חוזר המנהל הכללי

משרד הבריאות

כ״ו בשבט, התשע״ה
15 פברואר, 2015
מס׳: 3/15

הנושא: <u>הגנה על מידע במערכות ממוחשבות במערכת הבריאות</u>

סימוכין: חוזר המנהל הכללי מס׳ 18/2012

הננו להביא בזאת לידיעתכם נוסח מעודכן לחוזר שבסימוכין. (עדכון החוזר בוצע בסעיף 8.3. שלהלן)

1. <u>רקע כללי</u>

1.1. נושא אבטחת המידע הרפואי הינו בעל חשיבות גבוהה, ומחייב את מערכת הבריאות הישראלית להבטיח עמידה בסטנדרטים הגבוהים ביותר.

1.2. עם התגברות האיומים על מערכות מבוססות מחשוב, ובכלל זה הטרור הקיברנטי, אנו נדרשים להגן על מערכות המחשוב הקריטיות של מערכת הבריאות בכל הרמות, על מנת להבטיח רצף טיפולי וניהולי כנדרש.

1.3. למערכת הבריאות קיימים איומים ייחודיים בתחום ההגנה על המידע הכוללים, בין השאר:

1.3.1. מניעת שירות (Denial of Service) - דבר אשר עשוי לפגוע במתן שירות רפואי חיוני בשגרה ובמיוחד בחירום. התלות הקיימת כיום במערכות מידע לצורך אספקת חלק משירותי הרפואה, הופכת איום זה למוחשי במיוחד.

1.3.2. גניבת מידע – מידע רפואי הינו מידע אישי רגיש ולגניבתו עשויות להיות השלכות קשות ברמה האישית וברמת האמון במוסדות הבריאות במדינה.

1.3.3. שיבוש מידע – הנזק אשר יכול להיגרם משינוי מידע בתיקו הקליני של מטופל עולה לעיתים על הנזק מגניבתו, היות ויכול להוות בסיס להחלטות רפואיות שגויות.

1.4. החוזר מציג באופן תמציתי את העקרונות לשיפור אבטחת המידע במוסדות רפואיים ובמשרד הבריאות.

2. **<u>מטרה:</u>**

הנחיית מוסדות הבריאות במדינת ישראל לפעול לאבטחת המידע שברשותן בהתאם לעקרונות ולסטנדרטים המפורטים בחוזר, וזאת על מנת להגן על המידע הרפואי הרגיש המופקד בידינו מדי יום.

3. **<u>הגדרות</u>**

"מוסד רפואי" – מרפאה, קופת חולים או בית חולים.

"מרפאה" - מרפאה בה פועלים חמישה מטפלים לפחות.

"ספק" – בהקשר לחוזר זה, ספק חיצוני המחזיק בידיו מידע רפואי או מידע על תשתיות מערכת הבריאות (פרטי רופאים וכיו"ב), בסטנדרטים להגנת מידע ממוחשב.

4. **<u>מסמכים ישימים</u>**

4.1. נוהל תשתיות תקשוב מאובטחות במב"ר;

4.2. נוהל פיתוח מאובטח של מערכות מידע במב"ר;

4.3. תקנים וטכנולוגיות אבטחת מידע בתוקף.

נהלים אלה הינם חלק מחוזר זה ומהווים הנחיות מקצועיות המתעדכנות מעת לעת ומתפרסמות באתר משרד הבריאות

5. **<u>אחריות ליישום</u>**

5.1. מנהלי בתי החולים;

5.2. מנהלי מרפאות;

5.3. מנהלי קופות החולים;

5.4. מנהל מוסד רפואי אחראי באופן אישי להגנה על המידע הרפואי הנוצר ונאגר במוסד (אין בהוראות חוזר זה כדי להטיל אחריות אישית מעבר לזו הקבועה בחוק);

5.5. מטפל העובד במסגרת בת פחות מחמישה מטפלים - אחראי באופן אישי להגנה על המידע הרפואי הנוצר והנאגר אצלו ביחס למטופליו.

6. **<u>ועדת היגוי וממונה אבטחת מידע</u>**

6.1. בכל מוסד רפואי ימנה מנהל המוסד ועדת היגוי לתחום הגנת המידע, בראשות מנהל המוסד.

6.2. ועדת ההיגוי תתכנס אחת לשנה לפחות ותתווה את מדיניות אבטחת המידע במוסד.

6.3. ועדת ההיגוי תעביר דווח שנתי על פעילותה להנהלת משרד הבריאות, אשר יישלח לא יאוחר מיום 31 לחודש מרץ, עבור השנה החולפת.

6.4. בכל מוסד רפואי ימנה מנהל המוסד ממונה אבטחת מידע וועדת היגוי לנושא אבטחת מידע.

6.5. מנהל המוסד יעביר את שמות ותפקידי חברי ועדת ההיגוי וממונה אבטחת המידע לממונה אבטחת המידע במשרד הבריאות עד לתאריך 31 למרץ מדי שנה.

