ניהול שינויים

תאריך	מחבר	גרסה	שינוי
2014 - 2013	**גיבוש הנוהל בוצע במסגרת ועדה, שמונתה על ידי ראש המנהל לטכנולוגיות רפואיות ותשתיות, בראשות מנהל תחום תשתיות במשרד הבריאות**		
01/09/2014	חברת אבנת	1.0	טיוטה אחרונה
20/09/2014	גבי פטליס	1.0	**מקור**
31/11/2014	תמיר פלדמן	1.0	**בקרה** מנהל תחום סייבר ואבטחת מידע
31/12/2014	אמיר שי	1.0	**אישור** מנהל תחום תשתיות וטכנולוגיות תקשוב, CTO
20/12/2015	גבי פטליס	1.1	עדכון מספר נוהל לפי גרסת תקן חדשה

רגולציה לאבטחת מידע במכשור רפואי

1. רקע/מבוא:

1.1. אבטחת המכשור הרפואי מהווה כיום אתגר מיוחד במינו. אחת הסיבות העיקריות לצורך באבטחת המידע במכשור רפואי הינה השימוש בתשתיות מחשוב תקניות (דהיינו, מערכות הפעלה כדוגמת חלונות ולינוקס, ופרוטוקול תקשורת תקני וגם פרוטוקולי תקשורת ייעודים[1]) המפעילות יישום או מכשור ייחודי, לעיתים פולשני לגוף האדם המטופל.

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

1.3. 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.

1.4. ייצור שיווק ושימוש בציוד רפואי במדינת ישראל:

1.4.1. ציוד רפואי מיוצר, משווק, ומותר לשימוש במדינת ישראל על בסיס רישומו בפנקס הציוד הרפואי, המנוהל באגף הציוד הרפואי (אמ"ר) שבמשרד הבריאות.

1.4.2. התהליך לרישום ציוד רפואי באגף לציוד רפואי כולל בחינת מסמכים, אישורים, והצהרות של גופים רגולטוריים מוכרים. האגף רשאי לדרוש גם מסמכים ומידע נוסף שאינו נכלל בבקשה, וכן דוגמאות של הציוד הרפואי, ולהציג שאלות בכל עניין מן העניינים הנוגעים לרישום הציוד הרפואי .

1.4.3. להלן רשימת הרשויות הרגולטוריות המוכרות שעל אישורם נסמך האישור במדינת ישראל:

1.4.3.1. מנהל המזון והתרופות של ארה"ב (FDA).

1.4.3.2. האישור האירופי (CE Marking), שניתן בידי גופים פרטיים (Notified Bodies) שהוסמכו לכך בידי הרשויות הממשלתיות.

1.4.3.3. הרשות המוסמכת בקנדה (Health Canada).

[1] **SCADA - supervisory control and data acquisition מעולם המושגים של מערכות**

1.4.3.4. הרשות האוסטרלית (TGA).

1.4.3.5. הרשות היפנית (PMDA).

1.4.4. במידה והוכחה בטיחות ויעילות הציוד הרפואי ובמידה והמסמכים שהוצגו בפני האגף ענו על כל הדרישות המפורטות בחוק הציוד הרפואי ובהנחיות המפורטות באתר האינטרנט של האגף, יונפק אישור רישום הציוד הרפואי בפנקס הציוד הרפואי במשרד הבריאות.

2. <u>הגדרות:</u>

2.1. אבטחת מידע - הגדרת ISO (ISO 27000:2014):

שימור סודיות (Confidentiality), שלמות ואמינות (Integrity), וזמינות (Availability) של מידע. כאשר:

2.1.1. סודיות: תכונת אי זמינות/חשיפת מידע לבלתי מורשים (יחידים, ישויות או תהליכים).

2.1.2. שלמות ואמינות: תכונת הגנת דיוק ושלמות.

2.1.3. זמינות: תכונת הנגישות והשימושיות עפ"י דרישה ע"י ישות מורשית.

2.2. אבטחת מידע - הגנת סייבר (ה"ס) – לפי הגדרת ה-FDA:

תהליך של מניעת שינוי בלתי מורשה, שימוש לרעה או שלילת השימוש, או שימוש בלתי מורשה של מידע האגור, מעובד או מועבר מהמכשיר הרפואי ליעד חיצוני. הגנת סייבר מחולקת לשלושה נושאים:

2.2.1. סודיות: נתונים, מידע או מבנה המכשיר נגישים רק לעובדים וישויות מורשות ומופעלים בזמנים מורשים ובאופן מורשה.

2.2.2. שלמות ואמינות: נתונים ומידע הנם מדויקים ושלמים ולא שונו באופן בלתי הולם.

2.2.3. זמינות: נתונים, מידע ומערכות מידע נגישים ושמישים באופן המצופה, בזמן ובמקום שהוא דרוש.

2.3. אמ"ר (אביזרים ומכשירים רפואיים): אגף במשרד הבריאות (ציוד רפואי) העוסק ברישום אמ"ר במדינת ישראל, מתן היתרי יבוא מסוגים שונים לאמ"ר, מעקב אחר שיווק אמ"ר והנפקת מסמכים המסייעים ליצוא אמ"ר. האגף מפעיל מנגנון רישום, פיקוח ובקרה על ייצור, יבוא ושיווק אמ"ר.

2.4. הזדהות: אמצעי/שיטה להבטחה שתכונה הנטענת לגבי ישות הנה נכונה. אנו מייחסים בדרך כלל את השיטה לזיהוי אדם במערכת מידע. קיימות שלוש שיטות עיקריות: באמצעות נתון שהאדם יודע (לדוגמה: שם משתמש וסיסמה), רכיב שיש בידי האדם (לדוגמה: כרטיס חכם) ומרכיב ייחודי של האדם (מרכיב ביומטרי).

2.5. הזדהות חזקה: שימוש בתהליך ההזדהות ווידוא ההזדהות בשני גורמים שונים. לדוגמה: משהו שאני יודע (שם משתמש) ומשהו שיש בידי (כרטיס פיזי).

2.6. הערכת סיכונים (לחלופין: אתור וחישוב הסיכון השורשי בהיבטי אבטחת מידע, דהיינו, זמינות-שלמות ואמינות-סודיות-C-I-A): תהליך של הערכת רמת הסיכון של המערכות השונות בארגון. התהליך ממפה את האיומים השונים הנובעים מהפעילות במערכות השונות. תוצר הערכת הסיכונים הנו מסמך המדרג את רמת המסוכנות של המערכות השונות לארגון. מסקנות מסמך זה משמשות לגזירת פעילויות אבטחת המידע השונות.

2.7. הצפנה: תהליך המרה של מידע גלוי (Clear Text) למידע מקודד (Cipher Text) באופן שיוכל להיות מפוענח ומובן אך ורק לגורמים מורשים.

2.8. זיהוי חד ערכי: ערך ייחודי המזהה את מי שמתיימר להיות בעל אמצעי הזיהוי.

2.9. חתימה דיגיטלית (Digital Signature): פריט מידע ייחודי הנוצר כפונקציה קריפטוגרפית של פריט מידע אחר, כך שהוא מזהה את התוכן בצורה מדויקת ומאפשר לזהות שינוי בו.

2.10. לוג – Log: קובץ התיעוד של נתיב בקרה.

2.11. מכשור רפואי – ראה פירוט בפרק 6.

2.12. נזק/פגיעה/חבלה - HARM (ISO/IEC 80001-1:2010):

פגיעה פיזית או נזק לבריאותו הגופנית או הנפשית של המטופל, או נזק לציוד. או לסביבה, או צמצום ביעילות, או פגיעה באבטחת המידע האגור במכשיר או במערכת. הותאם מההגדרה בתקן ISO 14971:2007.

2.13. נתיב בקרה: תיעוד פעולות המתבצעות במערכות מידע. קובץ התיעוד מקשר את הפעולה לנתונים נוספים כגון: שם מבצע הפעולה, המועד, הפעולה עצמה ועוד.

2.14. סיכון שיורי (ISO/IEC 80001-1:2010):

הסיכון הנותר לאחר שאמצעי בקרה לסיכון יושמו. הגדרה 2.15 תקן ISO 14971:2007.

2.15. סקר סיכונים: סקר המאתר איומים/חשיפות הקשורות באבטחת מידע במערכות שונות והמעריך את רמת הסיכון שלהם לארגון.

2.16. תווך תקשורת ציבורי: תשתיות תקשורת המשרתות/משתפות מספר רב של צרכנים ואינן שייכות לאחד מהם. תשתיות אינטרנט מוגדרות כתווך תקשורת ציבורי.

3. מסמכים ישימים:

3.1. חוקים והנחיות

3.1.1. מדינת ישראל

3.1.1.1. חוק ציוד רפואי התשע"ב–2012.

3.1.1.2. הנחיות להגשת בקשה לרישום ציוד (רפואי (אמ"ר) במשרד הבריאות- באתר האינטרנט.

3.2. תקנים בנושא אבטחת מידע

3.2.1. ISO

3.2.1.1. סדרת תקני IEC_80001

3.2.1.1.1. IEC_80001-1:2010

3.2.1.1.2. IEC/TR 80001-2-1:2012

3.2.1.1.3. IEC/TR 80001-2-2:2012

3.2.1.1.4. IEC/TR 80001-2-3:2012

3.2.1.1.5. IEC/TR 80001-2-4:2012

3.3. מסמכים והנחיות רלבנטיות מה-FDA

3.3.1. מכשור רפואי- MEDICAL DEVICE:

http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/ucm051512.htm

3.3.2. Medical Device Data System:

http://www.fda.gov/MedicalDevices/ProductsandMedicalProcedures/GeneralHospitalDevicesandSupplies/MedicalDeviceDataSystems/ucm251906.htm

3.3.3. יישומים רפואיים ניידים – Mobile Device Applications (23.9.2013)

http://www.fda.gov/medicaldevices/productsandmedicalprocedures/connectedhealth/mobilemedicalapplications/default.htm

3.3.4. טיוטת הנחיה – CYBER SECURITY FOR MEDICAL DEVICES (14.6.2013)

Content of Premarket Submissions for Management of Cybersecurity in Medical Devices - Draft Guidance for Industry and Food and Drug Administration Staff
http://www.fda.gov/medicaldevices/deviceregulationandguidance/guidancedocuments/ucm356186.htm

3.3.5. FDA Safety Communication: Cybersecurity for Medical Devices and Hospitals Networks (14/6/2013)

http://www.fda.gov/medicaldevices/safety/alertsandnotices/ucm356423.htm

3.3.6. HIMSS/NEMA – National Electrical Manufacturers Association/Healthcare Information and Management Systems Society

3.3.7. **M**anufacturer **D**isclosure **S**tatement for **M**edical **D**evice **S**ecurity (MDS^2)

http://www.nema.org/Standards/ComplimentaryDocuments/MDS2%20form%20HN%201-2013.xlsx

4. אחריות ליישום:

4.1. משרד הבריאות מגדיר במסמך זה את דרישות אבטחת המידע שיש לכלול בתהליכי שילוב מכשור רפואי במדינת ישראל באופן הבא:

4.1.1. ליצרני מכשור רפואי:

4.1.1.1. באמצעות הגדרת דרישות סף מקומיות בתהליך הרישום, (המנוסחות במסמך זה, בפרק 7) הנסמכות על תהליכים תקניים המקובלים בעולם. כדוגמת MDS^2 המעודכן (גרסת 10/2013), טיוטת הנחיות אבטחת מידע למכשור רפואי של ה-FDA (יוני 2013) וכיו"ב.

