תקן בינלאומי ISO 27799

מהדורה ראשונה
01.07.2008

תורת המידע בתחום הבריאות – ניהול ביטחון המידע בתחום הבריאות על ידי שימוש בתקן ISO/IEC 27002

תורגם לעברית על ידי איציק כוכב וצוותו- ממונה הגנת המידע בשירותי בריאות כללית

מסמך מוגן בזכויות יוצרים

<u>תוכן עניינים</u>

פתח דבר ... 4

מבוא ... 5

1. טווח ... **8**

1.1 כללי ... **8**

1.2 חריגות מן הטווח ... **8**

2. סימוכין נורמטיביים להתייחסות ... **8**

3. מונחים והגדרות ... **9**

3.1 מונחי בריאות ... **9**

4. ראשי תיבות (אנגלית) ... **12**

5. ביטחון מידע בריאות ... **12**

5.1. יעדי ביטחון מידע בריאות ... **12**

5.2. ביטחון מידע כחלק מן השליטה על המידע ... **13**

5.3. שליטה על המידע כמרכיב בשליטה הארגונית והקלינית ... **13**

5.4. מידע בריאות החייב בהגנה ... **13**

5.5. איומים וחשיפה לפגיעות בתחום ביטחון מידע הבריאות ... **14**

6. תוכנית פעולה מעשית ליישום תקן ISO/IEC 27002 ... **15**

6.1 הטקסונומיה של תקני ISO/IEC 27002 ו- ISO/IEC 27001 ... **15**

6.2. התחייבות ההנהלה ליישום תקן ISO/IEC 27002 ... **15**

6.3. ההקמה, תפעול, שמירה ושיפור של מערך ניהול ביטחון המידע ... **16**

6.4 תכנון: הקמתו של מערך ניהול ביטחון המידע ... **16**

6.5 עשייה: יישום ותפעול מערך ניהול ביטחון המידע ... **23**

6.6 בדיקה: פיקוח על מערך ניהול ביטחון המידע וסקירתו ... **24**

6.7 פעולה: שמירה על מערך ניהול ביטחון המידע ושיפורו ... **25**

7 השלכות תקן ISO/IEC 27002 על שירותי הבריאות ... **26**

7.1 כללי ... **26**

7.2 מדיניות ביטחון המידע ... **26**

7.1 מסמך מדיניות ביטחון המידע ... **26**

7.3 ארגון ביטחון המידע ... **27**

7.4 ניהול נכסים ... **29**

7.5 ביטחון משאבי אנוש ... **31**

7.6 ביטחון פיסי וסביבתי **33**
7.7 ניהול התקשורת והתפעול **35**
7.8 בקרת גישה **39**
7.9 רכש, פיתוח ואחזקה של מערכות מידע **43**
7.10 ניהול תקרית ביטחון מידע **44**
7.11 היבטי ביטחון מידע של ניהול ההמשכיות העסקית **45**
7.12 ציות **45**
נספח א' איומים על ביטחון מידע הבריאות 48
נספח ב' משימות מערך ניהול ביטחון המידע ומסמכים נלווים 53
נספח ג' יתרונות פוטנציאליים ותכונות הנדרשות מכלי תמיכה 55

פתח דבר

ISO (International Organization for Standardization) היא פדרציה כלל-עולמית של ישויות תקינה לאומיות (גופים חברים בארגון ISO). עבודת הכנתם של תקנים בינלאומיים מבוצעת על פי רוב באמצעות הוועדות הטכניות של ISO. כל גוף חבר המתעניין בתחום אשר בעבורו הוקמה וועדה טכנית רשאי להיות מיוצג באותה הועדה. ארגונים בינלאומיים, ממשלתיים ולא ממשלתיים נוטלים אף הם חלק בעבודה, תוך שיתוף פעולה עם ISO. ארגון ISO מקיים שיתוף פעולה הדוק עם IEC (International Electrotechnical Commission) ("הוועדה האלקטרו-טכנית הבינלאומית") בכל נושאי התקינה האלקטרו-טכנית.

התקנים הבינלאומיים מנוסחים בהתאם לכללים המפורטים במסמך ההנחיות של ISO/IEC, חלק 2.

