification of Anonymized Data", 1 Geo. L. Tech. Rev. 202 (2017).

[4] Khaled EL Eman, *Perspectives on Health Data De-Identification, Privacy Analytics*.

(8) <u>הצפנה (Encoding)</u>: החלפת הערך בערך אחר חסר משמעות. חסרונה של שיטה זו הוא בקלות הזיהוי החוזר במקרה שמדובר במאגר מידע המהווה מדגם מייצג של האוכלוסייה. במקרה כזה, למשל, אפשר לנחש מה שם המשפחה שהוחלף בערך חסר משמעות, בהתאם למידת חזרתו במאגר התואמת את מידת הפופולריות שלו באוכלוסייה.[5]

(9) <u>K-anonymity</u>: טכניקת התממה זו מבוססת על ההבנה שהסרת פרטי מידע כמעט מזהים מסוימים עלולה לפגוע ביעילות המחקר. למשל, כאשר חוקר מבקש לבדוק את הקשר בין משקל עודף למחלת הסרטן, הסרה מלאה של הנתונים על משקל המטופלים תפגע באפשרות ביצוע מחקר כאמור. אולם מנגד, השארת פרטים על סוג המחלה ומשקל החולה עשויה להביא לזיהוי חוזר של נושא המידע על ידי אדם המחפש נושא מידע ספציפי במאגר המידע, יודע שהוא נמצא באותו מאגר ויודע גם שהוא סובל מעודף משקל. לכן במקום להסיר לחלוטין את פרטי המידע הכמעט מזהים, טכניקת K-anonymity מכלילה אותם באופן מובנה, כך של-K אנשים יש ערכים זהים מלבד הערך הרגיש. באופן זה מתקבלות במאגר המידע קבוצות שעדיין מאפשרות ניתוחים סטטיסטיים יעילים אך מסתירות פרטי מידע רגיש. הכללה מתאפשרת למשל באמצעות החלפת תאריך לידה בטווח גילאים או עיר מגורים באיזור גאוגרפי.[6] ככל ש-K גבוה יותר הסבירות לזיהוי חוזר נמוכה יותר, אולם גם יעילות המידע לצרכיי מחקר עשויה להיות נמוכה יותר ועלולים להוביל למחקר שתוצאותיו מוטות או חסרות.[7]

<u>דוגמא:</u> מאגר מידע של מטופלים המאושפזים בבית חולים דמיוני כלשהו, הכולל 10 אנשים ו-7 פרטי מידע על כל אחד מהם, ייראה כך:

---

[5] *Boris Lubarsky,* Re-Identification of Anonymized Data", 1 Geo. L. Tech. Rev. 202 (2017).

[6] Karim Abouelmehdi, Abderrahim Beni-Hessane and Hayat Khaloufi, Big healthcare data: preserving security and privacy, Big Data (2018) 5:1, עמ' 1-12.

[7] Karim Abouelmehdi, Abderrahim Beni-Hessane and Hayat Khaloufi, *Big Healthcare Data: Preserving Security and Privacy*, 5(1) Big Data (2018); Andrea Krusten, *Going beyond masking: how to anonymize large data sets*, SAP BLOG (Jan. 28, 2018).

שם	גיל	מין	עיר מגורים	דת	משקל	מחלה
דרק	29	זכר	אילת	נוצרי	96	סרטן
רוחמה	24	נקבה	באר שבע	יהודי	60	וירוס
מוחמד	28	זכר	רהט	מוסלמי	74	מחלת לב
נורית	27	נקבה	חיפה	יהודי	65	בריאה
ג'ון	24	זכר	נצרת	נוצרי	85	מחלת לב
לאה	18	נקבה	קרית מלאכי	יהודי	62	סרטן
ג'ורג'	19	זכר	תל אביב	נוצרי	77	מחלת לב
עומר	24	זכר	כאבול	מוסלמי	74	וירוס
שמעון	29	זכר	אילת	יהודי	78	סרטן
ספא	17	נקבה	יפו	מוסלמי	63	מחלת לב

לאחר הסרת שם נושא המידע ודתו, הופעלה גם טכניקת k-Anonimty כך שפרטי מידע כמעט מזהים של גיל, מיקום ומשקל הוכללו ונוצרו שתי קבוצות נושאי מידע בהתאם לשני טווחי גיל:

שם	גיל	מין	אזור מגורים	דת	משקל	מחלה
**	20<גיל<30	זכר	אזור הדרום	**	96	סרטן
**	20<גיל<30	נקבה	אזור הדרום	**	60	וירוס
**	20<גיל<30	זכר	אזור הדרום	**	74	מחלת לב
**	20<גיל<30	נקבה	אזור הצפון	**	65	בריאה
**	20<גיל<30	זכר	אזור הצפון	**	85	מחלת לב
**	20>גיל	נקבה	אזור הדרום	**	62	סרטן
**	20>גיל	זכר	אזור המרכז	**	77	מחלת לב
**	20<גיל<30	זכר	אזור הצפון	**	74	וירוס
**	20<גיל<30	זכר	אזור הדרום	**	78	סרטן
**	20>גיל	נקבה	אזור המרכז	**	63	מחלת לב

K עבור נתוני הגיל, אזור המגורים והמין הוא 2, משום שבכל שילוב אפשרי של הנתונים בכל שורה בטבלה יש לפחות אותם פרטי מידע זהים בשתי שורות לפחות בטבלה.[8]

מודל k-anonymity מתמקד באוסף מידע "כאילו מזהה" סטטי אחד ובכך נעוצה חולשתו. במציאות נתוני העתק אפשר להצליב אוספים של "כאילו מזהים" ממקורות שונים, שיש מספר פרטי מידע משותפים בניהם, וכך להגיע לזיהוי חוזר של נושא מידע המופיע בכל אחד מאוספי המידע ה"כאילו מזהים".[9]