4.1.2. למוסדות רפואיים המפעילים מכשור רפואי:

4.1.2.1. על בסיס ניהול סיכוני חיבור והפעלת מכשור רפואי האוגר/לא אוגר מידע מקומי (במכשיר) ומתחבר/איננו מתחבר לרשת המוסד הרפואי,

תוך הסתייעות בתקינה מאושרת לנושא זה בעולם (סדרת תקני IEC_80001), ובשילוב הגישות שננקטו ע"י המפקח על הבנקים בכותבו את הנחייתו לניהול תקין של טכנולוגיית המידע (נב"ת 357)[2], בשנת 2003, וע"י המפקח על הביטוח באגף שוק ההון במשרד האוצר בכתיבת: "הוראה לניהול סיכוני אבטחת המידע של הגופים המוסדיים"[3] בשנת 2006. אלו מצוינים בפרק 7 במסמך זה.

4.1.3. למשתמשים פרטיים של מכשור רפואי:

4.1.3.1. כחלק מאישור רישום של מכשור רפואי שיירכש ע"י צרכן פרטי ישירות ממשווק, יידרש יצרן המכשור הרפואי לספק למשתמש הנחיות אבטחת מידע. דומה להסדר הקיים היום בעת שיווק תרופות, כאשר לכל אריזת תרופה נלווה מסמך מאושר ובו הנחיות לשימוש, תופעות לוואי וכד'.

* לחשיבה לגבי תהליך עתידי. אין התייחסות לנושא זה במסמך הנוכחי.

[2] https://www.boi.org.il/he/BankingSupervision/SupervisorsDirectives/DocLib/357.pdf

[3] http://mof.gov.il/hon/Documents/%D7%94%D7%A1%D7%93%D7%A8%D7%94-%D7%95%D7%97%D7%A7%D7%99%D7%A7%D7%94/mosdiym/memos/2006-9-06.pdf

5. הסיכונים והאיומים למכשור רפואי ובמערך המכשור הרפואי הנובעים מכשל באבטחת המידע:

5.1. פגיעה בחיי אדם:

5.1.1. שינויי כיול או שינוי כלשהו בנתוני מכשור רפואי (בין בשגגה ובין בזדון) שתוצאותיו הינן תוצאות שגויות שמפיק המכשיר אשר עלולות לגרום לפגיעה בחיי אדם. פעולה זו יכולה להתבצע על ידי גורם אנושי או על ידי קובץ זדוני.

5.2. פגיעה בזמינות השירות המסופק באמצעות המכשור הרפואי:

5.2.1. גרימת נזק לרכיבי התוכנה של המכשור הרפואי, נזק שעלול לגרום להשבתתו המלאה/החלקית ובכך לפגוע בזמינות השירות שהמכשור מספק למטופלים באמצעות מכשור זה.

5.2.2. שינויי כיול או שינוי כלשהו בנתוני מכשור רפואי (בין בשגגה ובין בזדון) שתוצאותיו הינן תוצאות שגויות שמפיק המכשיר ובכך לגרום להשבתת השימוש במכשיר באופן מלא או חלקי.

5.3. פגיעה בסודיות הנתונים באחד ממרכיבי המכשור הרפואי או בעת העברת מידע מסווג בממשקי תקשורת (פנימיים או חיצוניים):

5.3.1. גניבת נתוני מטופלים (כולל מידע רפואי אישי) מהמכשור הרפואי עצמו או דרך אחד מהקישורים של המכשור (למשל ע"י יישום תקיפת Man-in-the-Middle)[4] באחד מממשקי המכשור הרפואי או מערכת הניהול שלו, או על ידי ציתות לתווך התקשורת).

5.3.2. גניבת נתונים מרשומה רפואית ממוחשבת האגורה במערכות המידע של המוסד שבו מופעל המכשור הרפואי ומחובר אליו בתקשורת, ע"י חדירה למערכת המידע של המוסד הרפואי תוך שימוש במכשור הרפואי שאיננו מאובטח כיאות/בממשק שבין המכשור הרפואי ומערכת ניהול התהליך הרפואי (שהמכשיר מהווה חלק ממנו) שאיננו מוגן באופן מספק/בממשק הגישה מרחוק אל המכשור הרפואי.

5.4. פגיעה בשלמות ואמינות הנתונים באחד ממרכיבי המכשור הרפואי או בעת העברת מידע מסווג בממשקי תקשורת (פנימיים או חיצוניים):

[4] **תקיפה המאפשרת התחזות לגורם מורשה בתווך התקשורת, חשיפת מידע לגורם לא מורשה ואף שינוי של מידע ללא הרשאה.**

5.4.1. שינוי בלתי מורשה של נתוני מטופלים (כולל מידע רפואי אישי) במכשור הרפואי עצמו או דרך אחד מהקישורים של המכשור (למשל על ידי יישום תקיפת Man-in-the-Middle באחד מממשקי המכשור הרפואי או מערכת הניהול שלו).

5.4.2. גרימת נזק לרכיבי התוכנה של המכשור הרפואי, נזק שעלול לגרום לפגיעה באמינות/שלמות הנתונים בתהליך העבודה עם המכשור הרפואי.

5.4.3. שימוש שלא כדין במכשור הרפואי שעלול לגרום לפגיעה באמינות/שלמות הנתונים.

5.5. חדירה למערכות:

5.5.1. שימוש שלא כדין במכשור הרפואי במטרה לחדור למערכות אחרות בארגון.

5.5.2. שימוש שלא כדין במכשור הרפואי על מנת לחדור באמצעותו למערכות המידע של יצרני/ספקי המכשור דרך הקישור מרחוק שמספק הלקוח של המכשור הרפואי ליצרן/ספק/מטמיע המכשור.

5.5.3. שימוש שלא כדין במערכות בארגון במטרה לחדור למכשור רפואי.

5.6. סיכוני אבטחת מידע טכנולוגיים:

5.6.1. ציתות לרשת התקשורת בממשקים פנימיים (לדוגמא בין תוכנת ניהול המכשיר הרפואי לבין רכיב הבקרה) או חיצוניים (למשל בין תוכנת ניהול המכשור הרפואי לתוכנות אחרות). פעילות זו עלולה לאפשר (בין היתר):

1. חשיפה של מידע רפואי של מטופלים לגורמים לא מורשים.

2. חשיפה של פרטי הזדהות והתחזות לגורמים מורשים.

5.6.2. גישה של גורם לא מורשה לרכיבי המכשור הרפואי תוך עקיפת מנגנוני בקרה תשתיתיים או אפליקטיביים (לדוגמא קיום חולשות מערכת הפעלה או שירותים, התחזות של גורם לא מורשה למשתמש מורשה, עקיפת מנגנון הזדהות על ידי Brute-Force, עקיפת מנגנון הרשאות, גישה פיזית ללא הרשאה).

5.6.3. גישה של גורם תחזוקה מורשה לרכיבי המכשור הרפואי, מרשת חיצונית[5], ברמת הרשאה כזו העלולה לאפשר לו גישה למערכות מידע/רכיבים אחרים ברשת, ללא כל הרשאה.

5.6.4. חדירה/החדרה מכוונת של קובץ זדוני לרכיבי המכשור הרפואי מתחנות/שרתים ברשת או רשתות מקושרות אליה תוך עקיפת מנגנוני בקרה (הקשחת מערכת הפעלה, אנטי וירוס).

5.6.5. חדירה/החדרה מכוונת של קובץ זדוני מרכיבי המכשור הרפואי לתחנות/שרתים ברשת או רשתות מקושרות אליהם תוך עקיפת מנגנוני בקרה (דוגמאות למנגנוני בקרה: הקשחת מערכת הפעלה, אנטי וירוס).

5.6.6. התחזות לתוכנת ניהול מכשור רפואי או למכשיר רפואי או לתוכנה חיצונית אחרת הקשורה לתהליך הרפואי.

5.6.7. ביצוע שינויים בהגדרות שונות במכשור הרפואי ללא כל הרשאה.

5.6.8. הסיכונים שהוצגו בסעיפים שלעיל עלולים לאפשר (בין היתר):

1. פגיעה בזמינות המכשור הרפואי.
2. שיבוש מידע רפואי של מטופלים.
3. שיבוש של מידע חיוני לביצוע טיפול ולכן שיבוש הטיפול עצמו.
4. חשיפה של מידע רפואי של מטופלים לגורמים לא מורשים.

[5] **שאינה מפוקחת על ידי גורם במערך הבריאות**

6. ארכיטקטורה כללית של מערך המידע של המכשור רפואי וחיבורו לרשת התקשורת:

6.1. ניתן לחלק באופן כללי את עולם המכשור עפ"י החלוקה הבאה המתייחסת להיבטי איום וסיכון ומתן מענה להם:

6.1.1. מכשור שאיננו אוגר מידע באופן מקומי ואיננו מחובר לרשת תקשורת.

6.1.2. מכשור שאוגר מידע באופן מקומי ואיננו מחובר לרשת תקשורת.

6.1.3. מכשור שאיננו אוגר מידע באופן מקומי ומחובר לרשת תקשורת.

6.1.4. מכשור שאוגר מידע באופן מקומי ומחובר לרשת תקשורת.