משימתן העיקרית של וועדות טכניות היא להכין תקנים בינלאומיים. טיוטות של תקנים בינלאומיים אלה מועברות לגופים החברים לצורך הצבעה, והפרסום כתקן בינלאומי דורש את אישורם של 75% מן הגופים המצביעים לכל הפחות.

תשומת הלב מוסבת לכך, כי מרכיבים מסוימים של מסמך זה עשויים להיות כפופים לזכויות פטנט.
אין לראות את ISO כנושאת באחריות לזיהוין של זכויות פטנט אלה, כולן או מקצתן.

תקן ISO 27799 הוכן על ידי הוועדה הטכנית ISO/TC 215, *תורת מידע הבריאות*.

מבוא

תקן בינלאומי זה מנחה ארגוני שירותי בריאות, וישויות אחרות השומרות על מידע בריאות אישי, באשר לדרך המיטבית להגנה על סודיותו, שלמותו וזמינותו של אותו המידע על ידי היישום של תקן ISO/IEC 27002[1]. באופן ספציפי מטפל תקן בינלאומי זה בצרכי ניהול ביטחון המידע המיוחדים של מגזר הבריאות ושל סביבותיו התפעוליות הייחודיות. בעוד שההגנה על מידע אישי וביטחונו חשובים לכל אדם, חברה, ישות וממשלה, במגזר שירותי הבריאות קיימים צרכים ייחודים החייבים למצוא מענה על מנת שיובטחו הסודיות, השלמות, יכולת הבקרה והזמינות של מידע הבריאות האישי. סוג זה של מידע מוערך על ידי רבים כמידע כמעט הרגיש ביותר מקרב כלל סוגי המידע האישי. ההגנה על המידע דלעיל היא חיונית אם אנו שואפים לשמר את פרטיותם של המטופלים היחידים בהם המערכת מטפלת. שלמותו של המידע הרפואי חייבת להישמר כדי להבטיח את בטיחותו של המטופל, ומרכיב חשוב של הגנה זו הוא היכולת להבטיח כי מחזור החיים השלם של המידע ניתן לבקרה בשלמותו. זמינותו של מידע הבריאות קריטי גם מן ההיבט של האספקה היעילה של שירותי בריאות. מערכות מידע בתחומי שירותי הבריאות חייבות לתת מענה לדרישות ייחודיות, כגון ההישרדות במקרים של אסונות טבע, כשלים מערכתיים, והתקפות מניעת שירות יזומות על מאגרי המידע. ההגנה על הסודיות, השלמות והזמינות של מידע בריאות דורשת, אם כן, כי תתקיים מומחיות ספציפית למגזר שירותי הבריאות.

הצורך בניהול ביטחון יעיל של מערכות המידע בתחום שירותי הבריאות הופך לדחוף יותר לנוכח השימוש ההולך וגובר בטכנולוגיות אלחוטיות ומבוססות אינטרנט באספקת שירותי הבריאות. אם לא מיישמים אותן כהלכה, טכנולוגיות מורכבות אלה יגבירו את הסיכון הקיים לסודיותו, שלמותו וזמינותו של מידע הבריאות. ללא קשר לגודלן, מיקומן ומודל אספקת השירות שהן מאמצות, חייבות כלל ישויות שירותי הבריאות ליישם ביקורות קפדניות על מנת להגן על מידע הבריאות המופקד בידיהן. עם זאת, גורמים מקצועיים רבים בתחומי הבריאות פועלים כספקי בריאות עצמאיים, או במסגרת קליניקות קטנות שאינן מייעדות משאבי טכנולוגית מידע לניהול ביטחון המידע שברשותן. ארגוני שירותי בריאות חייבים, על כן, לקבל הנחיות ברורות, תמציתיות וספציפיות באשר לבחירתן ויישומן של בקרות אלה. קובץ הנחיות זה חייב להיות גמיש די הצורך כדי להיות בר-יישום בעבור קשת רחבה של גדלים, אתרי פעילות ומודלים של שירות בהם אנו נתקלים במגזר שירותי הבריאות. לבסוף, לנוכח החלפת מידע הבריאות האישי האלקטרונית ההולכת ותופסת תאוצה גם בקרב אנשי מקצוע בתחום הבריאות, קיים יתרון ברור באימוצו של מפתח התייחסויות משותף לניהול ביטחון המידע בתעשיית שירותי הבריאות.