(10) l-Diversity: טכניקת התממה זו פותחה כשיפור לטכניקת K-anonymity. לפי טכניקה זו בכל קבוצה של K אנשים יכללו L פרטי מידע שונים בעמודת המידע אותו מבקשים להתמים. המטרה היא למנוע ככל האפשר קיום של קבוצות זהות עם שונות מעטה בפרטי המידע. בטבלה שלעיל, למשל, יש לוודא שבכל שתי שורות המציגות זהות בעמודות הגיל, המין ואזור המגורים תהא L שונות בעמודת המחלה (L צריך להיות קטן או שווה ל-k; בדוגמה שלנו L צריך להיות 2).

חסרונה של טכניקת L-Diversity בא לידי ביטוי כאשר יש שונות נמוכה בקרב נושאי המידע במאגר בנוגע לפרט המידע אותו מבקשים להתמים. במקרה זה יש צורך בשילוב פרטי מידע פיקטיביים, כלומר הוספת רעש. עם זאת, קיימות כיום טכנולוגיות טובות למדי להסרת רעשים במאגרי מידע.[10]

(11) T-Closeness: טכניקת התממה זו נחשבת לשיפור נוסף של טכניקות L-diversity ו K-anonymity. לפי טכניקה זו יש לבצע מחדש את שיטת K-anonymity באופן שיבטיח כי L השונות בעמודת המידע הרגיש תהיה קרובה או זהה להתפלגות המידע הרגיש בכלל האוכלוסייה. למשל, אם

---

[8] *Arvind Narayanan & Vitaly Shmatikov, Robust De-Anonymization of Large Datasets (How to Break Anonymity of the Netflix Prize Dataset) (2008)*

[9] Jordi Soria-Comas & Josep Domingo-Ferrer, Big Data Privacy: Challenges to Privacy Principles and Models, 1(1) Data Sci. Eng. 21-28 (2016)

[10] Khaled EL Eman, *Perspectives on Health Data De-Identification, Privacy Analytics*.

10% מהאוכלוסייה חולים בסרטן, אזי לאחר ההתממה בטכניקות האמורות הטבלה צריכה לשקף את המצב שבכל קבוצת K אנשים מופיעים רק 10% החולים בסרטן.[11] אולם גם בשיטה זו ככל שכמות ומגוון המידע במאגר עולה הסיכוי לזיהוי חוזר עולה.

(12) <u>פרטיות דיפרנציאלית (Differential Privacy):</u> בטכניקה זו מאגר המידע הכולל פרטי מידע מזהים וכאילו מזהים מוחזק במלואו על ידי גורם שניתן בו אמון. גורם זה מקבל שאילתות חיפוש ומשיב תשובות רנדומליות תוך הוספת "פרטי רעש" באופן מתמטי לנתונים ומבלי לפגוע באמינות התשובות. החוקר אינו יכול לראות את המידע הגולמי או את המידע המותמם, אלא רק יכול לשאול שאלות את מאגר המידע.

היישום של טכניקת הפרטיות הדיפרנציאלית מורכב יחסית וניתן לעשות בה שימוש רק על מאגרי מידע מספיק גדולים. ככל שיש יותר מידע רגיש יש להכניס לפי המודל יותר רעש ולכן עלות היישום גבוהה יותר.[12] בנוסף, יעילותה של שיטה זו תלויה לחלוטין בחישוב כמו הרעש הנדרשת. אם בעל המאגר יכשל בחישוב הרעש תכשל ההתממה על בסיס שיטה זו.[13]

2. <u>שיטות לזיהוי חוזר</u>

לצד טכניקות ההתממה המקובלות יש לתת את הדעת גם לשיטות המקובלות לפריצת ההתממה, כלומר לזיהוי חוזר:

(1) <u>התממה בלתי מספקת (insufficient de-identification):</u> כאשר פרט מידע מזהה או כאילו מזהה מושאר במאגר המידע, בטעות או בשל אי הבנת הפוטנציאל לזיהוי חוזר באמצעותו. למשל, מדינת מסצ'וסטס

---

[11] *Opinion 05/2014 on Anonymisation Techniques*, **לעיל** ה"ש **שגיאה! הסימניה אינה מוגדרת.**; Ninghui Li, Tiancheng Li, & Suresh Venkatasubramanian, *t-closeness: Privacy Beyond k-anonymity and l-Diversity*, 2007 IEEE 23RD INTERNATIONAL CONFERENCE ON DATA ENGINEERING (2007)

[12] Jordi Soria-Comas & Josep Domingo-Ferrer, Big Data Privacy: Challenges to Privacy Principles and Models, 1(1) Data Sci. Eng. 21-28 (2016)

[13] Karim Abouelmehdi, Abderrahim Beni-Hessane and Hayat Khaloufi, Big healthcare data: preserving security and privacy, Big Data (2018) 5:1, עמ' 12-10.