<u>הערות</u>:

א. המונח "מחובר לרשת" כולל גם שידור/קליטה ברשת אלחוטית/סלולרית.

ב. ככל שאנו מתקדמים בחומרת הסיכון כך גדלים האיומים ומתרחב עולם הפתרונות (הבקרות) שנדרש ליישם.

ג. מכשור רפואי גם אם איננו מחובר לרשת הארגונית עשוי להידרש לחיבור גישה מרחוק למטרת תחזוקה, כיול וטיפול בתקלות ע"י היצרן (בארץ או בחו"ל) או ספק התחזוקה (בארץ או בחו"ל).

6.2. ברמה העקרונית שימוש במכשור רפואי כולל את המרכיבים הבאים:

6.2.1. מכשור רפואי המבצע אבחון, טיפול או שניהם, כדוגמת מכשיר מעבדה, מכשיר דימות, מכשירי בדיקה פולשניים[6], כולל מחשב צמוד או משובץ מחשב[7].

6.2.2. רכיב ניהול ההליך הרפואי, כדוגמת מערכת ניהול מעבדות, מערכת ניהול צילומי דימות וכיו"ב.

6.2.3. מערכת ארגונית/מערכות ארגוניות המאפשרת/ות גישה למידע הנוצר במכשור הרפואי או בתהליך הרפואי שבו המכשור הרפואי נוטל חלק הן למטפל והן למטופל.

6.3. במקביל יידרשו מענים לדרכי הגישה הבאות:

---

[6] **המכשיר הרפואי עצמו מבוקר על ידי בקר אלקטרוני, שהוא מהווה רכיב ייעודי ונפרד בעל ממשקי תקשורת משלו.**

[7] **מתואר במסמך זה כתוכנת הניהול של המכשיר או של הבקר.**

6.3.1. גישה מקומית ומרוחקת של משתמשים לכל אחת משלושת סוגי המערכות הנ"ל.

6.3.2. גישה מרחוק על גבי האינטרנט של יצרני/תומכי שלושת המערכות הנ"ל.

6.3.3. ממשקי תקשורת פנימיים וחיצוניים שבהם מועבר מידע באופן דו כיווני בין שלושת המערכות הנ"ל.

7. <u>הגדרות אבטחת מידע – רשימת תיוג עבור יצרן האמ"ר:</u>

מקרא לטבלה:

1. **נושא בקרה: המרכיב הראשי שלגביו יישומו בקרות.**
2. **תיאור הבקרה: הסבר מפורט מהי הבקרה הנדרשת לכל נושא ראשי של בקרה יוצמדו אחד או יותר בקרות.**
3. **חשיבות הבקרה:**

א. **בקרה חיונית: כשמה כן היא, חיוני שתתקיים.**

ב. **בקרה חשובה: מומלץ שתתקיים, אך איננה חיונית.**

משרד הבריאות – נהלי אבטחת מידע			
פרק	**א-14 רכישה, פיתוח ותחזוקה של מערכות** **System acquisition, development and maintenance**	מהדורה	**1.1**
שם הנוהל	**רגולציה לאבטחת מידע במכשור רפואי**	בתוקף מ	**20/12/2015**
מספר	**א-14.2**		**עמוד 15 מתוך 43**

מס׳ סד׳	נושא הבקרה	תיאור הבקרה	חשיבות הבקרה	קטגוריות חיבור המכשור רפואי			
				מחובר לרשת ואוגר מידע	מחובר לרשת ולא אוגר מידע	לא מחובר לרשת ואוגר מידע	לא מחובר לרשת ולא אוגר מידע

מס' סד'	נושא הבקרה	תיאור הבקרה	חשיבות הבקרה	קטגוריות חיבור המכשור רפואי			
				מחובר לרשת ואוגר מידע	מחובר לרשת ולא אוגר מידע	לא מחובר לרשת ואוגר מידע	לא מחובר לרשת ולא אוגר מידע
.1	**כללי**	קיום תיעוד 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: • הערכת ההשפעה של האיומים והפגיעויות על תפקוד המכשיר ועל בריאות המטופל. • הערכה של ההסתברות לניצול לרעה של איום או פגיעות. • הגדרת רמות סיכון ואסטרטגיות מתאימות לצמצומם. • הערכת הסיכון השיורי וקריטריונים לרמות סיכון סבירות.	**חשובה**	X	X	X	X
.2	**כללי**	המכשיר הרפואי לא יחשוף מידע פנימי שאינו נדרש למשתמש בעת תקלה.	**חשובה**	X	X	X	X
.3	**הגבלת**	קיום מנגנונים המגבילים גישה למכשירים באמצעות תהליך הכולל הזדהות ווידוא ההזדהות של ישויות (יחידים, תהליכים, מכשירים). לדוגמה: שם	**חיונית**	X	X	X	X

משרד הבריאות – נהלי אבטחת מידע			
פרק	**א-14 רכישה, פיתוח ותחזוקה של מערכות System acquisition, development and maintenance**	מהדורה	**1.1**
שם הנוהל	**רגולציה לאבטחת מידע במכשור רפואי**	בתוקף מ	**20/12/2015**
מספר	**א-14.2**		**עמוד 17 מתוך 43**

מס' סד'	נושא הבקרה	תיאור הבקרה	חשיבות הבקרה	קטגוריות חיבור המכשור רפואי			
				מחובר לרשת ואוגר מידע	מחובר לרשת ולא אוגר מידע	לא מחובר לרשת ואוגר מידע	לא מחובר לרשת ולא אוגר מידע
	גישה למשתמשים	משתמש וסיסמה, כרטיס חכם, ביומטרי). תהליך ההזדהות חייב לכלול לכל הפחות שם משתמש וסיסמה.					
.4	**מורשים**	קיום מנגנון אוטומטי לסגירת session של משתמש על בסיס מרכיב זמן מתוכנן מראש באופן מותאם לסביבת הפעלת המכשיר.	**חשובה**	X	X	X	
.5		קיום מנגנון עצמאי ושכבתי להענקת הרשאות שמבוסס על רמות הרשאה שונות עפ"י תפקיד דורש ההרשאה (לדוגמה: אפליקציה רפואית, ספק שירות רפואי, מנהלן).	**חיונית**	X	X	X	X
.6		קיום מנגנוני נעילה פיסית ולוגית של ממשקים במכשירים ובציוד קישוריות, לצמצום הסיכון לחבלות.	**חיונית**	X	X	X	X
.7		גישה פריווילגית למכשיר (לדוגמה: למנהלנים, טכנאי	**חשובה**	X		X	

מס' סד'	נושא הבקרה	תיאור הבקרה	חשיבות הבקרה	קטגוריות חיבור המכשור רפואי			
				מחובר לרשת ואוגר מידע	מחובר לרשת ולא אוגר מידע	לא מחובר לרשת ואוגר מידע	לא מחובר לרשת ולא אוגר מידע
		שירות, אנשי תחזוקה) מחייבת שימוש ב- Multi Factor Authentication ("הזדהות חזקה").					
.8		קיום אמצעים המאפשרים הימנעות משימוש בסיסמאות מקודדות מראש (Hardcoded Passwords). קיום מנגנונים המאפשרים הגבלת גישה ציבורית לסיסמאות שבהן נעשה שימוש לגישה פריווילגיית למכשיר.	**חיונית**	X	X	X	X
.9		קיום מנגנוני הזדהות לפני ביצוע פעילויות רגישות: לפני אישור של עדכון תוכנה או קושחה.	**חשובה**	X	X	X	X
.10	**הבטחת**	קיום מנגנונים המאפשרים אימות של קודים (Authenticated code) לעדכוני תוכנה או קושחה.	**חשובה**	X	X	X	X
.11	**תוכן** **בר**	אפשור שימוש בתהליכים שיטתיים למשתמשים מאושרים להוריד גרסת תוכנה/קושחה ברת זיהוי מהיצרן.	**חשובה**	X	X	X	X

משרד הבריאות – נהלי אבטחת מידע			
פרק	**א-14 רכישה, פיתוח ותחזוקה של מערכות System acquisition, development and maintenance**	מהדורה	**1.1**
שם הנוהל	**רגולציה לאבטחת מידע במכשור רפואי**	בתוקף מ	**20/12/2015**
מספר	**א-14.2**		**עמוד 19 מתוך 43**

מס' סד'	נושא הבקרה	תיאור הבקרה	חשיבות הבקרה	קטגוריות חיבור המכשור רפואי			
				מחובר לרשת ואוגר מידע	מחובר לרשת ולא אוגר מידע	לא מחובר לרשת ואוגר מידע	לא מחובר לרשת ולא אוגר מידע
12.	**אמון**	קיום מנגנונים המבטיחים מניעה של שינוי של מידע רפואי על ידי גורם לא מורשה כשהוא שמור במכשור הרפואי. קיום מנגנונים המבטיחים את פרטיות המידע של המטופלים כשהוא שמור במכשור הרפואי, כשהוא מודפס וכשהוא מוצג לקהל (באמצעות המכשיר עצמו). יש להשתמש לשם כך במנגנונים קריפטוגרפים.	**חיונית**	X		X	
13.		קיום של מנגנונים המבטיחים מניעה של שינוי של מידע רפואי על ידי גורם לא מורשה בתהליך העברתו. קיום מנגנונים המבטיחים את פרטיות המידע של המטופלים בתהליך העברתו, כולל בעת הדפסתו והצגתו לקהל באמצעות החיבור הרשתי. יש להשתמש לשם כך במנגנונים קריפטוגרפים.	**חיונית**	X	X		

מס' סד'	נושא הבקרה	תיאור הבקרה	חשיבות הבקרה	קטגוריות חיבור המכשור רפואי			
				מחובר לרשת ואוגר מידע	מחובר לרשת ולא אוגר מידע	לא מחובר לרשת ואוגר מידע	לא מחובר לרשת ולא אוגר מידע
14.		באם ניתן לשמור מידע רפואי אישי במכשיר הרפואי נדרשת יכולת להציג בפני המשתמש את רמת סיווג המידע הנגיש, בהתאם לתקן 27799.	**חשובה**	X		X	
15.	**מנגנוני אל כשל והתאוששות**	קיום של מנגנוני אל כשל המגנים על תפקודים חיוניים של המכשיר, אפילו באם אבטחת המכשיר הועמדה בסיכון.	**חשובה**	X	X	X	X
16.		קיום של מנגנונים המאפשרים אתור, תיעוד ותגובה למצבים בהם אבטחת המכשיר מועמדת בסיכון Security Compromises).	**חיונית**	X	X	X	
17.		קיום יכולת לאושש את הגדרות המכשיר ע"י מנהלן מערכת מאומת.	**חיונית**	X	X	X	X
18.	**ממשקים**	מכשירים רפואיים שאינם	**חיונית**			X	X