7. <u>הסמכה לתקן אבטחת מידע למוסדות בריאות</u>

7.1. מוסדות הרפואה במדינת ישראל יוסמכו לתקן אבטחת מידע למערכות בריאות, ת"י 27799.

7.2. תהליכי אבטחת המידע יוטמעו בכלל המערכות הרלבנטיות של הארגון ובכלל זה: מערכות המידע, המכשור הרפואי, מערכות הלוגיסטיקה התומכות בתהליכי העבודה של המרכז הרפואי, מערכות כוח האדם ועוד.

7.3. החל מיום 1/1/2014 עמידה בתקן זה מהווה תנאי לקבלת רישיון למוסד רפואי ולחידוש הרישיון, ועמידה בתנאי התקן תיבדק במסגרת הבקרות שעורך משרד הבריאות.

8. <u>ספקים המספקים שירות למוסדות בריאות</u>

8.1. באחריות מנהל המוסד רפואי לוודא עמידתו של כל ספק חיצוני המחזיק בידיו מידע רפואי או מידע על תשתיות מערכת הבריאות (פרטי רופאים וכיו"ב), בסטנדרטים להגנת מידע ממוחשב.

8.2. מסירת גישה למידע אישי ורגיש לספקים חיצוניים תיעשה רק כשיש **הכרח** בדבר לשם ביצוע השירות, ובמידה המינימאלית האפשרית. החלטה על התקשרויות חיצוניות תיעשה בין היתר תוך שימת לב להיבטים של הגנת המידע האישי והרפואי.

8.3. עד ליום 31.12.2015- יש לתת עדיפות לספקים העומדים בתקן בינלאומי לאבטחת מידע – ISO 27001 או בתקן לאבטחת מידע במוסדות בריאות ISO 27799.
החל מה- 1.1.2016 יש לבצע התקשרויות רק עם ספקים העומדים בתקנים הנ"ל.

9. <u>אחריות לרישום מאגרי מידע</u>

9.1. באחריות מנהל המוסד רפואי לוודא רישום כלל מאגרי המידע שבאחריותו, בהתאם להנחיות רשם המאגרים במשרד המשפטים ועל פי הנחיות משרד הבריאות.

9.2. בהתאם להנחית רשם מאגרי מידע 1-2009 באחריות קופות החולים לוודא עמידתם של נותני שירותים חיצוניים בדרישות אבטחת המידע של המאגרים אליהם הם מקבלים גישה לצורך מתן השירות הרפואי.

10. <u>היבטים טכנולוגיים למימוש הגנה על המידע</u>

אבטחת מידע כמוגדר בתקן 27799: שמירה על סודיות, שלמות המידע ואמינותו, זמינות המידע ושרידותו - תיושם במערכות המידע הרפואיות הממוחשבות בבתי החולים, במרפאות בקהילה, ובמשרד הבריאות, בדגש על העקרונות הבאים:

אבטחת תשתיות

10.1. <u>אבטחת תשתיות</u> - תשתיות המידע, כגון: מערכות הפעלה בשרתים, בסיסי נתונים, תשתיות תוכנה יישומיות מרכזיות, רכיבי תקשורת יאובטחו בהתבסס על "נוהל תשתיות תקשוב מאובטחות במב"ר".

10.2. <u>כלי אבטחת מידע מאושרים</u> - רשימת הכלים והטכנולוגיות המאושרים לשימוש, כמפורט ב"תקנים וטכנולוגיות אבטחת מידע בתוקף", תתעדכן באופן תקופתי באחריות הממונה לאבטחת מידע במשרד הבריאות.

10.3. <u>טיפול במדיה</u> - מדיה הכוללת מידע רפואי אישי צריכה להיות מוגנת פיזית או שהמידע שבה יוצפן. נדרש לנטר מצבה ומיקומה של מדיה הכוללת מידע רפואי אישי לא מוצפן. מדיה מנוידת הכוללת מידע רפואי תוגן מפני גישה בלתי מורשית, באמצעות הצפנת המידע.

10.4. <u>הצפנת תווך</u> - גישה למידע רפואי של בתי החולים, מרפאות הקהילה ומשרד הבריאות ע"י צד שלישי, המאפשר עיבודו, אחסונו או העברתו, מחייב שילוב דרישות אבטחת מידע בתווך התקשורת, ובתשתיות המערכות.

10.5. <u>אבטחה פיזית</u> - ככל שהדבר רלוונטי, מעגל הגנה ראשון לרכיבי טכנולוגיית המידע יהיה מעגל אבטחה פיזי.

פיתוח מערכות מידע

10.6. <u>פיתוח מאובטח</u> - שילוב אבטחת מידע בכל רכש, פיתוח או שידרוג מערכות מידע, יתבסס על הדרישות לפיתוח מאובטח המנוסחות ב"נוהל פיתוח מערכות מידע מאובטח במב"ר".

10.7. אבטחת ממשקים - ייעשה שימוש במגוון שיטות וכלים טכנולוגיים להבטחת שלמות ואמינות הנתונים המועברים בין רכיבים שונים של מערכת, בין מערכות בתוך הארגון (ממשק פנימי) ומהארגון החוצה (ממשק חיצוני).