פירסמה דיווח אודות הביקורים של כל עובדי המדינה בבית חולים. מושל המדינה הבטיח שאין סיבה לדאגה שכן הנתונים הותממו. סטודנטית לתואר שני הצליחה באמצעות חיפוש אחר מושל המדינה לפי מינו, גילו והמיקוד של מקום מגוריו לחשוף את כל התיעוד הרפואי שלו מהמאגר.[14] ככלל, נמצא שניתן לזהות 63% מאוכלוסיית ארה"ב במאגרי מידע המפורסמים בציבור באמצעות הצלבת גיל, מין ומיקוד.[15]

(2) <u>הנדסה לאחור של הכינוי (pseudonym reversal):</u> ככל שנעשה שימוש באותו כינוי לאותו נושא מידע אזי יהיה קל יותר לבצע זיהוי חוזר. כאשר מדובר במאגר מידע המהווה מדגם מייצג של האוכלוסייה תיתכן חשיפה של פרטי מזהה על יד השוואת תפוצת הכינוי במאגר מידע לתפוצת הנתון באוכלוסייה, למשל כאשר מדובר בשם משפחה. בנוסף, במידה שנחשפת שיטת קביעת הכינוי אזי ניתן יהיה לזהות מחדש את כל המידע שהותמם באותה השיטה.[16]

(3) <u>הצלבת מקורות מידע ומאגרי מידע שונים:</u> זו השיטה המקובלת והטובה ביותר לזיהוי חוזר בעיקר במציאות של נתוני עתק המאופיינים בכמויות גדולות של מידע אישי זמין וביכולות עיבוד משופרות וזולות יחסית. במקרה של המידע הרפואי במדינת מסצ'וסטס הצליבה החוקרת את המידע הרפואי עם פנקס הבוחרים הזמין לרכישה. בדרך זו היא מצאה את המיקוד של המושל ותאריך הלידה שלו והצליבה נתונים אלו כדי לאתר אותו במאגר המידע הרפואי.[17] חוקרים אף הראו שבאמצעות מידע המצוי במאגרי מידע חינמיים באינטרנט ועל בסיס ההנחה ששם המשפחה מועבר מאב לבנו

---

[14] *Boris Lubarsky,* Re-Identification of Anonymized Data", 1 Geo. L. Tech. Rev. 202 (2017)

[15] *Boris Lubarsky,* Re-Identification of Anonymized Data", 1 Geo. L. Tech. Rev. 202, 203 (2017).

[16] *Boris Lubarsky,* Re-Identification of Anonymized Data", 1 Geo. L. Tech. Rev. 202 (2017)

[17] *Boris Lubarsky,* Re-Identification of Anonymized Data", 1 Geo. L. Tech. Rev. 202 (2017)

בדיוק כמו כרומוזום Y, ניתן להצליב שם משפחה, שנת לידה ומדינת מגורים ולזהות נושאי מידע במאגר מידע גנטי מותמם.[18]

[18] Melissa Gymrek, Amy L. McGuire, David Golan, Eran Halperin and Yaniv Erlich, *Identifying Personal Genomes by Surname Interferences,* 339 SCIENCE 321 (Jan. 18, 2013).

נספח ב: רקע השוואתי

שימוש במידע רפואי לצורך מחקר בנתוני עתק – הסדרים באיחוד האירופי, ארה"ב, אוסטרליה ופינלנד

1. האיחוד האירופי

המחוקק האירופי הכיר בחשיבותו החברתית והכלכלית של מחקר העושה שימוש במידע אישי ובצורך לעודד חדשנות במדינות האיחוד האירופי ועל כן עיגן בתקנות החדשות להגנה על פרטיות במידע באיחוד האירופי (להלן: "**GDPR**")[19] הסדר המתיר ביצועו של מחקר כאמור למטרות מדעיות, רפואיות או סטטיסטיות, גם במחיר של פגיעה מסוימת בזכות לפרטיות.[20] בכך משתקפת תפיסתו של המחוקק האירופי שאומנם מעדיף לאפשר מחקר, לרבות מחקר רפואי בנתוני עתק, נוכח יתרונותיו החברתיים והכלכליים על פני הגנה מלאה על הזכות לפרטיות, אך עדיין מכיר בזכות לפרטיות ובחשיבותה ולכן קובע דרישות שמטרתן למזער את הפגיעה בה.[21]

המונח "מחקר" (research) אינו מוגדר במפורש ב-GDPR. בסעיפי ההקדמה מוסבר שמחקר למטרה סטטיסטית משמעו **איסוף ועיבוד מידע אישי הדרוש לסקרים סטטיסטיים או להפקת תוצאות סטטיסטיות, אשר עשויות לשמש בעתיד בסיס למחקר מדעי**. ככלל, תוצאותיו של מחקר סטטיסטי אינן מידע אישי אלא מידע אגרגטיבי.[22] מחקר מדעי, לפי דברי ההקדמה, יפורש בהרחבה ככולל למשל פיתוח טכנולוגי, מחקר יסוד, מחקר במימון פרטי ומחקר המבוצע לטובת הציבור בתחום בריאות הציבור.[23]

---

[19] The General Data Protection Regulation (EU) 2016/679 (להלן: "**GDPR**").

[20] סעיף 157 להקדמה ל-GDPR מפרט את התועלות הנלוות למחקר במידע אישי, לרבות האפשרות שהמחקר יוביל לגילויים רפואיים חדשים שעל בסיסם ניתן להביא לשיפור באיכות החיים של ציבורים מסויימים ולשפר את יעילות השירותים החברתיים.

[21] Michael Birnhack, *A Process-Based Approach to Informational Privacy and the Case of Big Medical Data,* 20 THEORETICAL INQUIRIES L. XX 2 (2019).

[22] סעיף 162 להקדמה ל-GDPR.

[23] סעיף הקדמה 159 ל-GDPR.