מס' סד'	נושא הבקרה	תיאור הבקרה	חשיבות הבקרה	קטגוריות חיבור המכשור רפואי			
				מחובר לרשת ואוגר מידע	מחובר לרשת ולא אוגר מידע	לא מחובר לרשת ואוגר מידע	לא מחובר לרשת ולא אוגר מידע
		נדרשים בקישוריות לא יכילו ממשקי תקשורת.					
.19		ממשקי תקשורת אלחוטיים יכילו אמצעים לפעולות לפחות בהתאם לתקנים הבאים, בהתאמה: WPA2, Bluetooth 2.1.	**חיונית**	X	X		
.20	**תיעוד במסמכי טרום שיווק (להלן: מט"ש)**	ניתוח סיכונים (Hazard analysis), אמצעי צמצום / הקלה /הפגה (Mitigations), ושיקולי תכנון המתייחסים לסיכוני הגנת סייבר מכוונים ("זדוניים") ושאינם מכוונים ("בשוגג"), הנלווים למכשיר, כולל: • רשימה מפורטת של כל סיכוני הגנת סייבר אשר נשקלו בתכנון של המכשיר. • רשימה מפורטת ומנומקת של כל הבקרות שיושמו עבור המכשיר.	**חיונית**	X	X	X	X
.21		מטריצת מעקב המקשרת בין בקרות הגנת סייבר בפועל לסיכוני הגנת סייבר שנשקלו.	**חיונית**	X	X	X	X
.22		אפיון של תוכנית שיטתית	**חיונית**	X	X	X	X

מס' סד'	נושא הבקרה	תיאור הבקרה	חשיבות הבקרה	קטגוריות חיבור המכשור רפואי			
				מחובר לרשת ואוגר מידע	מחובר לרשת ולא אוגר מידע	לא מחובר לרשת ואוגר מידע	לא מחובר לרשת ולא אוגר מידע
		לאספקת עדכונים וטלאים מאומתים למערכות הפעלה, או לתוכנת המכשיר הרפואי, בהתאם לצרכים.					
.23		מענה לכלל השאלות המופיעות בקובץ MDS[2]	**חיונית**	X	X	X	X
.24		הצהרה כי המכשיר מסופק כשהוא נקי מתוכנות זדוניות.	**חיונית**	X	X	X	X
.25		רשימת כלל התקנים הטכנולוגיים שעל פיהם פועל המכשיר הרפואי, לרבות תקנים הקשורים לממשקים במכשיר הרפואי.	**חיונית**	X	X	X	X
.26		הוראות הפעלה למכשיר ומפרט המוצר בהתייחס לתוכנת אנטי ווירוס מומלצת ו/או FIREWALL ו/או כל מנגנון אבטחת מידע המתאים לסביבת השימוש.	**חיונית**	X	X	X	X
.27		ממצאי בדיקות אבטחת מידע שבוצעו למכשור הרפואי ובקרות שיושמו לצמצום סיכונים, אם אלו	**חשובה**	X	X	X	X

משרד הבריאות – נהלי אבטחת מידע			
פרק	**א-14 רכישה, פיתוח ותחזוקה של מערכות System acquisition, development and maintenance**	מהדורה	**1.1**
שם הנוהל	**רגולציה לאבטחת מידע במכשור רפואי**	בתוקף מ	**20/12/2015**
מספר	**א-14.2**		**עמוד 23 מתוך 43**

מס' סד'	**נושא הבקרה**	**תיאור הבקרה**	**חשיבות הבקרה**	**קטגוריות חיבור המכשור רפואי**			
				מחובר לרשת ואוגר מידע	**מחובר לרשת ולא אוגר מידע**	**לא מחובר לרשת ואוגר מידע**	**לא מחובר לרשת ולא אוגר מידע**
		נתגלו.					

8. <u>הנחיות למוסדות רפואיים ב תהליך הטמעת אבטחת מכשור רפואי</u>

8.1. ניהול סיכונים

8.1.1. תהליך ניהול סיכונים

מטרה: להבטיח הטמעת מכשור רפואי במוסד רפואי תוך שילוב ניהול סיכונים.

א) מוסד רפואי יבצע תהליך מיפוי מכשור רפואי ויתחזק המיפוי באופן שוטף. המיפוי יתייחס (בין היתר) לקבוצות הסיכון כפי המתוארות בסעיף ג' להלן.

<u>הערה</u>: מוסד שבצע את הפעילות כחלק מתהליך הסמכתו לתקן אבטחת מידע בבריאות (27799), יסתמך על המיפוי שבצע ויוסיף התייחסות ע"פ סעיף ג' להלן.

ב) מוסד רפואי יבצע תהליך ניהול סיכונים עבור הטמעה של מכשור רפואי ברשת בהתאם לתקן IEC 80001, בנושאים הבאים:

1. הגדרת ותיעוד תפקידים והרשאות.
2. הגדרת ותיעוד מדיניות ותהליכים בניהול סיכונים.
3. תכנון, יישום ותיעוד תהליך ניהול סיכונים.
4. תכנון, יישום ותיעוד תהליך ניהול שינויים וניהול הגדרות.
5. תכנון, יישום ותיעוד תהליך ניהול ניטור ואירועים.
6. יישום תהליך בקרה של תהליכים במחזור החיים של רשת המשלבת מכשור רפואי.

ג) בתהליך ניהול הסיכונים יש להתייחס לקבוצות הבאות של מכשור רפואי:

1. מכשור שאיננו אוגר מידע באופן מקומי ואיננו מחובר לרשת תקשורת.
2. מכשור שאוגר מידע באופן מקומי ואיננו מחובר לרשת תקשורת.
3. מכשור שאיננו אוגר מידע באופן מקומי ומחובר לרשת תקשורת.
4. מכשור שאוגר מידע באופן מקומי ומחובר לרשת תקשורת.

8.1.2. סקרי סיכוני אבטחת מידע ומבחני חדירה מבוקרים

מטרה: להבטיח עמידת מכשור רפואי וקישורו לרשת בדרישות מדיניות אבטחת המידע של המוסד ושל מתודולוגיות אבטחת מידע מקובלות בעולם.

א) מנהל אבטחת המידע ייזום סקרי אבטחת מידע של מערך המכשור הרפואי של המוסד.

1. מכשור רפואי בעל סיכון גבוה ייסקרו לפחות אחת ל – 18 חודש.
2. לגבי מכשור רפואי אחר ההנהלה תקבע את תדירות הסקרים בהתאם לרגישות המערך.

ב) הסקרים יבחנו את נושאי הניהול ואת יעילות אמצעי ההגנה (כולל אמצעים פיזיים ולוגיים) שיושמו במוסד ואת רמת הגדרות אבטחת המידע במכשור הרפואי הן ברמת

התשתית (ציוד ותווך תקשורת, מערכות הפעלה, בסיסי נתונים) והן ברמת האפליקציה (ברמת קוד מקור או חבילות תוכנה).

ג) המוסד יערוך סקרי אבטחת מידע לפני הטמעת שינויים משמעותיים במכשור הרפואי שהוגדר ע"י המוסד כבעל סיכון גבוה לפי הערכת הסיכונים, כאשר חלו שינויים משמעותיים במכשור רפואי זה או לפני הכנסת מכשור רפואי זה לשימוש תפעולי (Production).

ד) מנהל אבטחת המידע ייזום מבחני חדירה (Penetration Tests) הן ברמת התשתית והן ברמת היישום (אפליקציה), המדמים ניסיונות פריצה ע"י פורצים מתוך ומחוץ למוסד, הן כמשתמש קיים והן כפורץ ללא חשבון קיים, למערך המכשור הרפואי. תדירות מבחני החדירה תיקח בחשבון את רגישות המערך. מכשור רפואי הפתוח לתווך תקשורת ציבורי, יעבור מבחני חדירה לכל הפחות אחת ל – 18 חודש.

ה) סקרי אבטחת המידע ומבחני החדירה התקופתיים ייערכו ע"י גורם מקצועי, עצמאי, בלתי תלוי וחיצוני למוסד.

ו) הנהלת המוסד תקיים דיונים על תוצאות סקרי אבטחת המידע ומבחני החדירה ותפעל למימוש המלצותיהם תוך פרק זמן סביר.

8.2. בקרות אבטחת מידע

8.2.1. ניהול תקשורת ותפעול

8.2.1.1. נוהלי תפעול ואחריות תפעול

מטרה: להבטיח פעולה רציפה ובטוחה של מכשור רפואי.

כדי להבטיח פעולה רציפה ומאובטחת של מכשור רפואי המקושר לרשת הארגון יש ליישם תהליכים מבוקרים של תפעול המכשור הרפואי ואמצעי הקישור שלו לרשת הארגון ולתעדם בנוהל המתייחס בין היתר לנושאים הבאים: תהליכים, חלוקת אחריות, בקרות, טפסים.

8.2.1.2. הגנה מפני ניסיונות פגיעה

מטרה: להגן על שלמות, חיסיון ואמינות המידע והמכשור הרפואי ולמנוע פגיעה במטופלים.

א) על מנת להגן על סביבות המחשוב והתקשורת יבוצעו הפעולות הבאות:

1. הארגון יתקין, בנקודת הקישור של המכשור הרפואי לרשת, אמצעים מקובלים ונאותים המצמצמים את החשיפה לניסיונות פגיעה (כולל איתור, זיהוי ומניעת ניסיונות אלה). אמצעים אלו (אמצעי הבקרה) יגנו מפני פגיעה בשירותי המכשור הרפואי מפגיעה שמקורה ברשת הארגון ובשירותים ברשת הארגון מפני פגיעה שמקורה במכשור הרפואי, שימוש לא תקין במידע, במכשור הרפואי ובבסיסי הנתונים. דוגמא לאמצעים המצמצמים את החשיפה לניסיונות פגיעה הינה קיומן של מערכות לניהול בקרת גישה לרשת (NAC), לאיתור

ניסיונות חדירה מהאינטרנט ומתוך רשת הארגון (IDS/IPS), מערכות לסינון תכנים (Content Filtering) וכדומה.