התקן הבינלאומי ISO/IEC 27002 כבר נמצא בשימוש נרחב בתחומי ניהול ביטחון מידע הבריאות על בסיס הנחיות לאומיות, או אזוריות, במדינות שונות כמו אוסטרליה, קנדה, צרפת, הולנד, ניו זילנד, דרום אפריקה והממלכה המאוחדת. תקן בינלאומי זה (ISO 27799) מתבסס על הניסיון שנצבר במאמצים לאומיים אלה בכל הנוגע לטיפול בביטחונו של מידע הבריאות האישי, והוא נועד לשמש מסמך נלווה לתקן ISO/IEC 27002, אך אין הוא אמור להחליף את התקנים ISO/IEC 27002 או ISO/IEC 27001. תחת זאת, הוא מהווה השלמה לתקנים דלעיל הגנריים יותר.
תקן בינלאומי זה מיישם את ISO/IEC 27002 בתחום שירותי הבריאות, באופן בו ניתן שיקול זהיר לאפשרות יישומן הנאות של בקרות ביטחון שנועדו להגן על מידע הבריאות האישי. שיקולים אלה הובילו את המחברים, במקרים מסוימים, להסיק כי היישום של יעדי בקרה מסוימים הנכללים בתקן ISO/IEC 27002 הוא חיוני אם קיימת שאיפה להגן באופן ראוי על מידע בריאות אישי. לכן, מגביל תקן בינלאומי זה את יישומן של בקרות ביטחון מסוימות המפורטות בתקן ISO/IEC 27002. צעד זה, מאידך, הביא להכללתן של מספר הצהרות נורמטיביות בסעיף 7, המציינות כי יישומה של בקרת ביטחון מסוימת היא בגדר חובה. לדוגמה, סעיף קטן 7.2.1 מציין *על ארגונים המעבדים מידע בריאות, לרבות מידע בריאות אישי, תחול* ***חובה*** *להחזיק במדיניות ביטחון מידע המנוסחת בכתב המאושרת על ידי ההנהלה, והמפורסמת ומדווחת לכלל העובדים בארגון כמו גם לצדדים חיצוניים רלוונטיים.*
במגזר הבריאות יכול ארגון (בית חולים, לצורך הדוגמה) לקבל אישור על ידי שימוש בתקן ISO/IEC 27001 מבלי שיידרש לאישור רשמי על בסיס תקן בינלאומי זה, או אפילו לאישור בדבר הכרתו. יש לקוות, עם זאת, כי ככל שארגוני שירותי בריאות ישאפו לשפר את ביטחון מידע הבריאות האישי, העמידה בתקן בינלאומי זה, כתקן קפדני יותר לשירות בריאות תלך ותהפוך נפוצה יותר.

כל יעדי ביטחון מידע אלה, המתוארים בתקן ISO/IEC 27002 רלוונטיים לתורת מידע הבריאות, ואולם בקרות מסוימות דורשות הסברים נוספים באשר לאופן בו ניתן לעשות בהן שימוש מיטבי להגנה על הסודיות,

---

[1] הנחיה זו תואמת את הגרסה המעודכנת של ISO/IEC 27002: 2005.

השלמות והזמינות של מידע הבריאות האישי. כמו כן, נכללות כאן דרישות נוספות הספציפיות למגזר שירותי הבריאות. תקן בינלאומי זה מעניק הנחיות נוספות בפורמט המאפשר לנושא המשרה האחראי על ביטחון מידע הבריאות להבינן וליישמן בקלות.

אין כוונתם של המחברים של תקן בינלאומי זה לכתוב מסמך בתחום ביטחון מערכות המידע הממוחשבות, או לחזור על מה שנכתב זה מכבר בתקנים ISO/IEC 27002 או ISO/IEC 27001. קיימות דרישות ביטחון רבות המשותפות לכלל המערכות המבוססות מחשב, בין אם הן פועלות במגזרי השירותים הפיננסיים, הייצור, הבקרה התעשייתית ועוד, ובין אם בכל מאמץ מאורגן מסוג אחר. כאן נעשה מאמץ מרוכז כדי להתמקד בדרישות הביטחון העולות מן האתגרים הייחודיים של אספקת מידע הבריאות באמצעים אלקטרוניים, התומך בקידום הענקת שירות הבריאות בכללותו.

מי צריך לקרוא את התקן הבינלאומי הזה?

