שם הנוהל: מרשמים אלקטרוניים וחתימה אלקטרונית בקופת החולים ובמוסד רפואי		
תאריך הנוהל: יולי 2013	**מספר הנוהל: 107**	**עמוד 1 מתוך 23**

1. **כללי:**

1.1. נוהל זה נכתב בעקבות **תיקון לתקנות הרופאים (מתן מרשם)** בעניין חתימה אלקטרונית על מרשמים. המהלך לתיקון התקנות וקביעת הנוהל נועד לאפשר לרופאים לחתום על מרשמים גם באמצעות חתימה אלקטרונית מאובטחת, שהנפיקו להם קופת החולים או המוסד הרפואי בו הם עובדים, לצרכי מתן מרשמים במסגרת עבודתם באותה קופה או באותו מוסד רפואי בלבד.

1.2. לחתימה אלקטרונית פוטנציאל להיות מאובטחת עשרות מונים יותר מאשר חותמות הדיו וחתימות יד הנהוגות כיום. השימוש בחתימה אלקטרונית מאובטחת יקל במידה רבה על מבוטחים ומטופלים, ובפרט חולים כרוניים אשר מגיעים אל הרופא לעיתים קרובות רק כדי לקחת מרשם נייר בחתימת יד הרופא. התיקון יאפשר לרופא לשלוח מרשם כמסר אלקטרוני חתום בחתימה אלקטרונית, ישירות לבית המרקחת, ללא צורך בהגעת המטופל אל משרדו של הרופא.

1.3. כמו כן יתאפשר תיעוד אלקטרוני של הוראות רופא למתן טיפול תרופתי במסגרת תיק רפואי אלקטרוני המנוהל בבתי חולים ובתוך מוסדות רפואיים, ללא צורך להדפיס עותק נייר על מנת לייצר מרשם תקף

1.4. עם זאת, שימוש בחתימה אלקטרונית מחייב קיום רישום מאובטח ומעודכן של הרופאים בעלי החתימה, ושל אמצעי אימות החתימה שלהם, שימוש במערכות חומרה ותוכנה מהימנות ואבטחתן, ופרסום אופן השימוש במערכות אלה לציבור הרופאים, ולציבור המטופלים.

1.5. התיקון לתקנות אינו שולל את האפשרות לכל מוסד רפואי לבחור להשתמש בחתימה אלקטרונית **מאושרת** (שהונפקה על ידי גורם מאשר חיצוני), כפי שמאפשר חוק חתימה אלקטרונית כבר היום, אך הוא מאפשר הליך פנימי ליצירת חתימה אלקטרונית לצורך הפקת מרשמים פנים-ארגונית: בתוך המוסד הרפואי או קופת החולים (בין הרופא לבית המרקחת של המוסד/קופה), או בין הנ"ל לבין בתי מרקחת חיצוניים שיהיה עמם **הסדר מוקדם** לעניין זה.

שם הנוהל: מרשמים אלקטרוניים וחתימה אלקטרונית בקופת החולים ובמוסד רפואי		
תאריך הנוהל: יולי 2013	מספר הנוהל: 107	עמוד 2 מתוך 23

2. הגדרות:

"**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;

"**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;

"**מוסד רפואי**" - כהגדרתו בסעיף 24 לפקודת בריאות העם, 1940: בית חולים, מרפאה, מוסד לטיפול במשתמשים בסמים ומעבדה.

"**מרשם**" - הוראה בכתב חתומה ע"י רופא לספק לאדם סם או תכשיר רפואי - כהגדרתו בתקנות הרופאים (מתן מרשם) :.

"**מרשם אלקטרוני**" - מרשם שניתן בדרך אלקטרונית, ונחתם בחתימה אלקטרונית, כך שהמרשם ה"מקורי" והתקף הוא מסר אלקטרוני (קובץ מחשב, דוא"ל וכו') ולא נייר עם חותמת וחתימה ידניות.

"**קופת חולים**" – כאמור בסעיפים 24 ו-25 לחוק ביטוח בריאות ממלכתי התשנ"ד-1994.

"**רמו"ט**" - הרשות למשפט טכנולוגיה ומידע, במשרד המשפטים.

3. שיטה:

3.1. <u>תנאים לחתימה אלקטרונית על מרשמים</u>

3.1.1. קופת חולים או מוסד רפואי המבקשים לאפשר שימוש במרשמים חתומים בחתימה אלקטרונית מאובטחת (כלומר שחתימה אינה חתימה אלקטרונית מאושרת) על ידי רופאיהם:

(א) יקימו מערכת יעילה ומתוקפת לניפוק חתימות אלקטרוניות מאובטחות לרופאים בתצורת PKI, תוך שימוש במערכות חומרה ותוכנה מהימנות ואבטחתן ברמה מספקת בהתאם לנספחי נוהל זה ולחילופין ישתמשו בחתימה אלקטרונית מאושרת כמשמעה בחוק חתימה אלקטרונית;

(ב) ינהלו רישום מאובטח ומעודכן של כל הרופאים שהונפקה להם חתימה מאובטחת מטעמם, ושל אמצעי אימות החתימה שלהם.

(ג) יקבעו נהלים לשמירת אמצעי החתימה שהונפקו על ידי הארגון/מוסד לרופאים, על ידם, ולמניעת שימוש לרעה באמצעי החתימה.

(ד) ינקטו אמצעים למניעת הסתמכות בתי מרקחת על חתימה אלקטרונית מאובטחת שבוטלה (למשל אם אמצעי החתימה אבד או נגנב, פג תוקפה של החתימה וכדומה)

3.1.2. בשלב זה **טרם אושר** להשתמש בחתימה אלקטרונית מאובטחת - למרשמים **לסמים מסוכנים**.

שם הנוהל: מרשמים אלקטרוניים וחתימה אלקטרונית בקופת החולים ובמוסד רפואי		
תאריך הנוהל: יולי 2013	מספר הנוהל: 107	עמוד 3 מתוך 23

3.2. <u>הכנה ומשלוח של מרשם חתום אלקטרונית</u>

3.2.1. הרופא יזדהה למערכת הקלינית של המוסד הרפואי/ קופה כמקובל בכניסה למערכות מידע של הקופה.
3.2.2. הרופא יכין את המרשם ללקוח במחשב.
3.2.3. בסיום הכנת המרשם, יבצע הרופא חיתום אלקטרוני על המרשם באמצעי החתימה שברשותו:
3.2.3.1. אם המפתח הפרטי שישמש כאמצעי חתימה אלקטרונית שמור ברכיב אישי (כגון כרטיס חכם) - הרופא יזדהה בהזדהות באמצעות סיסמא חזקה או אמצעי ביומטרי אל הרכיב ויחתום באמצעות מפתח פרטי זה.
3.2.3.2. אם המפתח הפרטי שמור בשרת חיתום מרכזי - יזדהה הרופא מול מפתח החיתום האישי שלו המצוי על שרת החיתום המרכזי בהזדהות באמצעות סיסמא חזקה או אמצעי ביומטרי, ויחתום באמצעות המפתח הפרטי האישי השמור ברכיב החתימה המרכזי.
3.2.4. לכל מרשם יהיה תאריך תוקף - ולאחר חלוף המועד - יבוטל תוקפו.
3.2.5. בכל מקרה תבוצע **חתימה על כל מרשם בנפרד.** מרשם אחד יכול לכלול מספר תכשירים.
3.2.6. על המרשם, כשהוא בקובץ אלקטרוני, תופיע אינדיקציה לכך שהמסמך נחתם אלקטרונית, וכן פרטי החותם ומועד החתימה.
3.2.7. תדפיס/פלט של מרשם אלקטרוני אינו מרשם אלא "העתק" המרשם בלבד, ואין לחתום עליו ידנית. כל **תדפיס/פלט** של המרשם יכלול **במקום בולט** את ציון העובדה שמדובר ב**תדפיס והעתק בלבד**, של מרשם אלקטרוני, ש**אינו תקף כמרשם** למימוש בבית מרקחת.
3.2.8. במערכת בה נעשה שימוש בחתימה אלקטרונית מאובטחת - לאחר חתימתו של הרופא ולפני ארכובו, תבוצע החתמה דיגיטאלית מרכזית ארגונית של הקופה או של המוסד רפואי על כל מרשם וכחלק מהחתימה יכתב תאריך ושעה (Timestamp). מהלך זה נדרש לצורך השוואה מול תעודות דיגיטליות פגות תוקף, ולכן על הקופה לוודא כי התעודה של הרופא החתום על המרשם - תקפה.
3.2.9. המרשם האלקטרוני ישלח לארכיב ייעודי ומאובטח בו ישמרו כלל המרשמים האלקטרוניים. מרשמים אלקטרוניים ישמרו בארכיב לתקופה של 3 שנים לפחות, לשם הוכחת אמיתות החתימה.

