הנחיה לקיום תהליכי אבטחת מידע והגנות סייבר במכשור רפואי

1. רקע

1.1. בהתאם להחלטת ממשלה מס' 2443 מיום 15.2.2015 בנושא קידום אסדרה לאומית והובלה ממשלתית בהגנת הסייבר הונחו המנהלים הכלליים של משרדי הממשלה ויחידות הסמך לפעול לשיפור רמת הגנת הסייבר. מתוקף החלטת הממשלה מונה במשרד הבריאות ממונה הגנת סייבר והוקמה יחידת סייבר אשר אמונה על הנחיית ארגוני הבריאות במדינת ישראל.

1.2. אבטחת המכשור הרפואי מהווה כיום אתגר מיוחד במינו. הנושא נמצא בהתפתחות ושינויים תכופים לנוכח פוטנציאל האיומים העלולים לפגוע בבריאות הציבור ושרידות התהליכים הרפואיים מחד ומאידך התלות ההולכת וגוברת בפיתוחים טכנולוגיים בתחומי הרפואה ותועלות השימוש בחדשנות טכנולוגית.

1.3. המכשור הרפואי מהווה כיום חלק בלתי נפרד מהטיפול הרפואי וזמינותו הינה חיונית למתן מגוון רחב מאד של שירותי רפואה.

1.4. המכשור הרפואי הולך ותופס חלק נכבד מתהליכי האבחון והטיפול במטופלים ומחייב קישור בזמן אמת לרשתות תקשורת ארגוניות, ובה בעת לגישה מרחוק למטרות הענקת שירותי רפואה למרחוק, וכן לצורך מתן מענה מקצועי ומהיר לתמיכה ע"י יצרני המכשור וספקי תמיכה ותחזוקה בארץ ומחו"ל.

2. מטרת ההנחיה

2.1. משרד הבריאות מגדיר במסמך המצורף "מדיניות לאבטחת מידע (א- 14.2) במכשור רפואי" את דרישות אבטחת המידע שיש לכלול בתהליכי שילוב מכשור רפואי במדינת ישראל עבור :

2.1.1. יצרני מכשור רפואי (רשימת תיוג עבור יצרני האמ"ר)

2.1.2. מוסדות רפואיים המפעילים מכשור רפואי

2.1.3. משתמשים פרטיים של מכשור רפואי

2.2. הנחיה זו מהווה הנחיה לביצוע, ועל כן תוכנה **מחייבת את כלל הארגונים במגזר הבריאות** בישראל המונחות ע"י יחידת הסייבר המגזרית של משרד הבריאות.

3. הנחיות לביצוע

3.1. נדרש לבצע את ההתאמות הנדרשות לקיום ותיעוד של ניתוח סיכוני הגנת סייבר במכשור הרפואי ובממשקים בינו לבין מרכיבים חיצוניים תוך התייחסות לנזק / פגיעה / חבלה (HARM) במרכיבים הבאים בניתוח סיכוני הגנת הסייבר שלהם:

3.1.1. הערכת ההשפעה של האיומים והפגיעויות על תפקוד המכשיר ועל בריאות המטופל.

3.1.2. הערכה של ההסתברות לניצול לרעה של איום או פגיעות.

3.1.3. הגדרת רמות סיכון ואסטרטגיות מתאימות לצמצומם.

3.1.4. הערכת הסיכון השיורי וקריטריונים לרמות סיכון סבירות.

3.2. יש לוודא קיום תהליכי בקרה לאבטחת פעילות המכשיר הרפואי בהתאם לאופן חיבור המכשור הרפואי.

3.3. חשיבות הבקרה:

3.3.1. בקרה חיונית: כשמה כן היא, חיוני שתתקיים.

3.3.2. בקרה חשובה: מומלץ שתתקיים, אך איננה חיונית.

4. אחריות ליישום

4.1. מנהלי בתי החולים.

4.2. מנהלי מרפאות.

4.3. מנהלי קופות החולים.

4.4. מנהל מוסד רפואי אחראי באופן אישי להגנה על המידע הרפואי הנוצר ונאגר במוסד (אין בהוראות הנחיה זאת כדי להטיל אחריות אישית מעבר לזו הקבועה בחוק).

4.5. מנהל מוסד בריאות / ארגון בריאות.

בברכה,
ראובן אליהו
מנהל תחום תשתיות, שירות וסייבר – CTO
ממונה על הגנת הסייבר במערכת הבריאות.

משרד הבריאות – הנחיות אבטחת מידע			
		מהדורה	1.0
שם ההנחיה	הנחיה לקיום תהליכי אבטחת מידע והגנות סייבר במכשור רפואי	בתוקף מ	יוני 2018
מספר			עמוד 3 מתוך 3