הצעה למתווה בנושא מרשמים אלקטרוניים[1]

תוכן עניינים:

[1] מסמך זה מפורסם בהצעה של מתווה להערות הציבור ובכל מקרה, יישומו יתאפשר רק לאחר תיקון תקנות הרופאים (מתן מרשם), תשמ"א-1981

הגדרות

"מוסד רפואי"- כהגדרתו ב"חוזר מנכ"ל רגולציית יסוד להגנת סייבר במערכת הבריאות בישראל" דהיינו בית חולים ומרפאה/ מכון/ גן שיקומי כמשמעותם בפקודת בריאות העם, 1940 וכל מוסד אחר אשר תפקידו העיקרי הוא מתן שירותי בריאות;

"מערכת מאגר מרשמים" – מערכת המספקת שירותי ניהול, אחסון ועיבוד מידע לצורך ניהול מרשמים של מוסד רפואי לצורך הנפקתם כמרשם אלקטרוני בבתי המרקחת.

פרק א' - דרישות ממוסד רפואי המעוניין להפעיל מרשמים אלקטרוניים

1. העתק מרשם

1.1. על המוסד הרפואי לוודא כי לא ניתנים במקביל מרשם אלקטרוני ומרשם נייר לאותו עניין, ולנקוט אמצעים שיבטיחו כי הפקת מרשם נייר תבטל את תוקפו של מרשם אלקטרוני זהה שניתן, ולהיפך - הפקת מרשם אלקטרוני תביא לביטול תוקפו של מרשם ידני שהופק במקביל

1.2. תדפיס/פלט/קובץ בפורמט קריא לאדם של מרשם אלקטרוני לא יחשב כמרשם אלא "העתק" המרשם בלבד, אינו תקף כמרשם למימוש בבית מרקחת, ואין לחתום עליו ידנית.

1.3. כל תדפיס/פלט של המרשם יכלול במקום בולט את ציון העובדה שמדובר בהעתק בלבד של מרשם אלקטרוני

2. ניהול הרשאות גישה של מטפלים

2.1. על מוסד רפואי המעוניין להפיק מרשמים אלקטרונים לנהל הרשאות גישה של בעלי הרשאות למאגרי המידע ולמערכת מאגר המרשמים איתו הוא עובד, בהתאם להגדרות תפקיד; הרשאת הגישה לכל תפקיד תהיה במידה הנדרשת לביצוע התפקיד בלבד.

2.2. מוסד רפואי ינהל רישום מעודכן של תפקידים, הרשאות הגישה שניתנו להם, ושל בעלי ההרשאות הממלאים תפקידים אלה.

2.3. בטרם הפקת מרשם ושמירתו במאגר הנתונים של המערכת הקלינית, יש לוודא אימות המטפל/ת על פי רמת הבטחת אימות 3 (רב״א3) העונה לתנאי MFA מלא כפי שהוגדרה על ידי מערך הסייבר הלאומי.

2.4. במידה ומנגנון הזדהות במערכת הקלינית אינה תואמת רב״א 3 כברירת מחדל, מערכת/מודול הפקת מרשם אלקטרוני, יממש תהליך העלאת רמת אימות המטפל/ת לרמת רב"א 3 לצורך ביצוע פעולת חתימה על המרשם.

3. חתימה על מרשם אלקטרוני-

המוסד הרפואי יעשה שימוש באחד האופנים לחתימה על מרשם אלקטרוני המפורטים בפרק ד'.

4. שימוש במערכת מאגר מרשמים-

4.1. מוסד רפואי יוכל להפעיל מרשם אלקטרוני בתנאי שיעשה שימוש במערכת מאגר מרשמים העומדת בקריטריונים האמורים בפרק ב';

4.2. המוסד הרפואי ינהל את מערכת המאגר בעצמו או יעשה שימוש בצד ג' (ובכלל זה באמצעות מוסד רפואי אחר המפעיל מערכת מאגר מרשמים), ובלבד שיוודא כאמור כי מערכת מאגר המרשמים עומדת בהוראות נוהל זה.