10.8. זיהוי המטופל - מערכות מידע רפואיות שבהן נשמר מידע רפואי אישי נדרשות לספק מידע המזהה באופן חד משמעי את המטופל, במטרה לסייע לוודא כי הרשומה האלקטרונית הרפואית שאוחזרה משויכת בוודאות למטופל הנמצא בטיפול.

נהלי שימוש והגדרת משתמשים במערכות ממוחשבות

10.9. הזדהות - חובת הזדהות חד ערכית ע"י משתמש בכניסה למערכות המידע או לחילופין יכולת זיהוי חד ערכית לכל פעילות במערכת המבוצעת ע"י משתמש במערכת.

10.10. הפסקת שיח לא פעיל - שיח לא פעיל יופסק לאחר פרק זמן מוגדר של אי פעילות שיותאם למיקום תחנת העבודה ולפעילות המתבצעת באמצעותה.

10.11. הרשאות - הענקת זכויות פעילות במערכות המידע תבוצע על בסיס ה"צורך לדעת" ותותאם לתפקיד אותו ממלא העובד.

10.12. ביטול הרשאות - שינוי, הקפאה או ביטול זכויות פעילות במערכות המידע יבוצעו בהתאמה ובלו"ז רלוונטי לסטטוס העובד או המשתמש בארגון (דהיינו, בצמוד למעבר תפקיד, יציאה לחופשה ארוכה, ובסיום העסקה).

10.13. ביקורת הרשאות - נדרשת ביקורת תקופתית על פרטי רישום המשתמשים בכל מערכות המידע, על מנת לוודא את שלמותם ודיוקם וכי הגישה עדיין נדרשת.

10.14. בקרת גישה - מערכות מידע רפואיות שבהן מטופל מידע רפואי אישי נדרשות לתמוך בבקרת גישה מבוססת תפקיד, המסוגלת למפות כל משתמש לאחד או יותר תפקידים וכל תפקיד לאחד או יותר מפונקציות המערכת.

10.15. רישום וניטור גישת משתמשים

10.15.1. גישת משתמש ליצירת, עדכון או ארכוב מידע רפואי אישי תייצר במקביל רשומת בקרה מאובטחת שתזהה יחידנית את המשתמש, את המטופל, את סוג הפעילות שביצע המשתמש ותתעד את הזמן (תאריך, שעה) שבה הפעולה בוצעה ורכיב טכנולוגיית המידע שבו נעשה שימוש (לוג).

10.15.2. ניטור רשומות הלוג יבוצע באופן סדיר.

העברת מידע מחוץ לארגון

10.16. <u>העברת מידע רפואי אישי</u> - תעשה בכפוף לדרישות חוק זכויות החולה, חוק מידע גנטי, חוק ותקנות הגנת הפרטיות וחוקים נוספים לפי העניין - ולפי הנחיות רשות למשפט, טכנולוגיה ומידע במשרד המשפטים, והנחיות משרד הבריאות ובפרט, הצפנת תווך או מידע בעת העברתו בתווך ציבורי.

10.17. <u>החצנת מידע רפואי אישי בפורטל אינטרנט מאובטח</u> – תעשה בכפוף להגדרות משרד הבריאות לגבי מידע אשר מותר לחשוף באופן זה, ובכפוף להגדרות הזדהות מתאימות.

10.18. <u>אתרים חיצוניים</u> - כלל האתרים החיצוניים והפורטלים של בתי החולים הממשלתיים יוקמו באתר תהיל״ה ויהיו כפופים למדיניות אבטחת המידע של האתר.

זמינות וטיפול במשברים

10.19. <u>גיבוי</u> - יוכנו עותקי גיבוי של מידע ושל תוכנות והם ייבדקו באופן סדיר. לפי מדיניות הגיבוי המוסכמת.

10.20. <u>זמינות</u> – לכל מערכת מידע תוגדר הזמינות הנדרשת ובהתאם להגדרה זו ייבנה המענה הטכנולוגי והאו״שי.

10.21. <u>אירועי אבטחת מידע</u> – במערכות טכנולוגיית המידע ישולבו אמצעים לגילוי, מניעה, תיעוד, התאוששות והגנה מפני קוד זדוני בתחנות הקצה, בשרתים ובשערי הארגון או עפ״י ארכיטקטורה מתאימה עפ״י החלטת הארגון. יש להגדיר נוהל טיפול במקרה של כשל אבטחתי במערכות.

10.22. <u>חירום</u> - יש להגדיר תהליכי עבודה במערכות במצבי חירום, כגון: אר״ן, היערכות חירום לאומית ועוד.

על מנהלי מוסדות רפואיים לפעול להטמעת העקרונות ע״י גיבוש נהלים פנימיים של המוסד ברוח עקרונות חוזר זה.

בכבוד רב,

פרופ׳ ארנון אפק

העתק: ח״כ צחי הנגבי, מ״מ וסגן שר הבריאות

מא/12479515