תקן בינלאומי זה מיועד בעבור אלה הנושאים באחריות לפיקוח על ביטחון מידע הבריאות, לארגוני שירותי בריאות, וגם בעבור ישויות אחרות המחזיקות בקרבן מידע בריאות והמבקשות לקבל הנחיות בנושא זה, לרבות יועצי ביטחון המידע שלהן, יועצים אחרים, מבקרים, ספקים וצדדים שלישיים המהווים ספקי שירותים.

היתרונות הכרוכים בשימוש בתקן הבינלאומי

ISO/IEC 27002 הוא תקן רחב יריעה ומורכב, והעצות הכלולות בו אינן מיועדות באופן ספציפי לתעשיית שירותי הבריאות. תקן בינלאומי זה מאפשר את יישומו של ISO/IEC 27002 בסביבת בריאות באופן עקבי, תוך תשומת לב מיוחדת לאתגרים המיוחדים המאפיינים את התעשייה הזו. ארגון המאמץ ומיישם את התקן מסייע להבטיח כי נשמרות סודיותו ושלמותו של המידע המוחזק על ידו, כי מערכות מידע בריאות קריטיות ממשיכות להיות זמינות, וכי הנשיאה באחריות למידע הבריאות נשמרת אף היא.
יישומן של הנחיות אלה על ידי ארגוני שירותי בריאות, הן בתוך מדינות, ובמישור הבין-מדינתי, יסייע בתפעול ההדדי ובאימוץ הבטוח של טכנולוגיות שיתוף פעולה חדשות הזמינות באספקת שירותי הבריאות. שיתוף מידע בטוח, וכזה המגן על פרטיותו, יכול לשפר במידה ניכרת את תוצאותיהם של שירותי הבריאות.
כתוצאה מיישומן של הנחיות אלה, יכולים ארגוני שירותי הבריאות לצפות לקיטון במספרן ובחומרתן של תקריות הביטחון שלהם, מה שיאפשר את הפנייתם של משאבים לפעילות יצרנית אחרת. ביטחון מערכות המידע יאפשר על ידי כך את השימוש היעיל מבחינת עלויות, והיצרני, של משאבי הבריאות העומדים לרשות הארגון. ואכן, מחקר שנערך על ידי "פורום ביטחון המידע" בעל המוניטין, כמו גם על ידי אנליסטים שונים, מצביע על כך כי ביטחון יעיל ומקיף עשוי לתרום עד 2% בקירוב לשיפור תוצאותיו של הארגון.

לבסוף, גישה עקבית לנושא מערכות המידע הממוחשבות בארגון, המובנת לכלל המעורבים בהענקת שירותי הבריאות, תשפר את מוראל העובדים ואת אמון הציבור במערכות השונות המנהלות את מידע הבריאות האישי.

כיצד להשתמש בתקן בינלאומי זה

לקוראים שטרם התוודעו לפרטיו של ISO/IEC 27002 אנו ממליצים לקרוא את קטעי המבוא של התקן הבינלאומי דלעיל לפני שהם ממשיכים. המיישמים של התקן הבינלאומי הנוכחי (ISO/IEC 27799) חייבים לקרוא ראשית ביסודיות את תקן ISO/IEC 27002, שכן הטקסט שלהלן יפנה את הקורא לעיתים קרובות לקטעים רלוונטיים שונים בתקן בינלאומי זה. לא ניתן להבין את המסמך הנוכחי במלואו ללא גישה לנוסח המלא של ISO/IEC 27002.

קוראים כלליים שטרם התוודעו לנושא ביטחון מידע הבריאות ולמטרותיו, לאתגרים הגלומים בו, ולהקשרים הרחבים יותר, יראו תועלת בקריאתו של מבוא קצר הנמצא בפרק 5.
קוראים המעוניינים לקבל הנחיות באשר ליישומו של תקן ISO/IEC 27002 בסביבת שירותי בריאות ימצאו תוכנית פעולה מעשית בפרק 6, שאינו כולל כל דרישה מחייבת. תחת זאת, הוא מעניק עצות והנחיות כלליות באשר לדרך המיטבית לקראת יישומו של 27002 בתחום אספקת שירותי הבריאות. הפרק מאורגן סביב מחזור של פעילויות שונות ("תכנן/בצע/בדוק/פעל") המתוארות ביתר פירוט בתקן ISO/IEC 27001 ואשר, אם הוא ייושם, יוביל ליישום של מערך ניהול ביטחון מידע שייתן את אותותיו בכל רובדי הארגון.
קוראים המחפשים הכוונה ספציפית יותר באשר לאחד עשר סעיפי הביטחון ושלושים ותשע קטגוריות הביטחון העיקריות, המתוארים כולם בתקן ISO/IEC 27002, ימצאו אותם בפרק 7. פרק זה מפרט למען הקורא את כל