3.3. <u>מסירת העתק המרשם למטופל:</u>

3.3.1. **העתק/תמצית המרשם** שהופק אלקטרונית יסופק לכל מטופל בתדפיס נייר, בדוא"ל, באמצעות אתר הקופה, או ב-SMS (מסרון) - לפי העדפת המטופל ומדיניות הארגון/המוסד. מטופל רשאי לוותר על קבלת העתק/תמצית כאמור.

3.3.2. מטופל זכאי לבקש **מרשם ידני במקום אלקטרוני** – ואם ביקש זאת יש לתת לו מרשם נייר **במקום** מרשם אלקטרוני. אין להפיק מרשם אלקטרוני ובנוסף מרשם ידני - הואיל ומדובר ב"כפל מרשם".

3.3.3. על קופות החולים לוודא כי **לא ניתנים במקביל מרשם אלקטרוני ומרשם נייר** לאותו עניין, ולנקוט אמצעים שיבטיחו, ככל שניתן, כי מימוש מרשם נייר יבטל את תוקפו של מרשם אלקטרוני זהה שניתן (אם ניתן), ולהיפך - מימוש מרשם אלקטרוני יביא לביטול תוקפו של מרשם ידני שהופק במקביל, באמצעות מתן התראה לרוקחים בבתי המרקחת שבהסדר. ניתן להדפיס **העתק** של מרשם אלקטרוני שניתן אולם במקרה זה יש ליישם את האמור בסעיף 3.2.7 לעיל.

3.3.4. במתן מרשם ללא מפגש עם המטופל (כגון חידוש מרשם לחולה כרוני / רפואה מרחוק) יש להבהיר למטופל כי ניתן לממש את המרשם האלקטרוני רק בבתי המרקחת שבהסדר עם קופת החולים / המוסד הרפואי, ולהציע חלופות במידת הצורך.

3.4. נגישות המטופל לבתי מרקחת על ידי קופות החולים:

3.4.1. החל מתאריך 1.06.14 יוכלו קופות החולים להנפיק מרשם בחתימה אלקטרונית רק אם הקופה מאפשרת נגישות למימוש מרשמים כאלה **בכל בתי המרקחת שבהסדר עם הקופה בישראל**.

3.4.2. קופת חולים תאפשר **לכל בית מרקחת שבהסדר** לאתר את המרשם ולעדכן אם נופק או נופק חלקית.

3.4.3. על הקופות להבהיר את אופן ותנאי השימוש במרשמים אלקטרוניים לרופאים בצורה ברורה ותוך הדגשת מתן אפשרויות לחלופות שונות לפי העדפת המטופל, ו**לפרסם בקרב המבוטחים את אופן השימוש במרשמים אלקטרוניים**, את מגבלות המימוש של מרשם אלקטרוני בבתי מרקחת שבהסדר ואת זכותו של מטופל לקבל מרשם ידני במקום אלקטרוני, לפי בקשתו. .

3.4.4. קופת חולים המבקשת להשתמש במרשמים אלקטרוניים:

(א) תכלול בתפוצת המרשמים האלקטרונים את כל בתי המרקחת שלה וכן את כל בתי המרקחת הקשורים עימה בהסכם להנפקת תרופות למבוטחיה

(ב) תפרסם לרופאים בקופה הוראות מפורטות כיצד לרשום מרשם אלקטרוני וכיצד מרשם אלקטרוני מנופק ונאסף, וכן הוראות כיצד לפעול אם המטופל מבקש לקבל מרשם נייר חתום ידנית במקום מרשם אלקטרוני.

(ג) טרם תחילת הפעלת מתכונת מתן מרשמים אלקטרוניים על פי נוהל זה, ואחת לכמה שנים, תפרסם באופן נגיש לכלל מבוטחיה, ובכלל זה גם באמצעות התקשורת ובאמצעות שילוט בולט בסניפיה את אופן השימוש במרשם אלקטרוני ואת זכותם לקבל מרשם נייר ידני במקרה הצורך.

(ד) כאשר ידוע לקופת החולים כי קיים מחסור בתכשיר מסוים בבתי המרקחת של הקופה, או שבהסדר עם הקופה, או בכלל - תיידע הקופה את רופאיה בדבר המחסור בתכשיר, ותנחה אותם להנפיק למטופלים מרשם נייר החתום ידנית, שיוכלו לממש בכל בית מרקחת. ותיידע את המבוטח כי זכותו לקבל החזר בעד רכישת התרופה כך שלא יידרש לשלם עבורה תשלום הגבוה ממה שהיה משלם אילו סופק לו בבית מרקחת של הקופה או מטעמה.

(ה) תאפשר למטופל עפ"י בחירתו לבקש להמיר את המרשם האלקטרוני במרשם ידני

שם הנוהל: מרשמים אלקטרוניים וחתימה אלקטרונית בקופת החולים ובמוסד רפואי		
תאריך הנוהל: יולי 2013	מספר הנוהל: 107	עמוד 5 מתוך 23

3.5. <u>זיהוי המטופל במשיכת תרופות לפי מרשם אלקטרוני:</u>

3.5.1. מטופל שקיבל מרשם אלקטרוני מרופא קופת חולים יציג בפני הרוקח בבית המרקחת כרטיס חבר מגנטי בהתאם להנחיות הקופה, או תעודה מזהה מספקת אחרת לפי נוהלי הקופה.
3.5.2. זיהוי מטופל של מוסד רפואי אחר יהיה לפי הנחיות הזיהוי באותו מוסד, ובלבד שיבטיחו הליך זיהוי השווה לפחות לזיהוי המבוצע בעת הנפקת מרשם ידני.
3.5.3. אם קופה או מוסד רפואי מאפשרים ניפוק תכשיר למיופה כוח - ניתן לפעול לזיהוי מיופה הכוח והמטופל לפי ההוראות הקיימות.

3.6. <u>ניפוק מרשם החתום אלקטרונית:</u>

3.6.1. התכשיר הרשום במרשם החתום בחתימה אלקטרונית מאובטחת או מאושרת ינופק רק לאחר שרוקח בבית המרקחת מצא את המרשם במערכת הממוחשבת של הקופה / המוסד הרפואי, ויכול לעדכן בה כי המרשם נופק.
3.6.2. לא ינופקו תכשירים על סמך מרשם אלקטרוני כאשר לא ניתן להתחבר למערכת הממוחשבת או כאשר מופיע במערכת הממוחשבת כי המרשם כבר מומש / נופק, או שבוטל.
3.6.3. המערכת הממוחשבת תוודא אמינות ותקפות החתימה (כגון שהתעודה הדיגיטלית אינה מבוטלת) ובניפוק מרשם למבוטחי קופה - תוודא כי הרופא הוא רופא קופת החולים.
3.6.4. אין לדרוש מן המבוטח למסור לבית המרקחת העתק מודפס של מרשם אלקטרוני, ואין צורך להדפיס עותק של המרשם האלקטרוני בבית המרקחת, ובלבד שנשמר עותק במחשב בית המרקחת.
3.6.5. טרם ניפוק של מרשם אלקטרוני, יציג הרוקח למטופל רשימת התרופות במרשם ויוודא רצונו למימוש שורות המרשם השונות.
3.6.6. הרוקח המנפק יתעד את הניפוק במערכת הממוחשבת, תוך ציון שם בית המרקחת, מועד הניפוק – יום ושעה, שם הרוקח המנפק ומספר הרישיון.
3.6.7. יובהר כי יכול מרשם אלקטרוני להיות מנופק באופן חלקי, כך שלא כל התרופות הרשומות במרשם נופקו, ובלבד שישנו תיעוד מלא וברור של התרופות שנופקו. ניפוק יתר התרופות הרשומות במרשם יכול להיעשות במועד אחר.

4. <u>אבטחת מידע:</u>

הוראות אבטחת מידע מפורטות בנספחים לנוהל זה:

- **נספח א -** הנחיות המנהל להסדרים הנדרשים ליצירת ושמירת החתימות, מאגר המרשמים וסוגי החומרה ופרוטוקולי אבטחת מידע.
- **נספח ב** - הנחיות המנהל לשימוש במערכות חומרה ותוכנה מהימנות ואבטחתן.
- **נספח ג'** - הסיכונים וההתחייבויות של הרופא המשתמש בחתימה אלקטרונית.
- **נספח ד'** – תקנות הרופאים (מתן מרשם) – כולל התיקון בדבר חתימה אלקטרונית.