לפי הסדר זה, במידה שהמבקש לעבד מידע אישי לצרכי מחקר מיישם אמצעי אבטחה מתאימים, טכניים וארגוניים, המבטיחים שלא יעובד מידע מעבר לנחוץ להגשמת המטרה,[24] הוא רשאי לעבד מידע אישי ללא הסכמת נושא המידע על בסיס אינטרס לגיטימי של בעל השליטה במידע;[25] הוא רשאי לעבד את המידע האישי למטרות מחקר, אף אם זו מטרה משנית ואינה המטרה הראשונית שלשמה נאסף המידע האישי מלכתחילה, וכן הוא פטור מהמגבלות המוטלות על עיבוד מידע רגיש,[26] מהחובה להפסיק את עיבוד המידע האישי בעקבות התנגדותו של נושא המידע או מהחובה להיענות לבקשת נשוא המידע למחוק מידע אישי עליו מהמאגר.[27]

באשר לדרישת ההודעה,[28] ה-GDPR מכיר בקושי להגדיר במדויק ומראש את מטרת המחקר. בניגוד למחקר מסורתי שבו מניח החוקר הנחה מראש ובוחן את היתכנותה בשלב המחקר, במחקר בנתוני עתק החוקר מחפש קורלציות שמתגלות מעיבוד המידע ללא הנחת מוצא ספציפית. משום כך, אין החוקר יודע מראש לאפיין את היקף מחקרו ומטרתו. על כן, מקל ההסדר הקבוע ב-GDPR על חוקר במחקר מדעי ומאפשר לו לציין בהודעה רק את תחומי המחקר, פוטר את החוקר מהצורך במתן הודעה במידה שהוא מבסס את מחקרו על מידע אישי שהגיע לידיו שלא

---

[24] סעיפים 89(1) ו-5(e) ל-GDPR.

[25] סעיף 6(f)(1) וסעיפי הקדמה 47 ו-157 ל-GDPR: כאשר המחקר הוא המטרה הראשונית לשמה מבוקש המידע האישי הרי הוא יכול להיחשב אינטרס לגיטימי של בעל שליטה במידע שהינו חברה פרטית. במסגרת זו רשאי בעל השליטה במידע לעבד את המידע האישי ללא הסכמת נושא המידע ובלבד שזכויות יסוד של נושא המידע אינן גוברות על האינטרס הלגיטימי של בעל השליטה במידע או צד שלישי. האיזון בין האינטרס הלגיטימי של בעל שליטה במידע או צד שלישי לבין זכויות יסוד של נשוא המידע הוא תלוי הקשר ונסיבות: האיזון יבוצע על בסיס הערכת הציפייה הסבירה של נושא המידע בהתבסס על מערכת היחסים בינו לבין בעל השליטה במידע ובנסיבות המקרה. כאשר בעל השליטה במידע הוא חברה ציבורית באפשרותה לעבד מידע אישי ללא הסכמת נושא המידע לפי סעיף 5(e) ל-GDPR ובלבד שהעיבוד הוא לטובת אינטרס הציבור ונעשה באישור המדינה.

[26] סעיף 9(2)(j) וסעיף 52 להקדמה ל-GDPR מתיר עיבוד מידע רגיש למטרות מחקר באופן מידתי, בהתאם לסעיף 89(1), בהתבסס על חוק מדינתי ותוך נקיטת אמצעים מספיקים לאבטחת זכויות יסוד ואינטרסים של נושא המידע.

[27] סעיף 5(1)(b) ל-GDPR קובע שעיבוד משני למטרות אירכוב או מחקר סטאטיסטי בהתאם לסעיף 89(1) ל-GDPR לא יחשב כמפר את דרישת קיום המטרה, כלומר לא יחשב כבלתי תואם למטרה המקורית לשמה נאסף המידע.

[28] לפי סעיפים 12(1) ו-13(2) ל-GDPR בעת איסוף מידע אישי על בעל שליטה במידע לספק לנושא המידע הודעה הכוללת את פרטיו של בעל השליטה במידע, הסבר על מטרת עיבוד המידע, ציון האם המידע האישי צפוי לעבוד לידי צדדים שלישיים מחוץ למדינות האיחוד האירופי, מידע על זכויות נושא המידע ופירוט פרק הזמן או הקריטריונים לפיהם יקבע פרק הזמן במהלכו ישמר המידע בידי בעל השליטה במידע.

מנושא המידע, וזאת כאשר מתן ההודעה יטיל נטל לא מידתי על בעל השליטה במידע או כאשר סביר שמתן ההודעה יסכל את מטרות המחקר, ובלבד שהחוקר מיישם אמצעי אבטחה מתאימים לרבות מתן הודעה בציבור.[29] ציות לכללי אתיקה המוכרים במחקרים מדעיים, עשוי להיחשב כעמידה בדרישת הטמעת אמצעי אבטחה טכניים וארגוניים מתאימים,[30] כמו גם שימוש בטכניקת מיסוך על ידי כינוי (pseudonymization) במסגרתה מוחלפים פרטי מידע מזהים בכינויים.[31] עם זאת, מידע אישי שהוחלף בכינוי נותר כפוף למגבלות הקבועות ב-GDPR ואינו נחשב מידע מותמם. לצד ההקלות האמורות ממימוש חלק מזכויותיו של נושא המידע לפי ה-GDPR **מטיל ה-GDPR על בעל שליטה חובה לבצע הערכת פגיעה בפרטיות (Privacy Impact Assessment) כאשר הוא מבצע עיבוד אוטומטי של מידע אישי לשם גיבוש הערכה של היבטי האישיות של האדם (פרופיילינג) והחלטות בעלות השלכות משפטיות או דומות על נושא המידע עשויות להתקבל על בסיס עיבוד אוטומטי שכזה.**[32] במידה שתסקיר הערכת הפגיעה בפרטיות מצביע על סיכון גבוה לפרטיות, על בעל השליטה במידע לפנות להתייעצות מקדימה טרם עיבוד המידע עם הרשות האחראית על הגנת הפרטיות במדינה הרלוונטית.[33]

דרישה זו לביצוע סקר הערכת פגיעה בפרטיות היא בפועל אמצעי אבטחה נוקשה על עיבוד מידע אישי באופן אוטומטי לשם פרופיילינג. כמו כן, האיסור הקבוע ב-GDPR על קבלת החלטה המשפיעה באופן משפטי או משמעותי אחר על נושא מידע בהתבסס אך ורק על עיבוד אוטומטי של מידע רגיש, לרבות פרופיילינג, אלא בנסיבות מצומצמות,[34] עשוי בפועל למנוע ביצוע מחקרים באופן זה במידה שהם מיועדים לשמש כבסיס לקבלת החלטות בעלות השפעה משפטית או משמעותית אחרת על נושא המידע.