הארגון יעדכן את גרסאות מערכת ההפעלה של המחשבים השייכים למכשור הרפואי וגרסאות תוכנות ההפעלה של המכשור הרפואי בהתאם להוראות יצרן מערכת ההפעלה, להוראות יצרן המכשור הרפואי **והערכת סיכוני אבטחת המידע.**

2. הארגון יעדכן את גרסאות טלאי אבטחת המידע של מערכת ההפעלה של המחשבים השייכים למכשור הרפואי ושל תוכנות ההפעלה של המכשור הרפואי בהתאם להוראות יצרן המכשור הרפואי ובהתאם **להערכת סיכוני אבטחת המידע.**
3. הארגון יעדכן את גרסאות החומרה והתוכנה של אמצעי הבקרה השייכים לסביבת המכשור הרפואי בהתאם להוראות יצרן המכשור הרפואי ובהתאם **להערכת סיכוני אבטחת המידע.**

ב) הארגון רשאי להשתמש באמצעי בקרה מקובלים ונתונים אחרים, ובלבד שמהות אבטחת המידע הנדרשת בסעיף זה לא תפגע.

ג) על הארגון להתאים את אמצעי הבקרה המקובלים והנאותים בהתאם להתפתחויות הטכנולוגיות שישררו באותה עת, ולאיומים ולחשיפות הרלוונטיים לאותה תקופה, תוך התבססות על הוראות יצרן המכשור הרפואי.

8.2.1.3. **זמינות נתונים ושירותים**

מטרה: להבטיח זמינות של מידע חיוני, שירותי עיבוד מידע ושירותי תקשורת.

א) הארגון יישם כלים להבטחת זמינות מידע של מכשור רפואי, שירותי עיבוד מידע ושירותי תקשורת שהוגדרו כחיוניים בתהליך הערכת הסיכונים.

ב) לצורך כך ישקול הארגון שימוש ביתירות של מערכות ומכשור רפואי, ציוד קישוריות, אמצעי בקרה וכדומה, באמצעים מקומיים או דרך שירותים של ארגון אחר.

ג) הנהלת הארגון תגדיר דרישות גיבוי למידע של מכשור רפואי שהוגדר כחיוני בתהליך הערכת הסיכונים.

ד) מנהל אבטחת המידע יהיה אחראי על בקרת איכות הגיבויים.

ה) אמצעי הגיבוי ישמרו במקום מרוחק, מאובטח ומוגן בפני פגיעה באמצעים ובתוכנם.

8.2.1.4. **תיחום השימוש בתשתיות מכשור רפואי**

מטרה: להגדיר ולתחם את השימוש המבוצע בתשתיות מחשוב ותקשורת המספקות שירותים למכשור רפואי.

א) השירותים שיסופקו על ידי ציוד מחשוב ותקשורת בסביבת המכשור הרפואי יוגבלו לשימוש במכשור הרפואי בלבד.

ב) אמצעי הבקרה בסביבת המכשור הרפואי יאפשרו צמצום החשיפה לפגיעה ברשת הארגון שמקורה בסביבת המכשור הרפואי וגם צמצום החשיפה לפגיעה בסביבת המכשור הרפואי שמקורה ברשת הארגון.

8.2.1.5. ניהול סביבת הרשת של המכשור הרפואי

מטרה: להבטיח את הגנת המידע והשירותים בסביבת הרשת של המכשור הרפואי.

א) קישור גורמים חיצוניים אל סביבת הרשת של המכשור הרפואי יתבצע באופן ריכוזי, דרך נקודות כניסה מבוקרות. לא תאושר התחברות אחרת.

ג) קישור של סביבת המכשור הרפואי לרשת הארגון יתבצע באופן ריכוזי, דרך נקודות כניסה מבוקרות. לא תאושר התחברות אחרת. ייושם מידור בין הסביבות השונות ברשת באמצעות חלוקה לוגית או פיזית של הרשת והגבלת אפשרות הקישור בין סביבות הרשת השונות. רמת המידור תיקבע בהתאם לרמת הרגישות של המכשור הרפואי, בהתאם **לתהליך הערכת סיכוני אבטחת מידע.**

ד) תיושם בקרה וסינון של תקשורת יוצאת ונכנסת אל סביבת המכשור הרפואי על פי הגדרות הארגון.

ה) תיושם בקרה על הפעילויות המתבצעות בסביבת התקשורת של המכשור הרפואי לאיתור אירועים חריגים. בנוסף לבקרה בדיעבד, תיושם בקרה בזמן אמת.

8.2.1.6. ניהול סביבת המחשוב של המכשור הרפואי

מטרה: להבטיח את הגנת המידע והשירותים בסביבת המחשוב של המכשור הרפואי ואת הגנת התשתית התומכת.

א) חיבור של התקן חיצוני למחשב של מכשור רפואי יבוצע בהתאם להוראות יצרן המכשור הרפואי בלבד. ממשקי התקנים חיצוניים במחשבים של המכשור הרפואי יבוקרו. לא יאושר כל חיבור של התקן חיצוני למחשב של מכשור רפואי שלא דרך ממשקי כניסה מבוקרים אלו.

ב) תיושם בקרה וסינון של מידע וקבצים יוצאים ונכנסים אל סביבת המכשור הרפואי על פי הגדרות הארגון.

ג) תיושם בקרה על הפעילויות המתבצעות בסביבת המחשוב של המכשור הרפואי לאיתור אירועים חריגים. בנוסף לבקרה בדיעבד, תיושם בקרה בזמן אמת.

8.2.1.7. תהליך העברת מידע רגיש בין סביבת המכשור הרפואי לרשת הארגון

מטרה: להגדיר את רמת האבטחה המינימלית הנדרשת להעברת מידע על פי סיווגו.

א) בהתייחס לרמות סיווג המידע שהוגדר בארגון בהתאם **לתהליך סיווג נכסי מידע**, יגדיר הארגון את דרישות אבטחת המידע ההכרחיות ליישום בתהליך העברת מידע השייך לסביבת מכשור רפואי.

ב) מידע רפואי המועבר יוגן באמצעים הולמים לשמירה על שלמות ואמינות הנתונים.

ג) קישוריות להעברת מידע בין רשת הארגון לסביבת המכשור הרפואי, או בכיוון השני, תבוקר באמצעי בקרה מקובלים על מנת לוודא כי המידע מועבר ליעדו בלבד.

ד) במידה והעברת המידע מבוצעת בתווך תקשורת ציבורי או בתווך אלחוטי:

1. מידע בעל סיווג יוגן באמצעים מקובלים לשמירת סודיות, אמינות ושלמות הנתונים.
2. מידע רפואי אישי ומידע שסווג כבעל סיווג גבוה, בהתאם **לתהליך סיווג נכסי מידע**, יוגן במנגנוני הצפנה סטנדרטיים לשמירה על סודיות, אמינות ושלמות הנתונים.

8.2.2. בקרת גישה לוגית

8.2.2.1. אכיפת בקרות גישה

מטרה: לאכוף מדיניות בקרות גישה מ/אל המכשור הרפואי.

א) ייושמו מנגנונים ממוכנים לניהול בקרות גישה מ/אל סביבת המכשור הרפואי ומ/אל מערכת הניהול שלו.

ב) בקרות גישה יורכבו מאמצעי זיהוי ובקרת הנתיב בין גורם מורשה לסביבה.

ג) מדיניות בקרת גישה תיקח בחשבון מידור מתאים של הרשאות.

8.2.2.2. אמצעי זיהוי

מטרה: לזהות באופן חד ערכי כל מורשה גישה למכשור הרפואי.

א) ייקבעו אמצעי זיהוי למכשור הרפואי ולשירותים לצורך זיהוי חד ערכי (Unique User ID) של הגורם מורשה הגישה.

ב) אמצעי הזיהוי יהיו אישיים ולא יותר שיתוף של אמצעי הזיהוי.

ג) אמצעי הזיהוי יוחלו הן על מערכות, הן על עובדי הארגון והן על משתמשים אחרים (ספקים וכדומה) המתחברים למכשור הרפואי ומהמכשיר הרפואי לשירותים ברשת הארגון.

ד) לכל הפחות, אמצעי הזיהוי יורכבו משילוב של שם משתמש (User Name) וסיסמא.

ה) נתוני הזיהוי יישמרו חסויים (הן בתווך התקשורת והן במערכות השונות).

ו) למכשור רפואי מוגדר כבעלות סיכון גבוה, בהתאם **להערכת סיכוני אבטחת מידע**, הארגון ישקול שימוש באמצעי זיהוי חזק כמוגדר **בנספח מונחים**. יש להשתמש בטכנולוגיה המונעת אפשרות העתקה או שחזור הפריטים.

ז) ייקבע פרק זמן של אי פעילות (Session Time Out) במכשור הרפואי ובשירותים שאליו מתחבר המכשור הרפואי שלאחריו יופעל מנגנון ניתוק תקשורת שיחייב זיהוי מחדש של הגורם הניגש. במידה ומנגנון הניתוק מטיל מגבלה על פעילות בעלת אופי רציף, יש להתריע לפני ניתוק התקשורת.

8.2.2.3. ניהול הרשאות

מטרה: לוודא שהרשאות הגישה מ/ אל המכשור הרפואי מאושרות, מוקצות ומתוחזקות כראוי.

א) יוגדר תהליך רישום וביטול רישום להרשאות גישה למכשור הרפואי ולשירותים וכן להרשאות גישה מהמכשיר הרפואי לשירותים ברשת הארגון.

ב) מתן הרשאות גישה מ/אל מכשור הרפואי ושירותים יוגבל ויפוקח בהתאם לרגישות המכשור הרפואי ורגישות השירותים ברשת הארגון אליהם המכשור הרפואי פונה, ובהתאם **להערכת סיכוני אבטחת מידע.** חובה לנהל טבלת הרשאות לעובדים בהתאם לתפקידם ולמידע הנדרש להם לצורך ביצוע תפקידם. חובה לנהל טבלת הרשאות למכשור רפואי בהתאם לדרישות התפקוד התקין שלו ולמידע הדרוש לתפקודו התקין.