אחד מאחד עשר סעיפי הביטחון של ISO/IEC 27002. דרישות מינימאליות מצוינות כאשר הדבר נדרש, ובמקרים אחדים ניתן פירוט להנחיות נורמטיביות באשר ליישום הנאות של בקרות ביטחון מסוימות לנושא ההגנה על מידע בריאות הכלולות בתקן ISO/IEC 27002.

תקן בינלאומי זה מסתיים עם שלושה נספחים לידיעה. נספח א' מתאר את האיומים הכלליים למידע הבריאות. נספח ב' מתאר בתמציתיות את המשימות והמסמכים הנלווים של מערך ניהול ביטחון המידע, ואילו נספח ג' דן ביתרונותיהם של כלי תמיכה ככלים המסייעים ליישום. הביבליוגרפיה מציינת תקנים קשורים נוספים העוסקים אף הם בביטחון מידע בריאות.

תורת המידע בתחום הבריאות – ניהול ביטחון המידע בתחום הבריאות
על ידי שימוש בתקן ISO/IEC 27002

1. טווח

1.1 כללי

תקן בינלאומי זה מגדיר הנחיות לתמיכה בפרשנות והיישום של תקן ISO/IEC 27002 בתורת המידע בתחום הבריאות, והוא מהווה מסמך נלווה לתקן ההוא.[2]

תקן בינלאומי זה מפרט סדרה של בקרות מפורטות לניהול ביטחון מידע הבריאות, והוא מעניק הנחיות באשר לנהלים המיטביים בביטחון מידע הבריאות. על ידי יישומו של תקן בינלאומי זה יעלה בידי ארגוני שירותי בריאות, וישויות אחרות המחזיקות בקרבן מידע בריאות, להבטיח רמה מינימאלית של ביטחון המתאימה לנסיבות בהן פועל הארגון שלהם, ואשר יצליחו לשמר את הסודיות, השלמות והזמינות של מידע בריאות אישי.

תקן בינלאומי זה נוגע למידע בריאות בכל היבטיו, ללא קשר למאפייניו וצורתו (מילים וספרות, הקלטות קול, שרטוטים ותרשימים, או תמונות וידיאו ורפואיות מסוגים אחרים), לאמצעים המשמים לאחסונו (הדפסה, כתיבה על נייר, או אחסון אלקטרוני) ולאמצעים המשמים לשידורו או העברתו (ביד, פקס, הדואר, או באמצעות רשתות מחשב), שכן המידע חייב להיות מוגן כיאות בכל אחד מן המצבים דלעיל.

תקן בינלאומי זה ו-ISO/IEC 27002 יחד, מגדירים *מה* נדרש במונחי ביטחון מידע במגזר שירותי הבריאות; אין הם מציינים *כיצד* יש לעמוד בדרישות אלה. דהיינו, וככל שהדבר מתאפשר, תקן בינלאומי זה הוא ניטראלי מבחינה טכנולוגית. ניטראליות באשר ליישומן של טכנולוגיות היא מאפיין חשוב. טכנולוגית הביטחון עוברת עדיין שינויים ועדכונים מהירים, כאשר קצב ההתפתחות נמדד בעת הזו בחודשים ולא בשנים. בניגוד לכך, ובכפוף לעדכונים תקופתיים, קיימת ציפייה לכך כי תקנים בכללם יישארו תקפים לאורך שנים. חשוב באותה המידה, הניטראליות הטכנולוגית היא המעניקה לספקים ולספקי שירותים את החופש להציע טכנולוגיות חדשות או מתפתחות העונות לצרכים הדרושים המתוארים על ידי תקן בינלאומי זה.

כפי שצוין במבוא, הכרתו של ISO/IEC 27002 היא חיונית להבנתו של תקן בינלאומי זה.