פרק ב' – דרישות ממערכת מאגר מרשמים

1. מוסד רפואי המעוניין לעשות שימוש במרשמים אלקטרונים ירשם ברשם "מרשמים אלקטרוניים" של משרד הבריאות, אשר יכלול נתונים אלו:

1.1. שם בעל מאגר המרשמים בו הוא עושה שימוש

1.2. תצהיר בעל מאגר המרשמים כי הוא עומד בהוראות נוהל זה

1.3. פרטים נוספים שיקבעו על ידי הרוקח הראשי של משרד הבריאות

2. בעל מערכת מאגר מרשמים ינהל רישום מעודכן של תפקידים והרשאות הגישה שניתנו להם, ושל בעלי ההרשאות הממלאים תפקידים אלה.

3. (א) בעל מערכת מאגר מרשמים המנוהל על ידי מוסד רפואי, נדרש לעמוד בכלל ההוראות בחוזר מנכ"ל רגולציית יסוד להגנת סייבר במערכת הבריאות בישראל.

(ב) בעל מערכת מאגר מרשמים המשמש כספק למוסד רפואי– נדרש לעמוד בתקן ISO27001 ולהתחייב לאפשר למשרד הבריאות לבצע בקרות במסגרת סקר טכנולוגי אבטחתי המבוצע ע"י המשרד.

4. קריטריונים להפעלת מאגר מרשמים-

4.1. בעל המאגר יבטיח תקשורת מאובטחת למאגר עבור כל פניה למאגר מכל גורם מורשה

4.2. מערכת מאגר המרשמים תחתום בחתימה ארגונית של בעל המאגר בטרם העברת המרשם לניפוק לבית המרקחת.

4.3. בעל מאגר מרשמים יחזיק רישום עדכני של מרשמים בתוקף, ויתעד כל ניפוק באופן המאפשר לקשור בין כלל הניפוקים שבוצעו מתוקף מרשם מסוים ובין המרשם המקורי.

4.4. בעל מאגר מרשמים רשאי לשמור את פרטי תכשירי המרשם שנרשמו בנפרד מהמרשם המקורי כפי שהתקבל במאגר, ובלבד שלצד כל תכשיר נרשם באופן ברור המספר המזהה של המרשם (DPI), באופן שיאפשר יכולת בדיקה ושחזור טרנזאקציה לאחור של קשר בין התכשיר לבין המרשם המקורי ומפיק המרשם.

4.5. מאגר המרשמים יוגדר כמאגר שחלה עליו רמת אבטחה גבוהה ויעמוד, בהוראות החוק להגנת הפרטיות והנחיות של תקנות הגנת הפרטיות (אבטחת מידע) בגרסתן העדכנית.

4.6. בעל מאגר מרשמים יצור ממשק עדכון מול המוסד הרפואי לאחר ניפוק מרשמים.

5. מוסד רפואי אשר אינו מנהל את הרשאות הגישה עבור מטפליו כאמור בסעיף 2, רשאי להוכיח את עמידתו בכל הוראות פרק א', באמצעות ספק צד ג'

פרק ג' - אחריות בית מרקחת

1. תשאול מאגרי מרשמים- בית המרקחת יתשאל אך ורק מאגרי מרשמים הרשומים ברשם "מרשמים אלקטרוניים" של משרד הבריאות.
2. אימות חתימה של בעל המאגר- המערכת הממוחשבת של בית המרקחת תאמת את החתימה של בעל המאגר לפני העברת המרשמים לניפוק.
3. עדכון חוזר של בעל המאגר-

3.1. על המערכת הממוחשבת של בית המרקחת לעדכן את המערכת הממוחשבת של מאגר המרשמים בנוגע לתכשירים שנופקו וכמותם.

3.2. לפני שליחת המסר האלקטרוני למאגר המרשמים, המסר ייחתם בחתימה של בית המרקחת.