ג) הרשאות הגישה לכל העובדים והמכשירים הרפואיים ייבחנו לפי שיקול דעת ההנהלה. לכל הפחות, הפעילות תתבצע **אחת לשישה חודשים** במערכות בעלות סיווג גבוה.

ד) ניהול ההרשאות ייעשה ע"י מנגנון ממוכן לניהול הרשאות.

8.2.2.4. בקרת גישה בין רשת הארגון לסביבת המכשור הרפואי

מטרה: לאכוף מדיניות בקרת גישה חזקה בגישה בין מכשור הרפואי לרשת הארגון.

א) בגישה מרשת הארגון לסביבת המכשור הרפואי, או בכיוון השני, נתוני ההזדהות ומידע רפואי אישי יוגנו בפני ציתות (הצפנה מקצה לקצה).

ב) בגישה מרשת הארגון לסביבת המכשור הרפואי, או בכיוון השני, תיושם בקרת גישה לוגית לסביבה, שתורכב מאמצעי זיהוי ובקרת הנתיב בין גורם מורשה לסביבה, תוך לקיחה בחשבון מידור מתאים של הרשאות.

ג) מחשבים ברשת הארגון המאופשרים בגישה לסביבת המכשור הרפואי יכילו אמצעים מקובלים ונאותים המצמצמים את החשיפה לניסיונות פגיעה בסביבת המכשור הרפואי (כולל איתור, זיהוי ומניעת ניסיונות אלה).

ד) מחשבים בסביבת המכשור הרפואי המאופשרים בגישה לרשת הארגון יכילו אמצעים מקובלים המצמצמים את החשיפה לניסיונות פגיעה ברשת הארגון (כולל איתור, זיהוי ומניעת ניסיונות אלה) ובכפוף להוראות יצרן המכשור הרפואי.

8.2.2.5. **בקרת גישה מרשת האינטרנט/ רשת חיצונית לסביבת המכשור הרפואי**

מטרה: לאכוף מדיניות בקרת גישה חזקה בגישה למכשור הרפואי דרך האינטרנט/תשתית תקשורת ציבורית.

א) נתוני ההזדהות למכשור הרפואי ומידע רפואי אישי יוגנו בפני ציתות (הצפנה מקצה לקצה).

ב) תיושם בקרת גישה לוגית לסביבת המכשיר הרפואי, שתורכב מאמצעי זיהוי ובקרת הנתיב בין גורם מורשה לסביבה, תוך לקיחה בחשבון מידור מתאים של הרשאות.

ג) בגישה למכשור הרפואי לצורך ביצוע פעולות מהותיות ייעשה שימוש באמצעי זיהוי חזק, **לפי עקרונות אמצעי זיהוי**.

ד) בקישור עובדים, נותני שירות או סביבות תקשורת לסביבת התקשורת של המכשור הרפואי, תווך התקשורת יאובטח בפני ציתות וזליגת מידע. במקרה של חיבור עובדים תאובטחנה גם תחנות הקצה.

ה) לא תותר גישה ישירה מרשת האינטרנט / רשת חיצונית לסביבת מכשור רפואי של הארגון, אלא דרך מערכת שער (Gateway) מאובטחת, הממוקמת באזור מפורז מחוץ לסביבת המכשור הרפואי, שתיזום את ההתקשרות לסביבת המכשור הרפואי בשם הגורם הפונה.

ו) הארגון יממש אופן גישה מאובטח בהתייחס **להערכת סיכוני אבטחת מידע,** בקרת הגישה תכלול אמצעי זיהוי חזקים, הצפנת התווך מקצה לקצה, הקפדה על מדיניות הרשאות נוקשה ויישום בקרות למניעה ואיתור של חריגות.

ז) במקרה והמכשור הרפואי מכיל אופן גישה מרחוק מובנה, על הארגון לבחון את אופן הגישה בהתאם **להערכת סיכוני אבטחת המידע** ולפעול בהתאם.

ח) כל הגורמים הניגשים יזוהו באופן חד ערכי מול סביבת המכשור הרפואי (בהתאם **לעקרונות אמצעי זיהוי**).

ט) ארגונים יעגנו בהתקשרויות, כי גורמים הניגשים מרחוק למכשור הרפואי יפעלו לאבטחת המחשבים שלהם, על מנת למנוע פגיעה במכשור הרפואי, וכן ינקטו אמצעים לצמצום הפגיעה משימוש באינטרנט ובקרות גישה.

8.2.2.6. בקרת גישה ממכשור רפואי לרשת הארגון דרך רשת האינטרנט / רשת חיצונית

מטרה: לאכוף מדיניות בקרת גישה חזקה בגישה ממכשור רפואי לרשת הארגון דרך האינטרנט / תשתית תקשורת ציבורית / רשת אלחוטית / רשת סלולרית.

א) נתוני ההזדהות ומידע רפואי אישי יוגנו בפני ציתות (הצפנה מקצה לקצה).

ב) תיושם בקרת גישה לוגית לרשת הארגון, שתורכב מאמצעי זיהוי ובקרת הנתיב בין גורם מורשה לסביבה, תוך לקיחה בחשבון מידור מתאים של הרשאות.

ג) בגישה של המכשור הרפואי לרשת הארגון לצורך ביצוע פעולות מהותיות ייעשה שימוש באמצעי זיהוי חזק, לפי **עקרונות אמצעי זיהוי**.

ד) תווך התקשורת יאובטח בפני ציתות וזליגת מידע. במקרה של חיבור מכשור ארגוני הוא יאובטח.

ה) לא תותר גישה ישירה של מכשור רפואי מרשת האינטרנט / רשת חיצונית / רשת אלחוטית / רשת סלולרית לרשת הארגון, אלא דרך מערכת שער (Gateway) מאובטחת, הממוקמת באזור מפורז מחוץ לסביבת רשת הארגון, שתיזום את ההתקשרות לסביבת רשת הארגון בשם הגורם הפונה.

ו) הארגון יגדיר אופן גישה מאובטח בהתייחס **להערכת סיכוני אבטחת מידע**, בקרת הגישה תכלול אמצעי זיהוי חזקים, הצפנת התווך מקצה לקצה, הקפדה על מדיניות הרשאות נוקשה ויישום בקרות למניעה ואיתור של חריגות.

ז) כל הגורמים הניגשים יזוהו באופן חד ערכי מול רשת הארגון (בהתאם **לעקרונות אמצעי זיהוי**).

ח) ארגונים יעגנו בהתקשרויות, כי מכשור רפואי ארגוני הניגש מרחוק לרשת הארגון יופעל בסביבה מאובטחת, על מנת למנוע פגיעה במערכות המידע של הארגון, וכן ינקטו אמצעים לצמצום הפגיעה מקישוריות לאינטרנט ובקרות גישה.

ט) גישה של מכשיר רפואי לרשת הארגון דרך רשת אלחוטית תמומש בהתאם להוראות משרד הבריאות בנושא קישוריות אלחוטית במוסדות רפואיים.

8.2.2.7. ניהול סיסמאות במכשור רפואי וברשת הארגון

מטרה: לאכוף שימוש בסיסמאות חזקות שתמנענה גישה של משתמשים לא מורשים אל המכשור הרפואי או גישה של מכשירים לא מורשים לרשת הארגון.

א) הארגון יגדיר מדיניות סיסמאות ויחילה בסביבת המכשור הרפואי וברשת הארגון.

ב) הסיסמא תהיה ידועה אך ורק למשתמש.

ג) הסיסמא הראשונית תוגדר ע"י המשתמש או תימסר לידיו באופן חסוי. בכל מקרה, הסיסמא לא תימסר דרך רשת האינטרנט, רשת אלחוטית או דרך התשתית לה נדרשת הסיסמא להזדהות.

ד) במידה וסיסמא נמסרת למשתמש, יש לאמת ראשית את זהות המשתמש. המשתמש יחויב לשנות את הסיסמא בהתחברות הראשונה למערכת.

ה) סיסמאות לא ישמרו באופן גלוי (Clear Text) או באופן הניתן לשחזור ברשומות, בזיכרון או במאגרי מידע.

ו) סיסמא תבוטל מידית בכל מקרה של חשש לפגיעה בחשאיותה. לא יתאפשר לשחזר את הסיסמא.

ז) מורכבות הסיסמא, תוקפה ותחולתה לפי סוגי הקהל – עובדים, נותני שירותים וכדומה – ייקבעו בהתאם לתקנים מקובלים (כגון ת"י 1495). לדוגמא: הסיסמא תורכב משילוב של אותיות וספרות, לא יאופשר שימוש בתווים זהים רצופים, תוקפה יפוג לאחר 60 יום, המערכת תינעל לגישה לאחר 4 ניסיונות גישה כושלים וכדומה.

ח) סיסמאות ברירות המחדל בגישה לסביבת מכשור רפואי תשוננה בהתאם למדיניות הסיסמאות הארגון.

8.2.3. בקרות ומנגנוני קריפטוגרפיה (Cryptography)

מטרה: להגן על החיסיון, המהימנות או השלמות של המידע.

8.2.3.1. מדיניות שימוש בבקרות קריפטוגרפיה (Cryptography)

א) הארגון יפתח ויישם מדיניות שימוש במנגנוני קריפטוגרפיה (Cryptography) להגנה על מידע רגיש.

ב) הארגון יגדיר את סוגי המידע השונים הדורשים שימוש במנגנוני קריפטוגרפיה בהתאם לתהליך סיווג המידע שהארגון ביצע.

8.2.3.2. הצפנה (Encryption)

א) הארגון ישקול יישום מנגנוני הצפנה להגנה על חיסיון מידע בעל סיווג גבוה האגור באמצעי אחסון (קובץ, בסיס נתונים וכדומה), בהתאם **לתהליך סיווג נכסי מידע.**

ב) הארגון יישם הצפנה להגנה על חיסיון מידע בעל סיווג גבוה בתווך התקשורת מחוץ לארגון, בהתאם **לתהליך סיווג נכסי מידע.**

ג) בכל מקרה, יוצפנו כל סיסמאות הגישה לכל המכשור הרפואי וגם כל המידע הרפואי האישי (קצה לקצה).

8.2.3.3. חתימה דיגיטלית (Digital Signature)

א) הארגון ישקול יישום חתימה דיגיטלית להגנה על מהימנות ושלמות של מידע רפואי ומידע בעל סיווג גבוה, בהתאם **לתהליך סיווג נכסי מידע.**

ב) החתימה תיושם באופן שיאפשר לגופים מחוץ לארגון לזהות את בעלי החתימה הדיגיטלית באופן המקובל בסטנדרטים בין-לאומיים.