1.2 חריגות מן הטווח

התחומים הבאים של ביטחון המידע מצויים מחוץ לטווח של תקן בינלאומי זה:

(א) מתודולוגיות ובחינות סטטיסטיות לצורך אנונימיזציה יעילה של מידע בריאות אישי;

(ב) מתודולוגיות להשגת פסאודונימיזציה של מידע בריאות אישי (ראה התייחסות ביבליוגרפית [10] לדוגמה של הנחית ISO טכנית הדנה בסוגיה זו);

(ג) איכות רשת של שירות ושיטות לבחינת זמינותן של רשתות הנמצאות בשימוש בטכנולוגית המידע בתחום הבריאות;

(ד) איכות המידע (יש להבדילו משלמות המידע).

2. סימוכין נורמטיביים להתייחסות

המסמכים המפורטים להלן הם חיוניים ליישומו של המסמך הנוכחי. עבור מסמכים מתוארכים, הגרסה המצוינת בלבד היא החייבת להיות מיושמת. בעבור מסמכים להתייחסות שאינם נושאים תאריך, יש להתייחס לגרסתם האחרונה (לרבות כל שינוי).

[2] הנחיה זו תואמת את הגרסה המעודכנת של ISO/IEC 27002: 2005.

3. מונחים והגדרות

המונחים וההגדרות שלהלן תקפים למטרותיו של מסמך זה:

3.1 מונחי בריאות

3.1.1. תורת מידע בתחום הבריאות (אינפורמטיקה)

דיסציפלינה מדעית העוסקת במשימות הקוגניטיביות, עיבוד המידע והתקשורת של העבודה, החינוך והמחקר המתבצעים בתחום שירותי הבריאות, לרבות מדע וטכנולוגיות המידע הנדרשים לתמיכה במשימות אלה.

[הגדרה 3.73, ISO/TR 18307:2001]

3.1.2. מערכת מידע בריאות

מאגר מידע באשר לבריאותו של מטופל יחיד המקבל שירות בריאות, והקיים בצורת עיבוד ממוחשבת, מאוחסן ומועבר באופן בטוח, והזמין למשתמשים מורשים מרובים.

הערה – הותאם מהגדרה 2.25, מסמך ISO/TR 20514:2005

3.1.3. שירות בריאות

כל סוג של שירות המוענק על ידי אנשי מקצוע או שווי-ערך לאנשי מקצוע, ואשר יש לו השפעה על סטאטוס הבריאות.

[הפרלמנט האירופי, 1998, כפי שהוא צוטט על ידי ארגון הבריאות העולמי WHO]

3.1.4. ארגון שירות בריאות

מונח גנרי בו נעשה שימוש לתיאור סוגים רבים של ארגונים המעניקים שירותי בריאות.

[הגדרה 3.74, ISO/TR 18307:2001]

3.1.5. איש מקצוע בתחום הבריאות

אדם, המורשה מטעם ישות מוכרת, כמוסמך למלא אחר חובות מסוימים בתחום הבריאות.

הערה – הותאם מהגדרה 3.18, ISO/TS 17090-1:2002.

3.1.6 ספק שירות בריאות

כל אדם או ארגון המעורבים באספקתו של שירות בריאות ללקוח, או הקשורים לאספקה זו, או לחילופין באספקת רווחה כוללת ללקוח.

3.1.7. אדם הניתן לזיהוי

אדם הניתן לזיהוי, בין אם באופן ישיר ובין אם עקיף, בייחוד על ידי התייחסות למספר זיהוי, או לגורם אחד, או יותר, הייחודיים לזהותו הפיסית, הפיזיולוגית, המנטאלית, כלכלית, תרבותית או חברתית.

[הגדרה 3.7, ISO 22857:2004].

3.1.8 מטופל

האדם המקבל את הטיפול הרפואי (ראה להלן, **3.1.10**).