שם הנוהל: מרשמים אלקטרוניים וחתימה אלקטרונית בקופת החולים ובמוסד רפואי		
תאריך הנוהל: יולי 2013	מספר הנוהל: 107	עמוד 6 מתוך 23

5. <u>אחריות לביצוע:</u>

- מנהלי קופות החולים
- מנהלי מוסדות רפואיים
- מנהלי אגפי מחשוב של קופות חולים ומוסדות רפואיים

6. <u>מסמכים ישימים:</u>

- תקנות הרופאים (מתן מרשם), התשמ"א-1981 כולל תיקון תשע"ב בעניין חתימה אלקטרונית
- חוק חתימה אלקטרונית, התשס"א-2001[1];
- תקנות חתימה אלקטרוניות תקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס"ב-2001

7. <u>תפוצה:</u>

מנכ"ל משרד הבריאות
המשנה למנכ"ל משרד הבריאות
סמנכ"ל מידע ומחשוב, משרד הבריאות
ראש אגף הרוקחות, משרד הבריאות
היועצת המשפטית, משרד הבריאות
רוקחים מחוזיים: י-ם, ת"א, חיפה, מרכז, צפון, דרום
המכון לביקורת ולתקנים של חומרי רפואה
הסתדרות הרוקחים ענף בתי המרקחת
מוסדות רפואיים: שירותי רוקחות, מנהלי אבטחת מידע
קופות החולים: שירותי הרוקחות , שירותי אבטחת מידע
רשתות הפארמים
אגוד הרוקחים בהסתדרות
ארגון הרוקחות בישראל
ענף הכימיה והפרמצבטיקה- התאחדות התעשיינים בישראל
ענף הכימיה והפרמצבטיקה –אגוד לשכות המסחר

[1] ס"ח התשס"א, עמ' 210.

שם הנוהל: מרשמים אלקטרוניים וחתימה אלקטרונית בקופת החולים ובמוסד רפואי		
תאריך הנוהל: יולי 2013	**מספר הנוהל: 107**	**עמוד 7 מתוך 23**

8. <u>תחולה:</u>

נוהל זה בתוקף החל מיום **01.06.2014.**

<u>כותבי הנוהל</u>:	**<u>תפקיד:</u>**	**<u>חתימה ותאריך</u>:**
מגר' אלי מרום	סגן מנהל אגף הרוקחות	
עו"ד טליה אגמון	לשכת היועץ המשפטי משרד הבריאות	28/7/2013
<u>מאשר הנוהל</u>:	**<u>תפקיד</u>:**	**<u>חתימה ותאריך</u>:**
פרופ' רוני גמזו	מנכ"ל משרד הבריאות	

שם הנוהל: מרשמים אלקטרוניים וחתימה אלקטרונית בקופת החולים ובמוסד רפואי		
תאריך הנוהל: יולי 2013	מספר הנוהל: 107	עמוד 8 מתוך 23

נספח א -

הנחיות המנהל להסדרים הנדרשים ליצירת ושמירת החתימות, מאגר המרשמים וסוגי החומרה ופרוטוקולי אבטחת מידע

1. **כללי:**
מטרת הנספח הינה להציג את ההנחיות להנפקת התעודות האלקטרוניות וכן לשמירת החתימות, מאגר המרשמים.

2. **הגדרות:**

מונח	תיאור
כרטיס חכם	כרטיס חכם (Smart Card), הוא מחשב זעיר לכל דבר וענין עם יחידת עיבוד מרכזית (CPU), זיכרון וזכרון לא נדיף, המשמש לאחסון מאובטח של מפתחות פרטיים וציבוריים ולביצוע פעולות קריפטוגרפיות מצומצמות. כרטיס חכם חייב לעמוד בתקן FIPS 140-2
עמדת הנפקה	עמדת עבודה ממנה ניתן להנפיק כרטיס / תג. העמדה כוללת את תוכנת הניהול, מדפסת כרטיסים חכמים ומצלמה
קוראי כרטיסים חכמים	התקן המקשר בין תחנת המשתמש לכרטיס עצמו (קורא נפרד / מקלדת חכמה המשלבת קורא כרטיסים חכמים).
LDAP	פרוטוקול לניהול משתמשים מבוסס גישה ל- Directory
Directory Server	בסיס נתוני המשתמשים
CA (Certificate Authority)	רשות תעודות Certificate Authority המבצעת חתימה דיגיטאלית על מפתחות ציבוריים באמצעות הנפקת תעודה דיגיטאלית. שימוש ברשות מאשרת מאפשרת מניעת זיוף והתחזות למפתחות ציבוריים של משתמשים.
PKI	Public Key infrastructure - המושג הכללי המתאר את פתרון ההצפנה והחתימה הדיגיטאלית המבוסס על אלגוריתם הצפנה אסימטרית ושימוש במפתחות ציבוריים וגורם מאשר לצורך שירותי הזדהות, הצפנה (שלמות, אמינות וחסיון נתונים), מניעת התכחשות, ניהול מפתחות יעיל וסקלביליות.
IDM	**Identity Management** – מערכת ניהול הרשאות וזהויות לניהול מחזור החיים של המשתמש החל מכניסתו לארגון, ממשיך בהפסקות עבודה יזומות (כגון חופשה ארוכה) וכלה בסיום עבודה והכל בהתאם לתפקידו בכל רגע נתון בארגון.
חתימה אלקטרונית מאובטחת	כהגדרתה בחוק חתימה אלקטרונית, התשס"א-2001 ;
חתימה אלקטרונית מאושרת	כהגדרתה בחוק חתימה אלקטרונית, התשס"א-2001 ;
HSM	רכיב ה-HSM[2] הוא רכיב קריפטוגרפי בחומרה, העומד בתקן FIPS 140-2 Level 3, בו נשמרים מפתחות הצפנה וממומשים אלגוריתמים קריפטוגרפים.

[2] Hardware Security Module With FIPS140-2 Compliant TRSM — HSM

שם הנוהל: מרשמים אלקטרוניים וחתימה אלקטרונית בקופת החולים ובמוסד רפואי		
תאריך הנוהל: יולי 2013	**מספר הנוהל: 107**	**עמוד 9 מתוך 23**

מונח	תיאור
registration RA authority	רשות רישום
תעודה דיגיטאלית (certificate)	רכיב לוגי המאפשר הזדהות חכמה, שניתן להתקין על גבי השבב (צ'יפ) בכרטיס חכם או על גבי שרת חיתום מרכזי (רשתי).
אלגוריתם קריפטוגרפי	שיטה מתמטית ברורה לביצוע פעולות קריפטוגרפיות המגדירה הן את אופן הפעולה והן את חוזק (גודל) המפתח. אלגוריתם זה חייב לעמוד ברשימה של ארגון ה-NSA לאלגוריתמים הפתוחים המורשים לביצוע פעולות הצפנה מסווגות, כפי שמתעדכנת מעת לעת באתר: http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml דוגמאות לאלגוריתמים מאושרים בשנת 2013: AES 128, RSA2048, SHA256, DSA2048
מאגר התעודות הפסולות (CRL)	מאגר התעודות הפסולות (Certificate Revocation List) יכלול את התעודות שבוטלו במערך. ביטול תעודות יבוצע בין היתר בשל המקרים הבאים: אובדן כרטיס חכם, חשיפת מפתח פרטי של בעל התעודה, חשיפת מפתח פרטי של CA, החלפת כרטיס חכם / תעודה, הסרת הרשאות כללית וכד'.
הרשאות מבוססות תפקיד (RBAC)	גישה המבוססת Role Based Access Control הינה מתן גישה על פי הרשאה המבוססת תפקיד בפועל, קרי הרשאה על פי צורך (Need to have basis) המחולקת לקבוצות לוגיות המגדירות ההרשאות והפעולות שמשתמש יכול לבצע באמצעות התעודה והכרטיס על פי צרכי תפקידו.

שם הנוהל: מרשמים אלקטרוניים וחתימה אלקטרונית בקופת החולים ובמוסד רפואי		
תאריך הנוהל: יולי 2013	מספר הנוהל: 107	עמוד 10 מתוך 23

3. תהליכי הנפקת תעודה ו/או כרטיס חכם:

3.1. תהליך רישום וזיהוי:

3.1.1. הגורמים הרלוונטיים בארגון יבדקו במערכת המרכזית הארגונית את זכאותו של כל רופא להנפקת תעודה דיגיטאלית לצורך חתימה אלקטרונית על מרשמים, ויקבעו את ההרשאות הנחוצות לו ומגבלות בהרשאותיו לפי החלטת הארגון/המוסד.

3.1.2. יוגדר גורם אחראי על הנפקת הכרטיסים.

3.1.3. לפני הנפקת תעודה דיגיטאלית לרופא - הרופא יזדהה בפני הגורם המנפיק באמצעות הצגת שתי תעודות מזהות כמפורט להלן, או לפי הוראות רמו"ט לגורמים מאשרים:

(א) תעודת זהות ישראלית;

(ב) אחת מאלה: רישיון נהיגה ישראלי בתוקף, או דרכון ישראלי בתוקף, כרטיס עובד של הקופה או המוסד הרפואי המסוים בו תונפק התעודה ובלבד שהוא כולל תמונה, או תעודה מזהה אחרת שהונפקה על ידי אותו גורם ארגוני שאושר על ידיו מראש לצורך זה (והכוללת תמונה).