ג) בכל מקרה של ביצוע פעולות מהותיות ושינוי פרטים מהותי בסביבת המכשור הרפואי, על גבי האינטרנט/תשתית תקשורת ציבורית/אלחוטית, תיושם חתימה דיגיטלית באופן המבטיח את אימות זהות המשתמש.

ד) בכל מקרה של ביצוע פעולות מהותיות ושינוי פרטים מהותי ברשת הארגון על ידי מכשור רפואי, על גבי האינטרנט/תשתית תקשורת ציבורית/אלחוטית, תיושם חתימה דיגיטלית באופן המבטיח את אימות זהות המשתמש.

8.2.3.4. מנגנוני מניעת הכחשה (Non-Repudiation)

א) מנגנוני מניעת הכחשה יישומו בכדי ליישב מחלוקות לגבי התרחשות או אי-התרחשות של אירועים או פעולות, כפי שיוגדר במדיניות אבטחת המידע של הארגון.

ב) בכל מקרה של ביצוע פעולות מהותיות הכולל מידע בעל סיווג גבוה דרך האינטרנט וחברות צד שלישי, יבוצע שימוש בשירות זה באופן המבטיח את אימות זהות המבצע.

8.2.3.5. נתיב בקרה (Audit Trail)

מטרה: לגלות פעילויות לא מורשות ולזהות את מקורן.

א) הארגון יקיים מנגנון נתיב בקרה לניטור ומעקב אחר ביצוע פעולות ושאילתות במכשור רפואי וברכיבי תשתית שעליו הוא פועל, הן מתוך הארגון והן מחוצה לו.

ב) הארגון יקיים מנגנון נתיב בקרה לניטור ומעקב אחר ביצוע פעולות ושאילתות במערכות ברשת הארגון על ידי מכשור רפואי, הן מתוך הארגון והן מחוצה לו.

ג) על ה - Log להכיל את הנתונים הרלוונטיים, כך שיתאפשר לגלות ניסיונות גישה ופעולות לא מורשות ולזהות את מקורן. נתיב הבקרה יכלול מידע לפחות על מהות הפעולה, מקור הגישה וזמן הגישה.

ד) פרק הזמן לשמירת קבצי התיעוד ייקבע בהתאם לרגישות המכשור הרפואי ולמערכות ברשת שאליו ניגש המכשור הרפואי כפי שנקבעה בתהליך **הערכת סיכוני אבטחת מידע.**

ה) כל ניסיון גישה כושל וחריג למכשור הרפואי או למערכות ברשת שאליו ניגש המכשור הרפואי ינוטר ויתועד במנגנון אירועים.

ו) הארגון יידע את עובדיו וספקיו בדבר ביצוע רישום פעילויותיהם בקובץ לוג.

ז) על שעון מנגנון הניטור להיות מסונכרן עם מקור שעון מדויק לצורך דיוק התיעוד.

ח) קבצי ה – Log יאובטחו בפני מחיקה, שינוי או קריאה בלתי מורשים.

8.2.3.6. **קישור מכשור רפואי, עובדים ומערכות מידע המקושרות למכשור רפואי לאינטרנט**

מטרה: למנוע חשיפת מידע רגיש אל מחוץ לסביבת המכשור הרפואי ולצמצם יכולת פריצה של גורמים לא מורשים אל סביבת המכשור הרפואי.

א) הנהלת הארגון תגדיר את השימושים המותרים למכשור רפואי, לעובדים ולמערכות מידע המקושרות למכשור רפואי לקישור לאינטרנט.

ב) למערכות מידע ולעובדים המקושרים למכשור רפואי, וצריכים להיות מקושרים לאינטרנט, הקישור לאינטרנט יתאפשר באחד מן האופנים הבאים:

1. רשת ייעודית מנותקת לוגית או פיזית מסביבת המכשור הרפואי – תתאפשר הורדת קבצים ברשת ייעודית, תוך נקיטת אמצעי בקרה נאותים בלבד. הארגון יגדיר במסגרת מדיניות אבטחת המידע את סוגי הקבצים המורשים להורדה באופן קישור זה.
2. ממחשב שאינו מחובר לרשת (Stand Alone) – במקרה זה תתאפשר הורדת קבצים באופן מאובטח.

ג) הקישור לאינטרנט יאובטח בפני גישה בלתי מורשית מהאינטרנט, תוכנות זדוניות ושימוש בלתי תקין.

8.2.3.7. **מידע במכשיר רפואי**

מטרה: למנוע חשיפת מידע רגיש לגורמים לא מורשים בעלי גישה למכשור הרפואי.

א) במכשור רפואי המכיל מידע רפואי אישי יש ליידע את המשתמשים לגבי רמת סיווג המידע הנגיש.

ב) המכשור הרפואי לא יחשוף מידע פנימי שאינו נדרש למשתמש בזמן תקלה.

ג) באם ניתן לשמור מידע רפואי אישי במכשיר הרפואי נדרשת יכולת להציג בפני המשתמש את רמת סיווג המידע הנגיש, בהתאם לתקן 27799.

ד) תובטח פרטיות המידע הרפואי האישי השמור במכשור הרפואי, כשמידע רפואי מודפס וכשמידע רפואי מוצג לקהל.

9. נספח א' - מסמכים נוספים בנושא אבטחת מידע:

9.1. חוקים/דירקטיבות

9.1.1. ארה"ב

9.1.1.1 **HIPAA**

9.1.1.2 **HIPAA - OMNIBUS**

9.1.2. אירופה

9.1.2.1 **לא נכתב עדיין**

9.1.3. אסיה (סין, יפן, אוסטרליה)

9.1.3.1 **לא נכתב עדיין**

9.2. תקנים

9.2.1. ISO

9.2.1.1 **תקנים נוספים.**

9.2.2. Clinical Laboratory Standards Institute - CLSI

9.2.2.1 AUTO09-A:Remote Access to Clinical Laboratory Diagnostic

Devices via the Internet; Approved Standard

This document provides a standard communication protocol for instrument system vendors, device manufacturers, and hospital administrators to allow remote connections to laboratory diagnostic devices. The remote connections can be used to monitor instruments' subsystems; collect diagnostics data for remote system troubleshooting; and collect data for electronic inventory management.

http://shopping.netsuite.com/s.nl/c.1253739/it.A/id.963/.f

9.2.2.2 AUTO11-A: IT Security of In Vitro Diagnostic Instruments and Software Systems; Approved Standard

This document provides technical and operational requirements as well as technical implementation procedures related to security of IVD systems

(devices, analytical instruments, data management systems, etc.) installed at a healthcare organization.
http://shopping.netsuite.com/s.nl/c.1253739/it.A/id.955/.f

9.2.2.3. AUTO11 (Draft 2)—Information Technology Security of In Vitro Diagnostic Instrument and Software Systems

מסמך הטיוטה איננו נגיש (12/11/2013).

10. נספח ב' - מהו מכשור רפואי, סוגי מכשור רפואי:

10.1 FDA

10.1.1. כללי:

1. מכשור רפואי , לפי הגדרת ה- FDA , כולל גם מערכת מידע מכשור רפואי – Medical Device Data System (MDDS, וכן אפליקציות רפואיות לניידים – Mobile Medical Applications (25.9.2013)

הגדרות:

10.1.2. הגדרת ה-FDA למכשור רפואי – FDA Medical Device:

http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/ucm051512.htm

10.1.2.1. מכשור רפואי הנו כלי (instrument), מכשיר (apparatus), מכונה (machine), מתקן (contrivance), אביזר (contrivance), שתל (implant), חומר המשמש לריאקציה כימית מחוץ לגוף (in vitro reagent), או משהו דומה (or other similar or related article), כולל רכיב או תוסף (including a component part, or accessory) אשר:

10.1.2.1.1. מוכרת ב: official National Formulary, or the United States Pharmacopoeia, or any supplement to them

10.1.2.1.2. מיועד לשימוש בתהליך אבחון של מחלה, או מצבים אחרים, או בריפוי, טיפול, הקלה או מניעה של מחלה, באדם או חיות אחרות,

10.1.2.1.3. מיועד להשפיע על המבנה או כל פונקציה של גוף אדם או כל חיה אחרת, ואשר איננו משיג את מטרתו הראשונית באמצעות פעילות כימית בתוך הגוף או על גוף אדם או חיה אחרת, ואשר איננו תלוי בביצוע חילוף חומרים על מנת להשיג ולו אחת ממטרותיה הראשוניות.

10.1.2.2. דוגמאות למכשור רפואי:

10.1.2.2.1. דוחק לשון (Tongue depressor)

10.1.2.2.2. קוצבי לב

10.1.2.2.3. מתקני לייזר לניתוח

10.1.2.2.4. מכשור מעבדה

10.1.2.2.5. ציוד אבחון אולטרה סאונד

10.1.2.2.6. ציוד רנטגן (כיום קרויות CR-Computerized Roentgen)

10.1.2.2.7. לייזרים למטרות שימוש ברפואה.

10.1.2.3. ההגדרה מבטיחה:

10.1.2.3.1. הבחנה ברורה בין מכשיר רפואי (Medical Device) והמוצרים האחרים אשר ה- FDA מהווה עבורם רגולטור, כדוגמת סמים/תרופות (Drug).

10.1.2.3.2. במידה ומטרת השימוש הראשונית/העיקרית במוצר מושגת באמצעות פעילות כימית או באמצעות חילוף חומרים עם הגוף, המוצר מוגדר בדרך כלל סם/תרופה (Drug).

10.1.3. סוגי המכשור הרפואי עפ"י ה-FDA:

http://www.fda.gov/medicaldevices/deviceregulationandguidance/overview/classifyyourdevice/default.htm

10.1.3.1. ה-FDA הגדיר סיווג לכ-1,700 סוגים גנריים שונים של מכשירים וקיבץ אותם ל-16 קבוצות רפואיות המכונות פאנלים ("panels").