4. לא ינופקו תכשירים על סמך העתק מודפס של מרשם ואין לדרוש מן המטופל/ת למסור לבית המרקחת העתק מודפס של מרשם אלקטרוני.
5. זיהוי המטופל/ת על ידי בית המרקחת-

5.1. זיהוי מטופל/ת יהיה לפי הנחיות שיבטיחו הליך זיהוי השווה לפחות לזיהוי המבוצע בעת הנפקת מרשם ידני.

5.2. בעת ניפוק מרשם לסמים מסוכנים יחולו ההוראות המתאימות.

פרק ד' - אופני החתימה האפשריים על מרשם אלקטרוני

לכל אורך התהליך של מימוש מרשם אלקטרוני, גם בעת העברת המרשמים למאגר, וגם מהמאגר לבתי המרקחת וחזרה, ניתן לעשות שימוש בכל אחד משלושת אופני החתימה המפורטים להלן:

1. **"חתימה אלקטרונית מאובטחת"-** כהגדרתה בחוק חתימה אלקטרונית, התשס"א-2001: דהיינו חתימה שהיא מידע אלקטרוני או סימן אלקטרוני, שהוצמד או שנקשר למסר אלקטרוני, שהיא ייחודית לבעל אמצעי החתימה, מאפשרת זיהוי לכאורה שלו, הופקה באמצעי הניתן לשליטתו הבלעדית ומאפשרת לזהות שינוי שבוצע במסר האלקטרוני לאחר מועד החתימה ;

2. **"חתימה אלקטרונית מאושרת"** - כהגדרתה בחוק חתימה אלקטרונית, התשס"א-2001: חתימה אלקטרונית מאובטחת אשר גורם מאשר (גורם שאושר על ידי רשם הגורמים המאשרים במשרד המשפטים) הנפיק תעודה אלקטרונית בדבר אמצעי אימות החתימה, המזהה אותה ;

3. **"חתימה דיגיטלית"-** חתימה שהיא מידע אלקטרוני או סימן אלקטרוני, שהוצמד או שנקשר למסר אלקטרוני, שהיא ייחודית לארגון בעל אמצעי החתימה, מאפשרת זיהוי לכאורה שלו, הופקה באמצעי הניתן לשליטתו הבלעדית ומאפשרת

לזהות שינוי שבוצע במסר האלקטרוני לאחר מועד החתימה. (פירוט בנספח 1- הנחיות ליישום חתימה דיגיטלית)

נספח 1- הנחיות ליישום חתימה דיגיטלית

<u>כללי</u>

מסמך יישום זה מפרט את התנאים הנדרשים בכדי לאפשר חתימה דיגיטלית על מרשם אלקטרוני לכל אורך התהליך של מימוש מרשם אלקטרוני, בנוסף לאפשרות של חתימה אלקטרונית מאובטחת או מאושרת.

1. <u>כללים מנחים</u>

1.1. מוסד רפואי המבקש להפיק מרשמים אלקטרוניים באמצעות חתימה דיגיטלית יהיה:

1.1.1. מוסד רפואי העומד ברגולציית הייסוד להגנת סייבר במערכת הבריאות בישראל שפורסמה על ידי משרד הבריאות, המסדירה את עקרונות היסוד לניהול הגנת סייבר בארגוני בריאות, תוך התייחסות לצורכי הגנת המידע, שמירה על חוקי הפרטיות, וניהול סיכוני סייבר במגזר הבריאות בישראל.

1.1.2. מוסמך ISO27001:2022 או מאוחר יותר.

1.2. המרשם נחשב בר תוקף אך ורק כאשר מתקיימים כל התנאים הבאים:

1.2.1. המרשם הופק במערכת קלינית של מוסד רפואי.