---

[29] סעיף 14 וסעיפים 33 ו-62 להקדמה ל-GDPR.
[30] סעיף 33 להקדמה ל-GDPR.
[31] סעיף 89(1) ל-GDPR.
[32] סעיף 35(3)(a) ל-GDPR.
[33] סעיף 36 ל-GDPR.
[34] סעיף 22(1) ל-GDPR.

בנוסף, **כאשר מדובר בעיבוד מידע רגיש לצרכיי מחקר רפואי מחייב ה-GDPR כי המחקר יבוצע בהתאם לתנאי ה-GDPR המכוונים ליצירת הרמוניזציה בנושא, אולם גם מבהיר שעל המדינות החברות באיחוד לחוקק חוקים מדינתיים שיבטיחו שהמחקר יעשה לטובת הציבור בתחום בריאות הציבור ואשר עשויים להטיל דרישות נוספות כאשר מדובר בעיבוד מידע גנטי, ביומטרי או מידע בנוגע לבריאות**.[35]

ה-GDPR, אימץ אמת מידה גמישה ביחס להתממה ולמחקר בנתוני עתק הנשענת על ניהול סיכונים. אמת המידה לבחינה האם המידע הוא מידע אישי אשר הוראות ה-GDPR חלות עליו או שמדובר במידע מותמם היא: האם על ידי שימוש באמצעים סבירים, שסביר שבעל השליטה במידע או אדם שלישי יעשה בהם שימוש, ניתן לזהות את נושא המידע על בסיס המידע שבמאגר. כלומר, האם באמצעים סבירים ניתן לעקוף את האמצעים הארגונים והטכנולוגיים שיישם בעל השליטה במידע ולאתר מחדש פרטי מידע מזהים.[36] במסגרת זו ה- GDPR מאפשר סיכון מסוים נמוך לפגיעה בפרטיות, במידה שננקטים כל האמצעים הסבירים להבטחת מיזעור הפגיעה בפרטיות, אולם מחייב בביצוע הערכת סקר סיכונים ובהטמעת אמצעי אבטחה ארגוניים וטכנולוגיים הולמים.[37]

2. <u>ארצות הברית</u>

החקיקה הקיימת כיום בארה"ב מאד ידידותית למחקר רפואי בנתוני עתק מתוך הנחה שהתממה מאפשרת הגנה מספקת על פרטיותו של נושא המידע ועל בסיס ההנחה ששימוש משני במידע רפואי למטרות מחקר הוא פחות פוגעני לפרטיות מאשר במצב בו המידע נאסף מראש למטרות מחקר.[38] החוק המסדיר עריכת

---

[35] סעיף הקדמה 53 ל-GDPR.
[36] סעיף 26 להקדמה ל-GDPR.
[37] שרון בר זיו וטל ז'רסקי, *פרטיות במשבר זהו: אסטרטגיות הסדרה בעידן התממה*, משפט חברה ותרבות ב9, 142 (מיכאל בירנהק עורך, 2019).
[38] Michael Birnhack, *A Process-Based Approach to Informational Privacy and the Case of Big Medical Data,* 20 THEORETICAL INQUIRIES L. XX 26 (2019).

מחקרים רפואיים בארצות הברית (להלן: "**HIPPA**")[39] מציע שני מתווים להתממת מידע אישי רפואי (Protected Health Information):[40]

(1) אדם בעל ידע ומומחיות בכל הקשור לעקרונות מדעיים וסטטיסטיים מקובלים ושיטות להתממת מידע אישי קובע שהסיכון שאדם שסביר שיקבל את המידע המותמם ישתמש בו, לבד או במשולב עם פרטי מידע אחרים שזמינותם סבירה, לזיהוי נושא המידע הוא נמוך.[41] אולם, HIPPA אינו מסביר מהן אמות המידה לסיכון נמוך וכן אינו קובע מדדים למיהות המומחה הרלוונטי.[42]

(2) נמל המבטחים: הסרת 18 פרטי מידע מזהים ובהם שם נושא המידע, כל מחוון מיקום גיאוגרפי המצומצם יותר ממדינה,[43] כל תאריך הקשור במישרין לנושא המידע, למעט ציון שנה בלבד, מספר טלפון, מספר רישוי, מספר פקס, כתובת דוא"ל, נתון מזהה ביומטרי, או צילום פנים מלא; ובלבד שבעל השליטה במידע אינו יודע שניתן לזהות נושא מידע על בסיס המידע שבמאגר או שילובו עם מידע אחר.[44]

על שיטת נמל המבטחים נמתחה ביקורת לא מעטה, אם כי על אף חסרונותיה זו שיטת ההתממה הפופולארית יותר נוכח פשטותה, קלות ביצועה והוודאות שמאפשרת.[45]

מבין חסרונותיה ניתן למנות את חוסר הוודאות הנלווה לדרישה לחוסר ידיעה בפועל של בעל השליטה במידע, והיותה מעורפלת ונתונה

---

[39] The Health Information Insurance Portability and Accountability Act of 1996 (להלן: "**HIPPA**").