3.1.4. הארגון או המוסד לא ינפיק לרופא יותר מתעודה אחת, לצורך חתימה על מרשמים. תעודה חלופית תונפק רק לאחר ביטול של תעודה קודמת.

3.1.5. בארגון או מוסד שיש בו כבר מערכת של כרטיסים חכמים לצרכי זיהוי וצרכים ארגוניים שונים, ניתן להשתמש באותו כרטיס חכם כבסיס להרשאה למתן מרשמים באותו ארגון, ובלבד שאותו כרטיס עומד בדרישות החוק ונוהל זה.

3.1.6. המערכת תוגדר כך שהגורם המנפיק לא יוכל לקרוא או לקבל גישה למפתח הפרטי של הרופא שיחולל בתוך הכרטיס החכם בלבד ללא יכולת ייצוא החוצה.

3.2. אחריות והוראות כלליות

3.2.1. ככלל, האחריות לשימוש לרעה באמצעי החתימה הינה של הארגון המנפיק, אלא אם הוכח כי אמצעי החתימה היה נתון לשליטתו הבלעדית של הרופא.

3.2.2. האחריות לשימוש באמצעי חתימה שהותקן על גבי שרת רשתי ולא על גבי כרטיס חכם - היא ככלל, של המוסד המחזיק בשרת.

3.2.3. אסור שתהא אפשרות למנהל הרשת או כל גורם אדמיניסטרטיבי אפשרות לחתום בשם רופא או לבצע שימוש באף אחד מהמפתחות הפרטיים על הרכיבים הרשתיים.

3.2.4. חובה שיהיו חיווי ובקרה מלאה על התהליך.

3.2.5. בתעודה דיגיטאלית שמונפקת על ידי ארגון/מוסד רפואי שאינו גורם מאשר לפי חוק חתימה אלקטרונית, ואינו המדינה - , יצוין עליה אם היא תשמש לחתימה על מרשמים בלבד או למטרות נוספות, וכן יצוין אם התעודה מותקנת על גבי שרת חתימות.

3.2.6. אובדן כרטיס מחייב הודעה מידית לגורם המנפיק, לשם ביטול התעודה הדיגיטאלית ורישומה במאגר התעודות הפסולות (CRL).

3.2.7. רופא שמסר הודעה על אבדן התעודה או הכרטיס לגורם המנפיק בהתאם לנוהל - קיים את חובתו למסור הודעה לכל מי שסביר שיסתמך על חתימתו האלקטרונית לפי סעיף 7(ב) לחוק חתימה אלקטרונית.

שם הנוהל: מרשמים אלקטרוניים וחתימה אלקטרונית בקופת החולים ובמוסד רפואי		
תאריך הנוהל: יולי 2013	מספר הנוהל: 107	עמוד 11 מתוך 23

3.3. <u>תהליך ההנפקה של כרטיסים חכמים בעמדת המנפיק:</u>

3.3.1. לאחר קבלת אישור הפרופיל הרלוונטי של הרופא מגורם ההרשאות יזמן הגורם המנפיק את הרופא לעמדת הנפקה.
3.3.2. רופא יגיע לאחת מעמדות ההנפקה, עם הזימון שקיבל.
3.3.3. הרופא יזדהה בעמדת ההנפקה באמצעות שני אמצעי זיהוי כמפורט בסעיף 3.1.2.
3.3.4. המנפיק יוודא כי כלל הפרטים הנדרשים קיימים במערכת ונכונים.
3.3.5. יש לתת עדיפות לשימוש בכרטיס חכם הנושא תמונה.
3.3.6. המנפיק ישייך את הגורם לפרופיל ההרשאות שאושרו לו בעוד מועד.
3.3.7. הכרטיס יונפק.
3.3.8. לפני קבלת הכרטיס יקבל הרופא טופס קבלה והסכמה שיכלול את כלל הסיכונים האבטחתיים הכרוכים בשימוש בתעודה הדיגיטלית, לפי דוגמא כמפורט בנספח ג', ויחתום על קבלת הכרטיס ואישור ידיעת הכללים, בחתימת ידו.
3.3.9. המנפיק יבצע הנפקה של הכרטיס, הרופא יקליד PIN (קוד אישי) מתאים או טביעת אצבע ביומטרית והמערכת תעודכן בפרטים אלה. הקלדת PIN תבוצע באופן שלא יאפשר לגורם המנפיק לצפות בה.

3.4. <u>תהליך ניפוק תעודות וכרטיסים באצווה:</u>

3.4.1. הנפקה באצווה הינה הנפקה מרוכזת של מספר תעודות ו/או כרטיסים חכמים מראש, על ידי גורם ארגוני המנפיק עבור רופאיו
3.4.2. לפני הגעת הרופאים לאתר החלוקה של כרטיסים שהונפקו באצווה תועבר בקשת הנפקה לגורם האחראי על הנפקת הכרטיסים (המנפיק) לביצוע הנפקה מרוכזת של מספר תעודות ו/או כרטיסים.
3.4.3. המנפיק יוודא כי פרטי הרופאים הרלוונטיים קיימים במערכת ושניתן לבצע הנפקה לכלל האצווה.
3.4.4. אם חסרות תמונות במערכת, יעביר המנפיק בקשה לגורם האחראי במוסד הרפואי או בקופה לקבלת תמונות והכנסתן למערכת (כרטיסים חכמים יונפקו רק עם תמונות).
3.4.5. לאחר שיגיעו הכרטיסים לידי המנפיק, הוא יבצע הנפקת תעודה דיגיטאלית בשבב שעל גבי הכרטיסים ויקבע קוד אישי ראשוני קבוע לכלל הכרטיסים.
3.4.6. בשלב זה לא ניתן יהיה לבצע חיתום דיגיטאלי באמצעות הכרטיס, למשתמש לא יהיו הרשאות, ברמה הטכנולוגית, וזאת כדי לאפשר שליטה בלעדית של הרופא מקבל הכרטיס, בחתימתו.
3.4.7. המנפיק ישלח את הכרטיסים אל הגורם המפיץ בקופ"ח / המוסד הרפואי. השליחות תבוצע באופן מאובטח שהוא אחד מאלה:
(א) באמצעות גורם אנושי מוסמך ומאושר על ידי מנב"ט או מנהל אבטחת המידע של הארגון;
(ב) באמצעות שליחים - בלדרות מאובטחת ומאושרת על ידי מנב"ט או מנהל אבטחת המידע של הארגון.

שם הנוהל: מרשמים אלקטרוניים וחתימה אלקטרונית בקופת החולים ובמוסד רפואי		
תאריך הנוהל: יולי 2013	**מספר הנוהל: 107**	**עמוד 12 מתוך 23**

3.4.8. לאחר שיקבל את הכרטיסים לידו, בטרם העברת הכרטיס לידי הרופא, הגורם המפיץ יזהה את הרופא על בסיס שני מסמכים כמפורט בסעיף 3.1.2, יעזור לרופא להחליף את סיסמתו בדרך שבה המפיץ לא יכול לדעת את הסיסמה החדשה.

3.4.9. לאחר שהרופא החליף את סיסמתו ולפני קבלת הכרטיס יקבל הרופא טופס קבלה והסכמה שיכלול את כלל הסיכונים האבטחתיים הכרוכים בשימוש בתעודה הדיגיטלית, לפי דוגמא כמפורט בנספח ג', ויחתום על קבלת הכרטיס ואישור ידיעת הכללים, בחתימת ידו.

3.4.10. המפיץ יאשר למנפיק לשייך את זיהוי הרופא באמצעות התעודה החכמה להרשאות.

3.4.11. העתק הטופס החתום (סרוק) יועבר למנפיק והמקור יישמר אצל המפיץ.

3.5. <u>אחסון תעודות דיגיטליות:</u>

3.5.1. הנפקת התעודות הדיגיטליות תתבצע על רכיב חומרה העומד בדרישות לחתימה אלקטרונית מאובטחת לפי חוק חתימה אלקטרונית ותקנות חתימה אלקטרונית (חתימה אלקטרונית מאובטחת, מערכות חומרה ותוכנה ובדיקת בקשות), התשס"ב-2001.

3.5.2. רכיב החומרה יוכל להיות רכיב אישי של הגורם כדוגמת כרטיס חכם / טוקן או לחלופין על רכיב מרכזי (שרת חיתום מרכזי – HSM).