1.2.2. המרשם האלקטרוני חתום באמצעות תעודה אלקטרונית מאושרת שסופקה למוסד הרפואי על ידי גורם מאשר, או באמצעות תעודה אלקטרונית מאובטחת של המוסד הרפואי, או באמצעות תעודה אלקטרונית שתסופק לארגון בתשתית אשר תאושר על ידי משרד הבריאות (להלן "חתימה דיגיטלית")

2. <u>אימות זהות המטפל/ת (הזדהות)</u>

2.1. בטרם הפקת מרשם ושמירתו במאגר הנתונים של המערכת הקלינית במוסד הרפואי, יש לוודא אימות המטפל/ת על פי רמת הבטחת אימות 3 (רב״א3) העונה לתנאי MFA מלא כפי שהוגדרה על ידי מערך הסייבר הלאומי.

2.2. במידה ומנגנון הזדהות במערכת הקלינית אינה תואמת רב״א 3 כברירת מחדל, מערכת/מודול הפקת מרשם אלקטרוני, יממש תהליך העלאת רמת אימות המטפל/ת לרמת רב"א 3 לצורך ביצוע פעולת חתימה על המרשם.

3. <u>בקרת הרשאות המטפל/ת</u>

3.1. לכל מטפל/ת יקבעו הרשאות גישה, בהתאם להגדרות תפקיד; הרשאת הגישה לכל תפקיד תהיה במידה הנדרשת לביצוע התפקיד בלבד.

3.2. המוסד הרפואי ובעל מאגר המרשמים ינהלו רישום מעודכן של תפקידים, הרשאות הגישה שניתנו להם, ושל בעלי ההרשאות הממלאים תפקידים אלה.

3.3. כתנאי מקדים לפעולת ביצוע חתימה דיגיטלית על המרשם יש לשייך את המטפל/ת לאחת משתי קבוצות:

3.3.1. בעלי הרשאה פרטנית חד-פעמית להפקת מרשם יחיד.

3.3.2. בעלי הרשאה קצובה בזמן להפקת המרשמים במסגרת משמרת העבודה לתקופה קצובה בזמן ומוגדרת מראש ממועד ביצוע הזדהות במערכת.

3.4. לאחר אימות המטפל/ת, יתקבל טוקן הרשאה (OTP Authorization Token) חד-פעמי ייעודי וקצוב בזמן בהתאם לקבוצת הרשאות (פרופיל) המטפל/ת לקבוצת המורשים. הטוקן יהיה מסוג JWT (JSON Web Token) ויכיל בין היתר את פרטי הזיהוי של המטפל/ת

3.5. הטוקן ישמר ב-Cache בהתאם לתוקף המוגדר:

3.5.1. הרשאה פרטנית – תוקפו של הטוקן פג מייד עם הפקת המרשם ו/או לאחר תקופה של 2 דקות.

3.5.2. הרשאה תקופתית – תוקפו של הטוקן פג לאחר תקופה של עד X שעות ממועד היווצרו עפ"י הנחיית מנהל המערכת ולא יותר ממשך משמרת אחת ברציפות.

4. בקרת גישה לשרות מרשם אלקטרוני

4.1. כאשר מתקבלת בקשה להפקת מרשם אלקטרוני (לחיצה על כפתור "חתום" במערכת הקלינית) מופעל מנגנון בדיקת תוקף טוקן ההרשאה.

4.2. ככל שטוקן אינו קיים או שאינו בתוקף, מופעל מנגנון אימות המטפל/ת

4.3. באם קיים טוקן תקף, המרשם האלקטרוני יחתם בחתימה דיגיטלית וישמר במערכת

5. רישום פרטי פעולת החתימה וקיום תנאי אי הכחשה

5.1. כתנאי לקיום תנאי אי הכחשה, יכולת שחזור ותחקור הפעולה על המוסד הרפואי להקים מאגר "רשם חתימות" אשר יהיה נפרד מהמערכת הקלינית ותפקידו – שמירת פרטי פעולת חתימה דיגיטלית

5.2. ברשם החתימות יתועדו פרטי המידע אודות כל מרשם אלקטרוני הנחתם בחתימה דיגיטלית כדלקמן:

5.2.1. Digital Prescription Identifier – DPI

5.2.2. Authorization Token

5.2.3. DPI Timestamp

5.2.4. X.509 Cryptographic Certificate Thumbprint