[40] מידע אישי רפואי מוגדר בסעיף 160.103 ל-HIPPA כמידע אישי מזוהה.

[41] סעיף 164.514(b)(1) ל-HIPPA.

[42] שרון בר זיו וטל ז'רסקי, *פרטיות במשבר זהו: אסטרטגיות הסדרה בעידן התממה*, משפט חברה ותרבות ב9, 147 (מיכאל בירנהק עורך, 2019).

[43] הכללים מאפשרים ציון של שלוש הספרות הראשונות של המיקוד ובלבד שמספר נושאי המידע שספרות אלו ישוייכו אליו עולה על 20,000. אם מדבר במספר נמוך יותר יש לרשום במקום שלוש הספרות 000. ראו Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule.

[44] סעיף 164.514(b)(2) ל-HIPPA.

[45] Khaled EL Eman, *Perspectives of Health Data De-Identification,* Privacy Analytics.

לפרשנות.[46] בנוסף, שיטה זו אינה מתאימה לעידן נתוני עתק וחושפת את חולשת ההתממה במלואה. זאת משום שהסרת פרטי מידע מזהים ישירים בלבד אינה נותנת מענה לקיומם של פרטי מידע רבים שאינם מזהים ישירים אולם הצלבתם עלולה להביא לזיהוי נושא המידע.[47] כך, למשל, במאגר המידע על חולים שביקרו בבתי חולים בניו יורק בשנת 2007 מדובר במאגר מידע רפואי הכולל רשומות ביקור מתמשכות, כלומר פירוט של מספר ביקורים ומספר מקרים של מתן שירות רפואי לאותו נושא מידע. בהנחה שגיל ומין הם קבועים שאינם משתנים, ושהתוקף יודע מספר נתונים נוספים לגבי האדם אותו הוא מחפש במאגר, כמו למשל מקום מגורים, משך שהות בחל מהביקורים ואולי אף דיאגונזה כללית,[48] סיכוי סביר שיצליח לזהות את האדם המבוקש על ידו על בסיס פרטי המידע שיוותרו במאגר לאחר התממתו בשיטת נמל המבטחים.[49]

מנגד, הסרת חלק מפרטי המידע כנדרש עלולה לפגוע ביעילות המאגר המותמם בשיטה זו למחקר. למשל מחקרים של מחלות הרבה פעמים דורשים מידע גיאוגרפי אולם לפי נמל המבטחים ניתן לציין רק את שלוש הספרות הראשונות של המיקוד. כתוצאה המחקר עשוי להוביל לתוצאות לא מדויקת.

זאת ועוד, הנחת המוצא שבבסיס שיטת נמל המבטחים היא שהמאגר הנתונים משקף מדגם רדנומלי של אוכלוסיית ארה"ב. אולם, כאשר אין המאגר משקף מדגם רנדומלי של אוכלוסיית ארה"ב הוא אינו מספק הגנה מספקת מפני זיהוי חוזר. למשל, מאגר המידע הרפואי של חולים ששוחררו מבית החולים במדינת ניו יורק בשנת 2007 מכיל לאחר ניקויו מנתוני רעש 1.5 מיליון חולים. חוקר שהתמקד רק בנתונים על גברים מעל גיל 64

---

[46] שרון בר זיו וטל ז'רסקי, *פרטיות במשבר זהו: אסטרטגיות הסדרה בעידן התממה*, משפט חברה ותרבות ב9, 147 (מיכאל בירנהק עורך, 2019).

[47] Jordi Soria-Comas & Josep Domingo-Ferrer, Big Data Privacy: Challenges to Privacy Principles and Models, 1(1) Data Sci. Eng. 21, 23 (2016).

[48] פרטי מידע אלו עשויים להיות בידיעתו של שכן, עמית לעבודה, בן זוג לשעבר או כאשר נושא המידע הוא דמות ציבורית.

[49] Khaled El Eman, *Perspectives on Health Data De-Identification*, Privacy Analytics

שאושפזו לתקופה העולה על 14 יום בבית החולים הבחין כי 4% מתוכם מפגינים ייחודיות בהשוואה למדגם מייצג של אוכלוסיית ארה"ב. כאשר צומצם המאגר לבחינה רק של גברים מעל גיל 64 שאושפזו לתקופה העולה על 30 יום בבית החולים נמצא ייחודיות של 11.14%. הייחודיות מאפשרת למי שמחפש אדם ספציפי, בין שהוא יודע שהוא במאגר ובין אם לאו, וודאות גבוהה לזהות ברגע שמוצא במאגר נושא מידע שפרטיו דומים לאלו הידועים לו על האדם אותו הוא מחפש.[50]

נוסף על שיטות ההתממה, ה-HIPAA מאפשר לארגונים הכפופים לו[51] להעביר מידע אישי רפואי, לא מותמם, לשותפים עסקיים עמם יש להם מערכת חוזית,[52] מבלי לדווח על כך את נושאי המידע עצמם ובלבד שהמידע המועבר ישמש לסיוע לספק שירותי הרפואה בביצוע משימותיו ושהעברת המידע והשימוש בו נעשים בהתאם לקבוע בחוזה בין הצדדים.[53] מסגרת זו היא שאפשרה את העברת המידע הרפואי על עשרות מיליוני מטופלים ממערכת הבריאות השנייה בגודלה בארה"ב, Ascension, לגוגל.[54]

3. <u>אוסטרליה</u>

חוק הפרטיות באוסטרליה מציג 3 אפיקים לשימוש וגילוי מידע רפואי לצורך מחקר:

(1) הסכמת נושא המידע.[55]

(2) המידע מותמם. מידע מותמם מוגדר **כמידע שאינו על אדם מזוהה או שניתן לזהותו באופן סביר**. לפיכך, אם המידע האישי הותמם והסיכוי לזיהוי חוזר נמוך אזי אין חוק הפרטיות חל על השימוש במידע המותמם.[56]

---

[50] Khaled El Eman, *Perspectives on Health Data De-Identification*, Privacy Analytics

[51] הכוונה ל"covered entity" המוגדר בסעיף 160.103 ל-HIPAA ככוללים ספקי שירותי רפואה שונים וספקי ביטוח רפואי .