10.1.3.2. כל אחד מ-1,700 הסוגים הגנריים של מכשירים מוגדר לאחד משלוש רמות סיכון (Regulatory classes) עפ"י הסכנה הנשקפת לבריאות הציבור בעקבות תקלות בציוד או כשלים בבטיחות הציוד. רמת הסיכון של הציוד הרפואי קובעת את הכללים והבקרות שיחולו על הציוד כדלהלן: :

10.1.3.2.1. רמה 1 (Class I) – בקרות רגילות (general controls)

- כולל פטורים (With Exemptions)
- ללא פטורים (Without Exemptions)

10.1.3.2.2. רמה 2 (Class II) – בקרות רגילות (general controls) ובקרות מיוחדות (Special Controls)

- כולל פטורים (With Exemptions)
- ללא פטורים (Without Exemptions)

10.1.3.2.3. רמה 3 (Class III) – בקרות רגילות (general controls) ואישור טרם שיווק (Premarket Approval).

10.1.3.3. רמת הסיכון אליה משתייך המכשיר מגדירה (בין היתר) את תהליך הטרום שיווק הנדרש מהיצרן על מנת לקבל את אישור ה-FDA למכשיר. עבור רמות 1 ו-2 ללא פטורים, נדרש מילוי טופס 510(k). למכשירים ברמה 3 נדרש אישור טרם שיווק (PMA-PreMarket Approval Application). החלוקה לרמות מבוססת סיכונים שהמכשיר מציב למטופל או למשתמש בו. הסיכון מהווה מרכיב חשוב מאד בקביעת הרמה אליה משויך המכשיר. רמה 1 כוללת את המכשירים המציבים את הסיכון הקטן ביותר, ואילו רמה 3, את המכשירים המציבים את הסיכון הגבוה ביותר.

10.1.3.4. הקבוצות רפואיות הנן: :

http://www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/Overview/ClassifyYourDevice/ucm051530.htm

Medical Specialty (Panels)

1 Anesthesiology
2 Cardiovascular
3 Chemistry & Toxicology

4 Dental
5 Ear, Nose, and Throat
6 Gastroenterology and Urology
7 General and Plastic Surgery
8 General Hospital
9 Hematology & Pathology
10 Immunology & Microbiology
11 Neurology
12 Obstetrical and Gynecological
13 Ophthalmic
14 Orthopedic
15 Physical Medicine
16 Radiology

10.1.3.5. מכשיר המסווג לרמה 1 (Class I) הכולל פטורים עדיין מחויב בבקרות רגילות הכוללות (בין היתר) רישום (Registration & Listing), תיוות (Labeling) ונהלי ייצור תקינים (Good Manufacturing Practice, למעשה - Quality System , מערכת הבטחת איכות).

10.1.4. הגדרת ה-FDA עבור מערכת מידע מכשור רפואי – FDA Medical Device Data System (MDDS):

10.1.4.1. מערכת מידע מכשור רפואי (MDDS) הנה מכשור המיועד לספק אחד או יותר מהשימושים הבאים, ללא בקרה או שינוי הפונקציות או הפרמטרים של מכשירים רפואיים מקושרים:

1. העברה אלקטרונית של נתוני מכשור רפואי,
2. אגירה אלקטרונית של נתוני מכשור רפואי,
3. הסבה אלקטרונית שנתוני מכשור רפואי מתבנית אחת לתבנית אחרת בהתאם לספציפיקציות מוגדרות.
4. הצגה אלקטרונית של נתוני מכשור רפואי.

10.1.4.2. MDDS עשוי לכלול תוכנה, חומרה חשמלית או אלקטרונית כגון: תווך פיזי לתקשורת (כולל תווך פיזי אלחוטי), מודמים, ממשקים, ופרוטוקול תקשורת.

הגדרה זו איננה כוללת מכשירים שייעודם לפעול בהקשר של ניטור חולים אקטיבי.

10.1.4.3. באופן מעשי, MDDS הינו מכשור רפואי המיועד לספק אחד או יותר מהפונקציות הבאות:

1. העברה או החלפה אלקטרונית של נתוני מכשור רפואי ממכשור רפואי, ללא שינוי בפרמטר או בפונקציונאליות של מכשור רפואי מקושר כלשהו. לדוגמה, סעיף זה יכלול תוכנה האוספת נתונים ממכשיר לגבי רמות CO_2 אצל חולה ומשדרת את הנתונים למאגר נתונים מרכזי.
2. אחסון ואחזור אלקטרוני של נתוני מכשור רפואי, ללא שינוי בפרמטרים או פונקציונאליות של המכשור. לדוגמה: תוכנה האוגרת את היסטוריית רישומי לחץ הדם לבחינה מאוחרת יותר ע"י מטפל.
3. הסבה אלקטרונית של נתוני מכשור רפואי מתבנית אחת לאחרת בהתאם להגדרות שנקבעו מראש. לדוגמה, תוכנה הממירה נתונים דיגיטליים שיוצרו ע"י מכשיר oximeter לתבנית נתונים דיגיטליים שנתן להדפיסם.
4. הצגה אלקטרונית של נתוני מכשור רפואי, ללא שינוי של פונקציונאליות או פרמטרים במכשור רפואי. לדוגמה: תוכנה המציגה את הקרדיוגרם הקודם של חולה.

10.1.4.4. ישנו הסבר מפורט מה איננו MDDS. הדוגמה הבולטת הנם רכיבי IT רגילים שבהם נעשה שימוש במערכת הבריאות ואשר לא שונו או הותאמו מעבר להנחיות של יצרניהם. אלו אינם נחשבים MDDS גם באם בתהליך העבודה הם מאחסנים, מעבדים, מעבירים בתקשורת או מסבים נתוני מכשור רפואי בנוסף למידע אחר. דוגמאות הנם: נתבים, האבים, נקודות גישה אלחוטיות, NAS, SAN, תוכנת PDF, צג מחשב, מסך גדול ועוד.

10.1.4.5. MDDS הנו מכשור רפואי מרמה 1 (CLASS I) ופטור מהודעת טרום שיווק (premarket notification (510(k)). המשמעות הנה שכל התוכנות והחומרות הכלולות בהגדרת MDDS עדיין מחויבים בבקרות רגילות הכוללות (בין היתר) רישום (Registration & Listing), תיוות (Labeling) ונהלי ייצור תקינים

(Good Manufacturing Practice, למעשה - Quality System-מערכת הבטחת איכות).

10.1.5. הגדרת ה-FDA ליישום רפואי ניידת – FDA Mobile Medical Application (APPS):

10.1.5.1. יישומים ניידים הנם תוכנות המורצות על סמרטפונים ומכשירי תקשורת ניידים אחרים. הם יכולים להיות גם אביזרים נלווים (accessories) המתחברים לסמרטפון או מכשירי תקשורת ניידים אחרים או כשילוב של תוספת ותוכנה.

Mobile apps are software programs that run on smartphones and other mobile communication devices. They can also be accessories that attach to a smartphone or other mobile communication devices, or a combination of accessories and software.

יישומים רפואיים ניידים הנם מכשירים רפואיים (Medical Devices) שהנם יישומים ניידים, עומדים בהגדרת מכשירים רפואיים, והנם תוספת (Accessory) למכשירי רפואי הנתון למשטר רגולטורי או הופכות פלטפורמה ניידת ומכשיר רפואי במשטר רגולטורי.

Mobile medical apps are medical devices that are mobile apps, meet the definition of a medical device and are an accessory to a regulated medical device or transform a mobile platform into a regulated medical device.

10.1.5.2. כיצד יפעל ה-FDA על מנת לנהל את היישומים הרפואיים הניידים? ה-FDA יפעיל גישת ניהול סיכונים מדורגת המתמקדת בקבוצה קטנה יחסית של יישומים ניידים העונים להגדרה של "מכשיר" וגם:

1. מיועדים לשימוש כאביזר נילווה למכשיר רפואי המצוי במשטר רגולטורי של מכשיר רפואי, או
2. הופכים פלטפורמה ניידת למכשיר רפואי המצוי במשטר רגולטורי.

מדיניות ה-FDA איננה מחייבת מפתחי יישומים רפואיים ניידים לפנות לקבלת הערכה מחודשת עבור שינויים מינוריים במוצר.

FDA's mobile medical apps policy does **not** require mobile medical app developers to seek Agency re-evaluation for minor, iterative product changes.

10.1.5.3. על קבוצת המוצרים הבאה, המהווה סיכון מינימלי למטופל, ה-FDA יפעיל תהליך של enforcement discretions ללא דרישה מהיצרנים להעביר מידע קדם שיווקי או רישום מוקדם ב-רישומי ה-FDA:

- מסייעים לחולים/משתמשים לנהל את מחלתם/מצבם באופן עצמאי ללא אספקה של הנחיות או עצות טיפוליות,
- מספקים לחולים כלים פשוטים לארגן ולעקוב אחר מצבם הרפואי,
- מספקים גישה קלה למידע הקושר למצב רפואי או טיפול,
- מסייעים לחולים לתעד, להציג או להעביר בתקשורת מצבים רפואיים אפשריים לספקי שירות רפואי,
- ממכנים פעולות פשוטות של ספקי שירות רפואי,
- מאפשרים למטופלים או ספקים לקיים אינטראקציה עם מערכות רשומה רפואית אישית או רשומה רפואית אלקטרונית.

- Help patients/users self-manage their disease or condition without providing specific treatment suggestions;
- Provide patients with simple tools to organize and track their health information;
- Provide easy access to information related to health conditions or treatments;
- Help patients document, show or communicate potential medical conditions to health care providers;
- Automate simple tasks for health care providers; or
- Enable patients or providers to interact with Personal Health Records (PHR) or Electronic Health Record (EHR) systems.

10.2. מתוך חוק ציוד רפואי התשע"ב - 2012– מדינת ישראל:

10.2.1. "ציוד רפואי" – כל אחד מהמפורטים להלן, ולמעט תכשיר כהגדרתו בפקודת הרוקחים [נוסח חדש], התשמ"א–81981:

(1) מכשיר המשמש לטיפול רפואי, וכן מכשיר או תוכנת מחשב הנדרשים להפעלת מכשיר כאמור; לעניין זה, "מכשיר" – לרבות אבזר, חומר כימי, מוצר ביולוגי או מוצר ביוטכנולוגי;

(2) עדשות מגע;

(3) מכשיר חשמלי הפולט קרינה מיוננת או בלתי מיוננת המשמש לטיפול קוסמטי.

[8] **דיני מדינת ישראל, נוסח חדש 35, עמ' 694.**