3.5.3. אם אמצעי חתימה (מפתחות) מותקנים על גבי שרת רשתי מרכזי ולא על גבי כרטיס חכם - האחריות לשימוש בחתימה היא, ככלל, של הארגון/המוסד המחזיק בשרת שעליו החתימות. על הארגון מוטלת חובה לקבוע הוראות אבטחה למניעת שימוש לרעה בחתימה הרשתית כדי להבטיח את שליטתו הבלעדית של הרופא בחתימה ולמנוע חתימה ע"י מנהל רשת בחתימת הרופא או כל שימוש במפתחות הפרטיים על הרכיבים הרשתיים, על ידי מי שאינו מורשה לכך, ובכלל זה קיום בקרה מלאה על התהליך, והכל – בהתאם להנחיות של רמו"ט לעניין זה.

שם הנוהל: מרשמים אלקטרוניים וחתימה אלקטרונית בקופת החולים ובמוסד רפואי		
תאריך הנוהל: יולי 2013	מספר הנוהל: 107	עמוד 13 מתוך 23

3.6. תהליך הנפקת תעודות דיגיטליות:

3.6.1. במטרה להנפיק תעודות דיגיטליות לרופאים לשם חתימה על מרשמים, שלא באמצעות גורם מאשר לפי חוק, הארגון/מוסד רפואי יקים תשתית PKI ארגונית שתאובטח לרמת אבטחה כנדרש בחוק.

3.6.2. תשתית ה-PKI הארגונית תעבור בקרה של גורם צד ג' (גורם לא תלוי) בהקמתה, ולאחר מכן כל חצי שנה תבוצע בקרה לעמידה ברמת האבטחה הנדרשת.

3.6.3. אם הארגון הוא ממשלתי ניתן יהיה להשתמש בתעודות המונפקות על ידי הממשלה, ובהתאמה לכך לא נדרש להקים תשתית PKI ארגונית נוספת.

3.6.4. הארגון יבצע זיהוי של הגורם, ומפתחות (ציבורי ופרטי) יחוללו על הכרטיס החכם / הטוקן / HSM.

3.6.5. המפתח הציבורי ישלח לשרת המאשר (CA) והתעודה תתקבל מהשרת המאשר לרכיב על בסיס תבנית מאובטחת שתוגדר מראש לפי ההרשאות המתאימות (והרולים המשויכים) כאמור לעיל.

3.6.6. אם הרכיב הינו רכיב אישי (כרטיס חכם / טוקן) - הגורם יבחר סיסמא אשר באמצעותה יבצע זיהוי לרכיב (ניתן לבצע שימוש בזיהוי חד חד ערכי כדוגמת ביומטרי). אם הרכיב הינו רכיב מרכזי יזדהה הגורם באופן חד חד ערכי באמצעות התעודה הקיימת על כרטיסו החכם אל ה-HSM / שרת החיתום.

3.6.7. כל מקבל תעודה יחתום על טפסי אחריות לשמירה על הסיסמא לרכיב וכן על השלכות האבטחתיות אם הכרטיס חכם יאבד / מחשבו של הגורם ייפרץ.

3.7. הנפקה מחדש של תעודה הדיגיטליות:

3.7.1. חידוש התעודה יבוצע לאחר לא יותר מארבע שנים;

3.7.2. החידוש יכול להתבצע באופן מרוחק תוך התבססות על התעודה הקיימת (רק אם התעודה עדיין לא פגה/פקעה), או חידוש מקומי על ידי הגעת הרופא לגורם המנפיק (או הגעת הגורם המנפיק לרופא).

3.7.3. תהליך החידוש הינו תהליך לחידוש התעודות בלבד. אם נדרש לחולל מפתחות מחדש - יבוצע כל תהליך ההנפקה מחדש.

3.7.4. תהליך החידוש של תעודה שטרם פגה יבוצע בצורה אוטומטית מעמדת המשתמש. התהליך יתבסס על זיהוי התעודה שכבר הונפקה לרופא.

3.7.5. אם התעודה לא חודשה בזמן יש לבצע זיהוי של המשתמש לפי סעיף 3.1. לעיל.

3.7.6. זמן סביר שיקבע לפני מועד בו יפוג תוקף התעודה יקבל המשתמש הודעה על כך לפי נוהלים פנימיים שיקבעו בארגון.

שם הנוהל: מרשמים אלקטרוניים וחתימה אלקטרונית בקופת החולים ובמוסד רפואי		
תאריך הנוהל: יולי 2013	מספר הנוהל: 107	עמוד 14 מתוך 23

3.8. <u>שחרור כרטיס חכם:</u>

3.8.1. הכרטיס ינעל לאחר לא יותר מ-10 נסיונות כושלים לכניסה, וישוחרר ובאחת הדרכים הבאות:
3.8.1.1. בעמדת מנפיק - לאחר זיהוי בשני מסמכים מזהים כאמור בסעיף 3.1.2;
3.8.1.2. בעמדת שחרור ייעודית;
3.8.1.3. מרחוק על ידי מרכז התמיכה; לאחר זיהוי המשתמש כמפורט להלן;

3.8.2. שחרור הכרטיס בעמדת שחרור, או מרחוק, יבוצע בכפוף לזיהוי הכולל מענה ל"שאלות סבתא", באמצעות מנגנון Challenge-Response ובאמצעות חיוג למרכז התמיכה למספר טלפון של הרופא שהוגדר מראש בלבד.

3.8.3. לאחר שחרור כרטיס באמצעות עמדת שחרור או מרחוק - יידרש המשתמש להחליף את הקוד האישי.

3.9. <u>אבדן או גניבת הכרטיס:</u>

3.9.1. במקרה של אובדן או גניבת הכרטיס באחריות הרופא להודיע על כך לגורם המנפיק או למי שקבע אותו גורם - באופן מיידי.

3.9.2. המנפיק יפעל באופן מיידי כדלהלן:
(א) יבטל את הכרטיס במערכת, ובמקביל יזמין כרטיס חדש.
(ב) יסיר את הרופא מפרופיל ההרשאות עד להנפקת תעודה חלופית.
(ג) יבטל את תוקף התעודה הדיגיטאלית.
(ד) יפרסם מיידית את התעודה במאגר התעודות המבוטלות (CRL) ויפיץ למקומות בהם ה-CRL מפורסם.
(ה) יבצע כל פעולה נוספת המקובלת במוסד אליו הוא שייך במקרה של אבדן ציוד או גניבה.

שם הנוהל: מרשמים אלקטרוניים וחתימה אלקטרונית בקופת החולים ובמוסד רפואי		
תאריך הנוהל: יולי 2013	מספר הנוהל: 107	עמוד 15 מתוך 23

3.10. <u>גילוי סיסמה לגורם שאינו בעל הכרטיס:</u>

3.10.1. חל איסור חמור על רופא להעביר את הכרטיס החכם שלו לכל גורם למעט למפיץ/מנפיק לצורך בדיקת תקינות.
3.10.2. אסור לרופא לגלות את סיסמתו (PIN – קוד אישי) לכל גורם אחר, כולל למפיץ/מנפיק.
3.10.3. אם יש חשש או חשד כי הסיסמה נתגלתה לגורם אחר, באחריות הרופא להחליף את הסיסמא באופן מיידי.
3.10.4. אם לרופא יש חשש או חשד כי גורם אחר השתמש בכרטיס החכם שלו לצורך ביצוע חתימה דיגיטאלית בשמו, באחריותו להודיע על כך מיידית לממונה הביטחון במוסד הרפואי / קופת החולים או למנהל אבטחת המידע בארגונו. במקרה כזה יש לפעול לפי האמור בסעיף 3.8 לנוהל (אובדן או גניבת כרטיס).

3.11. <u>כרטיס שנשכח או תקול:</u>

3.11.1. ככלל, רופא ששכח את הכרטיס או שכרטיסו תקול יעבוד באותו היום עם מרשמים ידניים.
3.11.2. ניתן להנפיק כרטיס חלופי זמני רק באתרים שיוגדרו על ידי הארגון וזאת על ידי הגעה פיזית של הרופא וזיהויו כנדרש בלבד.
3.11.3. לפני הנפקת כרטיס זמני מערכת ההנפקה תוודא קיום תעודה והרשאות תקפים.
3.11.4. אין להנפיק יותר מכרטיס זמני אחד. כרטיס זמני יהיה תקף לתקופה מוגבלת לפי הנסיבות ויש להחזירו לעמדת המנפיק בגמר השימוש.
3.11.5. הקידוד של הפס המגנטי יהיה בהתאמה לכרטיס החסר. המערכת תשייך את התעודה הדיגיטלית שהונפקה למשתמש ב- Active Directory.
3.11.6. בגמר השימוש הכרטיס הזמני יפורמט וניתן יהיה לקודדו מחדש.
3.11.7. אם התקלה בכרטיס אינה נפתרת יש להנפיק כרטיס חדש ולבטל את הכרטיס התקול לפי הוראות נוהל זה.
3.11.8. אם מסתבר שהכרטיס ש"נשכח" למעשה אבד - יש לפעול לפי סעיף 3.10 לעיל.