[52] ראו הגדרת "business associate" בסעיף 160.103 ל-HIPAA.

[53] סעיף 164.502(e)(1)-(2) ל-HIPAA.

[54] Gregory Barber and Megan Holteni, *Google Is Slurping Up Health Data – and It Looks Totally Legal,* WIRED (Nov. 11, 2019)

[55] Privacy Act 1998, Schedule 1 – Australian Privacy Principles, 6.1(a).

[56] Australian Government, National Health and Medical Research Council, Guidelines Under Section 95 of the Privacy Act 1988 (2014), עמ' 1; סעיף 6 ל- Privacy

הקביעה האם המידע מותמם נעשית בהתאם לאמת מידה של סבירות וניהול סיכונים, כלומר נדרש שבהתחשב בנסיבות הסיכוי לזיהוי חוזר יהיה נמוך. סבירות הזיהוי החוזר תקבע בהתאם לנסיבות הספציפיות לרבות אופי המידע והיקפו, מי מחזיק במידע ולמי ניתנת הרשאה לעשות בו שימוש, מהו המידע הנוסף הזמין בידי מי שניתנת לו הרשאת גישה למידע המותמם, האם אפשרות השימוש במידע המותמם לשם זיהוי נושא המידע היא מעשית, ומה עשויה להיות המוטיבציה לזיהוי חוזר של נושא המידע מהמאגר. ככלל, סביר שנושא מידע יהיה מזוהה כאשר הזיהוי החוזר אפשרי מבחינה טכנית וקיימת סבירות שיבוצע זיהוי חוזר.[57]

בספטמבר 2016 הצליחו חוקרים מאוניברסיטת מלבורן לזהות מחדש נושאי מידע ממידע רפואי מותמם אשר פורסם באתר האינטרנט הממשלתי שכתובתו data.gov.au. תגובת ממשלת אוסטרליה היתה הצעת חוק המטילה ענישה פלילית וקנסות בגין זיהוי חוזר, אולם היא טרם התגבשה לכדי חוק.[58]

(3) לא ניתן להשיג את מטרת המחקר באמצעות שימוש במידע רפואי מותמם ומתקיימות נסיבות רפואיות מותרות (Permitted Health Information).

בהקשר של איסוף מידע רפואי מתרחשות נסיבות רפואיות מיוחדות בהתקיים התנאים הבאים:[59]

(א) איסוף המידע נחוץ להגשמת אחת מהמטרות הבאות:

(i) מחקר רפואי הרלוונטי לבריאות או לביטחון הציבור;

Act 1988 מגדיר מידע אישי כמידע או דעה על אדם מזוהה או שניתן לזהותו באופן סביר (...“ information or an opinion about an identified individual, or an individual who is reasonable identifiable"); מידע מותמם מוגדר כמידע אישי שכבר אינו על אדם מזוהה או על אדם שמזוהה באופן סביר.

[57] Australian Government, Office of the Australian Information Commissioner, De-identification and the Privacy Act (March 21, 2018).

[58] Simon Lewis, Roland Fan, Sylvia NG, Steph Baker, *Health Data Governance: Re-Identification of Health Records*, P.W.C. (May 11, 2017); Privacy Amendment (Re-identification offence) Bill 2016.

[59] סעיף 16B(2) ל-Privacy Act 1988.

(ii) אגריגציה או ניתוח מידע סטטיסטי הרלוונטי לבריאות או לביטחון הציבור;

(iii) ניהול, מימון ופיקוח על שירות רפואי.

(ב) לא ניתן להגשים את המטרה על ידי איסוף מידע מותמם;

(ג) לא מעשי להשיג את הסכמת נושא המידע;

(ד) מתקיים אחד מהתנאים הבאים:

(i) איסוף המידע נדרש לפי חוק.

(ii) האיסוף נעשה בהתאם לכללים שקבע גוף רפואי מתאים להתמודדות עם חובת הסודיות המקצועית החלה עליו;

(iii) האיסוף נעשה בהתאם לקווים מנחים שהפיצה מועצת הבריאות הלאומית והמחקר הרפואי באוסטרליה ושאושרו על ידי נציבות הפרטיות במדינה.

בהקשר של שימוש או גילוי מידע רפואי מתרחשות נסיבות רפואיות מיוחדות בהתקיים התנאים הבאים:[60]

(א) איסוף המידע נחוץ להגשמת אחת מהמטרות הבאות:

(i) מחקר רפואי הרלוונטי לבריאות או לביטחון הציבור;

(ii) אגריגציה או ניתוח מידע סטטיסטי הרלוונטי לבריאות או לביטחון הציבור;

(ב) לא מעשי להשיג את הסכמת נושא המידע;

(ג) השימוש או הגילוי מתבצעים בהתאם לקווים מנחים שהפיצה מועצת הבריאות הלאומית והמחקר הרפואי באוסטרליה ושאושרו על ידי נציבות הפרטיות במדינה.

---

[60] סעיף 16B(3) ל-Privacy Act 1988.