3.1.9 מידע בריאות אישי

מידע הנוגע לאדם הניתן לזיהוי, והקשור למצבו הפיסי או הנפשי, או לחילופין לאספקת שירותי בריאות לאותו האדם, והיכול לכלול:

(א) מידע באשר לרישומו של היחיד לקבלת שירותי בריאות;

(ב) מידע על אודות תשלומים או ההתאמה לשירות בריאות, הנוגע למטופל יחיד;

(ג) מספר, סימן או ציון אחר המוקצים ליחיד כדי שניתן יהיה לזהותו באופן ייחודי למטרות בריאות;

(ד) כל מידע הנוגע ליחיד ואשר נאסף במהלך הענקתם של שירותי בריאות ליחיד;

(ה) מידע הנגזר מן הבחינה או הבדיקה של איבר בגוף או של חומר השייך לגוף האדם;

(ו) זיהויו של אדם (כגון איש מקצוע בתחום הבריאות) כספק של שירות בריאות ליחיד.

הערה: מונח מידע הבריאות אישי **אינו** כולל מידע, בין אם כשלעצמו ובין אם בשילוב עם מידע אחר הזמין למחזיק במידע, שעבר תהליך של אנונימיזציה, כלומר מידע אשר לגביו, ומן המידע עצמו, לא ניתן לקבוע את זהותו של בעליו.

3.1.10 הנהנה משירות הבריאות

אדם אחד, או יותר, המתוכנן לקבל, או המקבל, או שקיבל בעבר, שירות בריאות כזה או אחר.

[הגדרה 3.40, ISO/TS 18308:2004].

3.2. מונחי ביטחון מידע

3.2.1. נכס

כל דבר שהוא בעל ערך לארגון.

[הגדרה 2.2, ISO/IEC 13335-1:2004]

הערה: בהקשר של ביטחון מידע בריאות, המונח "נכסים" כולל:

(א) מידע בריאות;

(ב) שירותי טכנולוגית מידע;

(ג) חומרה;

(ד) תוכנה;

(ה) מתקני תקשורת;

(ו) מדיה;

(ז) מתקני טכנולוגיות מידע;

(ח) מתקנים או מכשירים רפואיים הרושמים מידע או מדווחים עליו.

3.2.2. נשיאה באחריות

תכונה המבטיחה כי ניתן לקשור את מהלכיה של ישות כלשהי באופן ייחודי לישות עצמה.

[הגדרה 3.3.3, ISO 7498-2:1989]

3.2.3. ביטחון, וודאות

התוצאה של סדרה של תהליכי ציות, דרכם ארגון משיג מידה של אמון בסטאטוס של ניהול ביטחון המידע שלו.

3.2.4. זמינות

התכונה של להיות זמין ובר-שימוש על ידי ישות מורשית, על פי הצורך.

[הגדרה 3.3.11, ISO 7498-2:1989]

3.2.5. הערכת ציות

תהליכים על פיהם ארגון מוודה כי בקרות ביטחון המידע הקיימות בקרבו נותרות תפעוליות ויעילות.

הערה: הציות החוקי מתייחס באופן מפורש לבקרות הביטחון הקיימות לצורך השגת ציות לחקיקה הרלוונטית, כגון הנחיית האיחוד האירופי בדבר ההגנה על מידע אישי.

3.2.6. סודיות

תכונה לפיה מידע אינו הופך גלוי, זמין או שהוא מועבר ליחידים, ישויות או תהליכים בלתי מורשים.

[הגדרה 3.3.16 ISO 7498-2:1989]

3.2.7. שלמות המידע

תכונה לפיה מידע לא שונה או נהרס באופן שאינו מורשה.

[הגדרה 3.3.21 ISO 7498-2:1989]

3.2.8. ניהול מידע

תהליכים לפיהם ארגון מקבל מידה של ביטחון באשר לכך כי הסיכונים למידע שלו, ובאמצעות כך גם היכולת התפעולית והשלמות של הארגון, מזוהים ומנוהלים באופן יעיל.

3.2.9. ביטחון מידע

השמירה על סודיות, שלמות וזמינות המידע.

הערה: תכונות אחרות, במיוחד הנשיאה באחריות של משתמשים, אך גם האמיתות, מקוריות, אי-ההתנערות והמהימנות מצוינים לעיתים קרובות כהיבטים של ביטחון המידע, ואולם ניתן להתייחס אליהם כנגזרים משלושת התכונות הגרעיניות הגלומות בהגדרה.

3.2.10 סיכון

שילוב בין הסבירות לכך כי אירוע יתרחש והשלכתו.

[הגדרה 3.1.1, מדריך ISO 73:2002]

3.2.11 הערכת סיכון

התהליך הכולל של ניתוח והערכת סיכונים.