4. <u>סוגי החומרה ופרוטוקולי אבטחת מידע:</u>

4.1. סוגי החומרה ופרוטוקולי אבטחת המידע יקבעו בהתאם לחוק חתימה אלקטרונית ולתקנותיו העדכניות, ובכל מקרה לא יפחתו מעמידה בתקן FIPS 140-2 Level 3 לHSM (לא רק יכולת המכונה אלא הפעלת שירות FIPS-140 בפועל במכונה), 140-2 לכרטיסים, ובהגדרות NSA לאלגוריתמים מיושמים כאמור בפרק ההגדרות דלעיל.

5. כל שינויי או חריגה מההוראות בנספחים אלה חייב את אישור מנהל אבטחת המידע במשרד הבריאות.

שם הנוהל: מרשמים אלקטרוניים וחתימה אלקטרונית בקופת החולים ובמוסד רפואי		
תאריך הנוהל: יולי 2013	מספר הנוהל: 107	עמוד 16 מתוך 23

נספח ב -
הנחיות המנהל לשימוש במערכות חומרה ותוכנה מהימנות ואבטחתן ברמה מספקת

1. <u>מערכות חומרה ותוכנה מהימנות:</u>

1.1. תשתית ה- PKI הפנים-ארגונית תותאם לחוק חתימה אלקטרונית ולתקנותיו.
1.2. ההגדרות יפורטו באתר האינטרנט של משרד הבריאות בכתובת www.health.gov.il ;
1.3. בעת שינוי / עדכון של ההגדרות יופץ חוזר לגורמים הרלוונטים.

2. <u>הגדרות בסיסיות לתשתית:</u>

2.1. <u>ארכיטקטורה (פיסית ולוגית)</u>

2.1.1. תשתית ה-PKI תוקם בארון מחשוב ייעודי, עם כלל ההגנות הפיסיות הנדרשות על חדר מחשב. תהא בקרה מלאה על הגישה לתשתית (הן ויזואלית – מצלמות והן מחשובית).
2.1.2. התשתית תוקם בסגמנט נפרד לוגית באמצעות Firewall או לחלופין רשת וירטואלית מסגמנט השרתים ותחנות המשתמשים. עמדות ההנפקה יוגדרו ברשת וירטואלית נפרדת.
2.1.3. תשתית ה- PKI שתוקם תכלול מבנה של שניים / שלושה גורמים מאשרים Certificate Authority – הראשון ב-Offline והשני ב-Online.
2.1.3.1. ה-Root CA – יוקם לפחות ל-25 שנים. מפתח 4096.
2.1.3.2. ה-ICA – יוקם לפחות ל-13 שנים. מפתח 4096.
2.1.3.3. ה- OCA– יוקם לפחות ל-5 שנים. מפתח 4096.
2.1.4. ה-CA שיוקם יהא OCA ייעודי למשתמשים / רופאים.
2.1.5. במידת האפשר ה- Repository המרכזי יהיה ה- Active Directory הקיים בארגון, כאשר יקושר אליו ה-OCA המשרת את המשתמשים והמערכות.
2.1.6. כלל המפתחות הפרטיים של ה-CA-ים יחוללו על רכיב HSM. המפתחות יגובו על ידי רכיב HSM נוסף או לחלופין באמצעות כרטיס חכם שישמר בכספת פיסית אצל מנהל אבטחת המידע / קב"ט.
2.1.7. מבנה התעודה יהא בהתאם למבנה התעודה הממשלתית – http://www.gov.il/FirstGov/smartCard
2.1.8. תוקף התעודה יהא לשנתיים עד ארבע שנים, לפי החלטת הארגון.
2.1.9. ה"רשימה השחורה" – CRL תונפק ל-24 שעות עם עדכון Delta / הפצה מידי. הפצת ה-CRL תהא לכלל הגורמים הרלוונטיים, אך לא פחות משני מקומות מרכזיים.
2.1.10. גישה לתשתית ה-PKI תתאפשר רק לגורמים מורשים מסוימים בארגון, אשר יאושרו על ידי מנהל אבטחת מידע / קב"ט הארגון. אם ייגשו גורמים שאינם מורשים כדוגמת מנהלי המערכת (Administrators) יש ליידע את מנהל אבטחת המידע / קב"ט ועליהם לנקוט אמצעים לטיפול במערכת.
2.1.11. לא תינתן גישה לניהול מרוחק בפרוטוקולים שונים (כדוגמת RDP) למעט תפעול המערכת. תחזוקה ותמיכה של מערכות ההפעלה יבוצעו באופן מקומי או לחלופין באמצעות "שרת ניהול מאובטח" אשר יבקר ויקליט את ה-Session. אם לארגון ישנה גישה מרחוק ו/או גישה של ספקים / יצרנים – לא תהא גישה למערכת לעבודה מרחוק.
2.1.12. הנפקת תעודה תדרוש זיהוי עם כרטיס חכם / ביומטרי של המנפיק/ ה-RAO (Registration Authority Operator).
2.1.13. "מפתחות" ה-HSM יישמרו במחלקת אבטחת מידע / אצל הקב"ט הארגוני וכל גישה למפתחות תתועד.

שם הנוהל: מרשמים אלקטרוניים וחתימה אלקטרונית בקופת החולים ובמוסד רפואי		
תאריך הנוהל: יולי 2013	מספר הנוהל: 107	עמוד 17 מתוך 23

2.1.14. אם נדרשת סביבת פיתוח / ניסוי - יוקמו סביבות עבודה שונות לפיתוח, ניסוי וייצור אשר לא יקושרו זו לזו. למפתחי המערכות תהא גישה רק למערכות הפיתוח והניסוי ללא גישה למערכת הייצור. העברת תיקונים וגרסאות במערכות תבוצע בתהליך של בדיקת התיקון במערכת הפיתוח, תהליך ניסוי ולאחר מכן העברה לייצור.

2.2. <u>זיהוי:</u>

2.2.1. הזיהוי אל מול כל מערכת ניהול הכרטיסים יבוצע באמצעות זיהוי חד-חד-ערכי של המשתמש - כרטיס חכם עם תעודות דיגיטליות או לחלופין זיהוי ביומטרי.

2.2.2. מערכת הכרטיסים תתמוך בזיהוי כפול (גש"ם) - שני משתמשים שידרשו להזדהות אל מול המערכת בעלי כרטיסים חכמים ומפתחות שונים, המערכת לא תאפשר פעולות ללא הזיהוי הכפול או לחלופין ב-Split Keys / Secret Splitting – כניסה של שני משתמשים כאשר כל אחד מהם מחזיק חלק מהמפתח לכניסה אל המערכת.

2.2.3. זיהוי המערכת אל מול רכיבי תשתית ה-PKI ו/או רכיבי אבטחה נוספים יבוצע תוך יישום זיהוי דו כיווני מבוסס תעודות דיגיטליות באופן מאובטח (זיהוי, הצפנה וחתימת שדר).

2.3. <u>הרשאות:</u>

2.3.1. מערכת הנפקת הכרטיסים תכלול לפחות ארבע רמות של הרשאה על בסיס ה"צורך לדעת" – need to know (מנהל מערכת, מפעיל, אורח ומבקר).

2.3.2. לא יעשה שימוש במשתמש אפליקטיבי אלא כלל המשתמשים יהיו מבוססי Active Directory או כלי מקביל לניהול משתמשים.

2.4. <u>ניהול המערכת:</u>

2.4.1. ניהול המערכת יבוצע מקומית ומרוחק. ניהול המערכת נדרש להתבצע באופן מאובטח - זיהוי המשתמש חד חד ערכית והצפנת התווך.

2.4.2. נדרש לבצע הגבלת התחנות מהן יבוצע ניהול המערכת באמצעות הגבלת כתובת IP.

2.5. <u>בקרה:</u>

2.5.1. נדרש כי יבוצע חיווי הן על כלל הפעולות המבוצעות במערכת והן על פעולות אבטחתיות. תיאור החיווי הנדרש:

2.5.1.1. בקרה על כניסה / יציאה מהמערכת (Login/Logoff)

2.5.1.2. בקרה על כישלונות בגישה אל המערכת וסיבתה - שגיאה בסיסמא, משתמש חסום וכדומה.

2.5.1.3. תהליכים במערכת - תהליך הנפקה / חידוש / שלילה / השהייה / שחרור מנעילה וכו' - על התהליכים לכלול את מספר הכרטיס, שם המשתמש, הפעולה שבוצע, תאריך ושעה, הגורם המבצע, הצלחה / כשלון בתהליך.