(ד) כאשר נעשה גילוי של המידע הרפואי, על הארגון להאמין באופן סביר שמקבל המידע לא יגלה את המידע שנמסר לו או כל מידע אישי שניתן ללמוד ממנו.

על נציבות הפרטיות לאשר קווים מנחים שמגישה מועצת הבריאות הלאומית והמחקר הרפואי באוסטרליה **רק אם שוכנעה שאינטרס הציבור בקידום המחקר מהסוג שהקווים המנחים מבקשים להסדיר, כלומר באיסוף, בשימוש ובגילוי של מידע רפואי למטרת המחקר הספציפי, גובר בצורה משמעותית על אינטרס הציבור בשמירה על הפרטיות ברמה הקבועה בעקרונות ההגנת על הפרטיות לפי החוק**.[61]

לפי הקווים המנחים של מועצת הבריאות הלאומית והמחקר הרפואי באוסטרליה, ושאושרו על ידי נציבות הפרטיות במדינה, על המבקש לעבד מידע רפואי לצרכי מחקר לקבל את אישורה של הועדה האתית לאישור מחקרים בבני אדם (Human Research Ethics Committee) ולאחר מכן לפעול בהתאם לנדרש בקווים המנחים. פעולה בהתאם להנחיות אלו תפטור אותו מאחריות לפגיעה בפרטיות.[62]

4. <u>פינלנד</u>

בפינלנד, לאחר קרוב לארבע שנים של דיונים בפרלמנט,[63] נכנס במאי 2019 לתוקף חוק בנוגע לשימוש משני במידע רפואי וסוציאלי[64] המיועד לעגן בחקיקה ראשית את האיזון הרצוי לדעת ממשלת פינלנד בין הגנה על הזכות לפרטיות לבין האינטרס הציבורי בחדשנות ושגשוג כלכלי בתחום הבריאות והשירותים הרפואיים והסוציאליים. חוק השימוש המשני הוא גם החוק המדינתי הראשון המיישם את ה-GDPR בהקשר של שימוש במידע רפואי לצרכי מחקר.

---

[61] סעיף 95 ל – Privacy Act 1988.

[62] Australian Government, National Health and Medical Research Council, Guidelines Under Section 95 of the Privacy Act 1988 (2014).

[63] Aino Vesikansa, *New act on Finnish health and social data provides opportunities for research and business*, MEDENGINE (11/04/2019).

[64] Act on the Secondary Use of Health and Social Data (להלן: "**חוק השימוש המשני**").

חוק השימוש המשני מתווה מסגרת לפיה רשות רישוי ייעודית, שתפעל במוסד הפיני לבריאות ורווחה,[65] היא שאוספת את המידע הרפואי או הסוציאלי, מתמימה אותו ומתירה את העיון והשימוש בו, לתקופה קבועה מראש, למטרות שימוש משני הקשורות בבריאות הציבור וברווחתו החברתית.[66] הרשות רשאית גם להפקיע רישיון במידה שנמצא שמקבל הרישיון אינו עומד בדרישות האבטחה הקבועות בחוק וברישיון.[67]

במסגרת שימוש משני מונה החוק מספר מטרות[68] כגון מחקר מדעי;[69] ניתוחים סטטיסטיים; הוראה;[70] מחקר ופיתוח וחדשנות, כלומר השימוש במידע לפיתוח מוצרים, תהליכים ושירותים משופרים;[71] ניהול מבוסס ידע לשם תמיכה בתפעול, ייצור, שליטה כלכלית, ניהול וקבלת החלטות;[72] וביחס לרשויות מדינה המפקחות על גופים המעניקים שירותים רפואיים ושירותי רווחה – שימוש במידע לשם פיקוח על גופים אלו, הנחייתם ואכיפת החוק עליהם.[73]

כלומר רשות הרישוי הייעודית הופכת לגורם המרכזי והיחיד שבסמכותו לאשר שימוש משני במידע רפואי או סוציאלי. בדרך זו ביקשה הממשלה הפינית להקל על הנטל הרגולטורי המוטל על המבקשים לעבד מידע רפואי וסוציאלי למטרות שימוש משני, לשפר, לייעל לזרז את תהליך מתן אישורי העיון והשימוש במידע רפואי וסוציאלי.

בנוסף, תוקם לפי חוק השימוש המשני יחידה נפרדת שתורכב ממומחים בתחום אבטחת מידע ושתפקידה יהיה לבחון האם המידע המונגש על ידי רשות הרישוי מעובד באופן מאובטח ותוך שמירה על הזכות לפרטיות.[74]

---

[65] סעיף 4 לחוק השימוש המשני.
[66] סעיף 5 לחוק השימוש המשני.
[67] סעיף 27 לחוק השימוש המשני.
[68] סעיף 2 לחוק השימוש המשני.
[69] סעיף 38 לחוק השימוש המשני.
[70] סעיף 39 לחוק השימוש המשני.
[71] סעיף 3(4) לחוק השימוש המשני.
[72] סעיפים 3(5) ו-41 לחוק השימוש המשני.
[73] סעיפים 3(6),(7) ו-42 לחוק השימוש המשני.
[74] סעיף 29 לחוק השימוש המשני.

כאשר הבקשה היא לשימוש במידע רפואי או סוציאלי למטרות מחקר וחדשנות יש לקבל את הסכמתו המפורשת של נושא המידע לשימוש. ללא הסכמה ניתן לעשות שימוש רק במידע אגרגטיבי. בכל מקרה העיון והשימוש במידע יעשה תוך נקיטת כל אמצעי האבטחה הדרושים.[75]

[75] סעיף 36 לחוק השימוש המשני.