2.5.1.4. ניהול המערכת - יצירת פרופיל הרשאות, שינוי פרופיל הרשאות, מתן הרשאות למשתמש במערכת, הגדרות במערכת וכדומה - על כל פעולה נדרש לתעד את הגורם המבצע, תאריך ושעת ביצוע, כישלון / הצלחה בביצוע.

2.5.1.5. סיסמאות לכרטיסים - הנפקת סיסמא, החלפה, חידוש, וכדומה.

שם הנוהל: מרשמים אלקטרוניים וחתימה אלקטרונית בקופת החולים ובמוסד רפואי		
תאריך הנוהל: יולי 2013	מספר הנוהל: 107	עמוד 18 מתוך 23

2.5.1.6. גישה לקובץ הלוג - גישה לקובץ - משתמש, תאריך ושעה. ביצוע פעולה על הקובץ - משתמש, תאריך ושעה.

2.5.2. על החיווי להיות "Tamper proofed" למניעת שינוי על-ידי גורם חיצוני.

2.5.3. כל גישה למערכת שתתועד תשמר ותשלח למערכת מרכזית לבקרה ולרבות כל פעולת חילול מפתחות, חתימת מפתחות, הפקת תעודות, גישה לוגית או פיסית לליבת המערכת (HSM, CA), גישה לארון השרתים - תגרור בקרה ורישום בקובץ יומן.

2.5.4. נוהל חריגים - יופעל נוהל טיפול באירוע חריג וכל אירוע הקשור לתשתית ה-PKI ידווח למנהל אבטחת המידע במשרד הבריאות.

2.6. <u>נהלים:</u>

2.6.1. נוהל תפעול התשתית – על כל ארגון לכתוב נוהל תפעול תשתית ה-PKI הארגונית.

2.6.2. נוהל BCP – על כל ארגון לכתוב נוהל BCP להפעלת תשתית ה-PKI הארגונית.

2.7. <u>הגדרת מדיניות אבטחה במערכת – הקשחה:</u>

2.7.1. על הארגון לבצע הקשחה לכלל המערכות המשולבות בהצעה - תשתית ה-PKI על כלל רכיביה ומערכת הניהול. רמת ההקשחה הנדרשת תהא בהתאם למדיניות ההקשחה של כל אחד מהרכיבים.

2.7.2. יש לבצע בדיקות חוסן לתשתית ה-PKI אחת לשישה חודשים.

שם הנוהל: מרשמים אלקטרוניים וחתימה אלקטרונית בקופת החולים ובמוסד רפואי		
תאריך הנוהל: יולי 2013	מספר הנוהל: 107	עמוד 19 מתוך 23

נספח ג –
הסיכונים וההתחייבויות של הרופא המשתמש בחתימה דיגיטאלית

1. <u>מטרה:</u>
מטרת הנוהל הינה הגדרת הסיכונים וההתחייבויות של הרופא בכל הקשור לכרטיס חכם.

2. <u>שיטה:</u>

2.1 **תיאור הסכנות הכרוכות בשימוש בחתימה אלקטרונית מאובטחת והחובות המוטלות על הרופא לפי חוק חתימה אלקטרונית:**

2.1.1 חתימה אלקטרונית הינה חתימה המבוצעת במחשב, או באמצעי אלקטרוני דומה, באופן טכנולוגי, ומחליפה את החתימה הידנית.

2.1.2 כפי שניתן לזייף חתימה ידנית ניתן באמצעים מסוימים ל"זייף" גם חתימה אלקטרונית. זיוף החתימה האלקטרונית יכול להתבצע בשני מצבים עיקריים: אחד- על ידי גניבת הכרטיס החכם המשמש כאמצעי חתימה עם הקוד הסודי והשני - על ידי שכפול הכרטיס החכם. גניבה של כרטיס והקוד הסודי לכרטיס תאפשר לגורם לא מורשה לחתום על מרשמים בשם הרופא.

2.1.3 לכן, נדרש לשמור על אבטחת הכרטיס החכם, הקוד הסודי וכל אמצעי אחר המשמש לחתימה אלקטרונית, על מנת שהחתימה תיחשב חתימה אלקטרונית מאובטחת.

2.1.4 חוק חתימה אלקטרונית קובע כי לחתימה אלקטרונית מאובטחת מעמד המשפטי זהה למעמד המשפטי של חתימה ידנית, אם מתקיימים התנאים המוגדרים בחוק והם: שהחתימה האלקטרונית היא חתימה ייחודית לבעל אמצעי החתימה, מאפשרת זיהוי של בעל אמצעי החתימה, הופקה באמצעי חתימה שנמצא בשליטה בלעדית של בעל החתימה, וכן מאפשרת זיהוי של כל שינוי שנערך במסר האלקטרוני לאחר שנחתם.

2.1.5 החובה המרכזית המוטלת על רופא שנופקה לו חתימה אלקטרונית היא לשמור על אמצעי החתימה (בד"כ כרטיס חכם), ולא לאפשר שימוש בו לאף גורם אחר פרט לרופא עצמו.

2.1.6 השמירה על אמצעי החתימה מתמקדת בשני נושאים עיקריים

(א) אחסון ושמירה נאותה על הכרטיס החכם (שמירתו במקום מאובטח במטרה למנוע גניבתו)

(ב) שמירה על הקוד הסודי המגן על ביצוע חתימה על ידי גורם לא מורשה – הן מפני גורמים עוינים והן מפני גורמים פנים ארגוניים שאינם מורשים לחתום על מרשמים (כגון צוות מינהלי וצוות מחשוב).

2.2 להלן מפורטת רשימת ההתחייבויות שיש להביא לידיעת הרופא ולהחתים אותו על קבלתה והבנתה – שמטרתן להבהיר לו שעליו לנקוט בכל האמצעים הסבירים לשם שמירה על אמצעי החתימה שלו ולשם מניעת שימוש בו בלא הרשאתו ולפרט חלק מן האמצעים שבאפשרותו לנקוט לשם כך:

☐ ידוע לי כי הכרטיס החכם שניתן לי מאפשר חתימה בשמי על מסמכים, ובפרט – על מרשמים אלקטרוניים ועלי לשמור אותו ולהגן עליו מפני אבדן, גניבה או שימוש על ידי מי שלא מורשה.

☐ ידוע לי כי אם אאבד את הכרטיס / לא אשמור עליו כראוי והכרטיס יאבד - כל מרשם אשר יחתם באמצעותו יחשב כמרשם תקין ובאחריותי.

☐ אני מתחייב לא להעביר את הכרטיס ו/או הסיסמא לכל אדם, כולל עובדי הארגון.

☐ אני מתחייב לא לגלות לאיש את פרטי ההתקשרות ברשת הארגון – כגון כתובות IP.

☐ אני מתחייב לנקוט בכל אמצעי הזהירות הסבירים על מנת לא לגרום נזק לארגון על ידי הפרת כללי הזהירות.

☐ אני מתחייב להודיע מיידית למנהל אבטחת המידע בארגון ו/ או למנב"ט אם נחשפה הסיסמא / נגנב הכרטיס / אבד הכרטיס וכו'.

☐ אני מתחייב לשמור את הכרטיס החכם באופן בטוח, ובנפרד מן הסיסמא.

שם הנוהל: מרשמים אלקטרוניים וחתימה אלקטרונית בקופת החולים ובמוסד רפואי		
תאריך הנוהל: יולי 2013	מספר הנוהל: 107	עמוד 20 מתוך 23

2.3 **הסבר מפורט כיצד ניתן לבטל את התעודה במידת הצורך:**

2.3.1 ביטול התעודה יעשה מול מנהל אבטחת המידע, או מנהל הבטחון (מנב"ט) בארגון או עובד מטעמם שהוסמך לכך.

2.3.2 על הרופא להודיע באופן אישי אל מרכז התמיכה או לחלופין להגיע פיזית למנב"ט, מנהל אבטחת מידע או עמדת הנפקה ולהודיע על אובדן / גניבת הכרטיס / הסיסמא.

2.3.3 מנהל אבטחת המידע, המנב"ט בארגון או בא כוחו יחל בתהליך לביטול הכרטיס. בעל התעודה יזוהה באמצעות תעודה זהות או רישיון נהיגה בתוקף. במידה ובעל התעודה הודיע טלפונית - הוא יזוהה באמצעות "שאלות הסבתא" (שאלות אשר מולאו בעת מתן הכרטיס).

2.3.4 כרטיס שאבד או נגנב יבוטל. כתוצאה מביטול כרטיס תישלח מיידית הודעה על הביטול למערכות הרלוונטיות וכן תוכנס התעודה הדיגיטלית לרשימה השחורה - CRL.

2.3.5 כדי להנפיק מיידית כרטיס חדש במקום המבוטל (במידת האפשר) - על הרופא להגיע אישית אל עמדת ההנפקה עם תעודת זהות ותעודה נוספת עם תמונה. אם הרופא הודיע טלפונית על אבדן/גניבת הכרטיס – לאחר זיהוי באמצעות "שאלות סבתא" יסוכם עימו כיצד יקבל את הכרטיס החלופי שיונפק לו.

2.4 **התחייבות הרופא להודיע למרכז התמיכה ו/או יחידת הביטחון מיד כשנודע לו כי נפגעה שליטתו באמצעי החתימה.**

על הרופא להתחייב על גבי טופס קבלת הכרטיס כי יודיע למנהל אבטחת המידע, או למנהל הבטחון בארגון או לאדם שהוסמך מטעמם לשם כך - מייד לאחר שגילה כי נגנבה הסיסמא לכרטיס / נגנב הכרטיס / אבד הכרטיס / בוצעה כל פעולה אחרת אשר תאפשר לגורם לא מורשה לעשות שימוש בכרטיס.

2.5 **הבהרת המשמעות המשפטית של עמידה בהתחייבויות**

על הגורם המנפיק להסביר לרופא מקבל התעודה, ולתעד זאת באופן ברור בטופס עליו יחתום הרופא, כי אם הרופא יקיים את כל חובותיו כאמור לעיל, הוא לא יהיה אחראי לנזק שנגרם עקב שימוש באמצעי החתימה שלו בלא הרשאתו, ואילו אי עמידה בהתחייבויות עלולה לגרור אחריות לכל נזק שנגרם עקב שימוש לא מורשה בכרטיס, הן לארגון והן למטופלים או לצד שלישי שהסתמך על תקפות החתימה.

שם הנוהל: מרשמים אלקטרוניים וחתימה אלקטרונית בקופת החולים ובמוסד רפואי		
תאריך הנוהל: יולי 2013	מספר הנוהל: 107	עמוד 21 מתוך 23

טופס התחייבות רופא בעת קבלת כרטיס חכם לחתימה אלקטרונית על מרשמים

שם פרטי:	שם משפחה:	ת.ז.
מספר רישיון:	טלפון:	נייד:
שם הארגון:	E-mail:	
הנמקה לצורך		
[ ] תעודה לצורך שימוש כאמצעי חתימה על מרשמים [ ] נוסף:		
אישור מנהל		
שם המנהל:	חתימה:	

אישור והתחייבות הרופא

א. ידוע לי כי הכרטיס החכם שניתן לי מאפשר חתימה בשמי על מסמכים, **ובפרט – על מרשמים אלקטרוניים**, ועליי לשמור אותו ולהגן עליו מפני אבדן, גניבה או שימוש על ידי מי שלא מורשה.

ב. ידוע לי כי אם אאבד את הכרטיס / לא אשמור עליו כראוי והכרטיס יאבד כל מרשם אשר יחתם באמצעותו יחשב כמרשם תקין ובאחריותי.

ג. אני מתחייב לא להעביר את הכרטיס ו/או הסיסמא לכל אדם, כולל עובדי הארגון.

ד. אני מתחייב לא לגלות לאיש את פרטי ההתקשרות בארגון – כגון כתובות IP

ה. אני מתחייב לנקוט בכל אמצעי הזהירות הסבירים, על מנת לא לגרום נזק לארגון על ידי הפרת כללי הזהירות.

ו. אני מתחייב להודיע מיידית למנהל אבטחת המידע ו/או לממונה הבטחון בארגון אם נחשפה הסיסמא / נגנב הכרטיס / אבד הכרטיס וכו'.

ז. אני מתחייב לשמור את הכרטיס החכם באופן בטוח ובנפרד מן הסיסמא.

הבהרה

הוסבר לי כי אם אקיים את כל חובותיי כאמור לעיל – לא אהיה אחראי לנזק שנגרם עקב שימוש באמצעי החתימה בלי הרשאה, אולם אם לא אעמוד בהתחייבויות אני עלול להימצא אחראי לכל נזק שיגרם עקב שימוש לא מורשה בכרטיס, הן לארגון והן למטופלים או לצד שלישי שהסתמך על תקפות החתימה.

תאריך:	שם הרופא:	חתימה:
אישור מערכות מידע		
שם המנהל/ת	חתימה	
אישור ביצוע		
תאריך	שם המבצע/ת	תפקיד
שם המשתמש שהוגדר במערכת		

שם הנוהל: מרשמים אלקטרוניים וחתימה אלקטרונית בקופת החולים ובמוסד רפואי		
תאריך הנוהל: יולי 2013	מספר הנוהל: 107	עמוד 22 מתוך 23

נספח ד –

תקנות הרופאים (מתן מרשם), התשמ"א-1981
(כולל תיקון התשע"א)

בתוקף סמכותי לפי סעיף 61(א) לפקודת הרופאים [נוסח חדש], התשל"ז-1976 (להלן - הפקודה), אני מתקין תקנות אלה:

1. הגדרות

בתקנות אלה -

"**אמצעי חתימה**", "חתימה אלקטרונית מאובטחת", "מסר אלקטרוני" - כהגדרתם בחוק חתימה אלקטרונית, התשס"א-2001;

"**מוסד רפואי**" - כהגדרתו בסעיף 24 לפקודת בריאות העם, 1940;

"**מרשם**" - הוראה בכתב חתומה ביד רופא לספק לאדם סם או תכשיר רפואי;

"**סם**" - כמשמעותו בפקודת הרוקחים;

"**קופת חולים**" - כהגדרתה בחוק ביטוח בריאות ממלכתי, התשנ"ד-1994;

"**רופא**" - רופא מורשה כמשמעותו בפקודה;

"**רשם הגורמים המאשרים**" - רשם כהגדרתו בחוק חתימה אלקטרונית, התשס"א-2001;

"**תכשיר רפואי**" - כמשמעותו בתקנות הרוקחים (תכשירים רפואיים), התשל"ח-1977.

2. הוראות לכתיבת מרשם רפואי

לא ייתן רופא מרשם לאדם אלא אם נרשמו בו באותיות ברורות כל אלה:

(1) שם הרופא, מקום עבודתו או מענו ומספרי הטלפון שלו;

(2) מספר רישיון רופא שלו;

(3) תאריך מתן המרשם;

(4) שם האדם שלו מיועד המרשם ומספר תעודת הזהות שלו, מינו וגילו אם הוא מתחת לגיל 18 שנים;

(5) פירוט מלא של הרכב הסם או שמו המקובל של התכשיר הרפואי באותיות לטיניות כתובות באותיות דפוס או מודפסות במכונת כתיבה;

(6) הוראות שימוש לפי המינון וצורת השימוש;

(7) הוראות חזרה על אותו מרשם אם יש צורך בכך;

(8) חתימה וחותמת הרופא.

שם הנוהל: מרשמים אלקטרוניים וחתימה אלקטרונית בקופת החולים ובמוסד רפואי		
תאריך הנוהל: יולי 2013	מספר הנוהל: 107	עמוד 23 מתוך 23

2א. חתימה אלקטרונית על מרשם:

לעניין תקנה 2(8) - על מרשם שהוא מסר אלקטרוני ניתן לחתום גם בחתימה אלקטרונית מאובטחת ובלבד שהתקיימו בחתימה כל אלה:

(1) החתימה האלקטרונית המאובטחת הונפקה לרופא על ידי קופת חולים או מוסד רפואי, לשימוש לצורך חתימתו על מרשמים שהם מסרים אלקטרוניים שהונפקו במהלך ובמסגרת עבודתו בקופת החולים או במוסד הרפואי בלבד;

(2) קופת החולים או המוסד הרפואי שהנפיקו את החתימה האלקטרונית המאובטחת מנהלים רישום מאובטח ומעודכן של הרופאים שהונפקה להם חתימה מאובטחת מטעמם ושל אמצעי אימות החתימה שלהם והכל תוך שימוש במערכות חומרה ותוכנה מהימנות ואבטחתן ברמה מספקת בהתאם להנחיות שהנחה המנהל;

(3) קופת החולים או המוסד הרפואי קבעו נהלים לשמירת אמצעי החתימה שהונפקו על ידם בידי בעל החתימה ומניעת שימוש לרעה בו ונוקטים אמצעים למניעת הסתמכות בתי מרקחת על חתימה אלקטרונית מאובטחת שבוטלה;

(4) הנחיות ונהלים כאמור בפסקאות (2) ו–(3) ייקבעו בהתייעצות עם רשם הגורמים המאשרים.

3. תוקף מרשם:

סם או תכשיר רפואי הניתנים על פי מרשם יינתנו פעם אחת בלבד, זולת אם הורה בו הרופא על מספר הפעמים שיש לחזור עליו; תוקפו של מרשם לא יעלה על שנה.