[הגדרה 3.3.1, מדריך ISO 73:2002]

3.2.12 ניהול הסיכון

פעילויות מתואמות שנועדו לכוון ולבקר ארגון בכל הנוגע לסיכון.

הערה: ניהול הסיכון יכלול בדרך כלל הערכת סיכון, הטיפול בו, קבלת הסיכון ודיווח בדבר הסיכון.

[הגדרה 3.1.7, מדריך ISO 73:2002]

3.2.13 טיפול בסיכון

תהליך הבחירה והיישום של צעדים שנועדו לשנות (על פי רוב להקטין) את הסיכון.

הערה: הותאם מהגדרה 3.4.1, מדריך ISO 73:2002.

3.2.14 שלמות מערכת

תכונה לפיה מערכת מבצעת את תפקידה המיועד ללא הפרעה, ללא מניפולציה מכוונת או מקרית.

3.2.15 איום

הסיבה הפוטנציאלית של תקרית בלתי רצויה, היכולה להתבטא בגרימת נזק למערכת או ארגון.

[הגדרה 2.25, ISO/IEC 13335-1:2004].

3.2.16 פגיעות

חולשתו של נכס, או של קבוצה של נכסים, היכולה להיות מנוצלת על ידי איום אחד או יותר.

[הגדרה 2.26, ISO/IEC 13335-1:2004].

4. ראשי תיבות (אנגלית)

ISMF	פורום ניהול ביטחון המידע
ISMS	מערכת ניהול ביטחון המידע
IT	טכנולוגית מידע
SLA	הסכם רמת שירות
SOA	הצהרת יישום.

5. ביטחון מידע בריאות

5.1. יעדי ביטחון מידע בריאות

השמירה על סודיותו, זמינותו ושלמותו של המידע (לרבות אמיתות, נשיאה באחריות ויכולת הכפיפות לביקורת) מהווה את היעד המרכזי של ביטחון המידע. בכל הנוגע לשירותי בריאות, תלויה פרטיותו של המטופל בשמירה על סודיות מידע הבריאות האישי. כדי לשמר סודיות זו חייבים להינקט, גם, צעדים לשמירה על שלמותו של המידע, ולו רק כדי למנוע את האפשרות להשחית את מנגנוני הגישה למידע ושל הבקרה עליו באופן כזה שיאפשר הפרה של סודיות, או של הפרת סודיות שלא תאותר. בנוסף, בטיחותו של המטופל תלויה בשמירה על שלמות מידע הבריאות האישי; הכישלון בכך עלול להוביל גם להתפרצותה של מחלה, פגיעה או אפילו למותו של המטופל. באופן דומה, דרגה גבוהה של זמינות מהווה מאפיין ראשון במעלה בחשיבותו בקרב מערכות בריאות, בהן עיתוי הטיפול הוא לעיתים קרובות קריטי. יתרה מזו, זמינותם של מאגרי מידע בריאות עשויה להתגלות כקריטית במקרים של פגיעה או השחתה של מערכות מידע שאינן מערכות בריאות. כמו כן, מניעת התקפות שירות נגד מערכות מרושתות הופכת גם היא לנפוצה יותר ויותר.

הבקרות הנדונות בפרק 7 הן אלה שזוהו כמתאימות למגזר שירותי הבריאות במאמץ להגן על סודיותו, שלמותו וזמינותו של מידע הבריאות האישי, וכמבטיחות כי הגישה למידע דלעיל תוכל להיות נתונה לבקרה ומעקב. בקרות אלה מסייעות למנוע טעויות בעבודה הרפואית העלולות להיגרם מחוסר היכולת לשמר את שלמותו של מידע הבריאות. בנוסף, בקרות אלה תורמות את חלקן להמשכיותם של השירותים הרפואיים.

קיימים שיקולים נוספים המעצבים את יעדי ביטחון מידע הבריאות, והם כוללים את המפורטים להלן:

(א) כיבוד הוראות החוק כפי שאלה מבוטאות בחקיקת ההגנה על המידע והתקנות הרלוונטיות לשמירה על זכותו של מטופל לפרטיות;[3]

(ב) ההקפדה על שיטות עבודה מיטביות בתחומי הפרטיות והביטחון במערכות מידע הבריאות;

(ג) שמירה על הגדרות נשיאה באחריות ברורות, הן ברמת הפרט והן ברמת הארגון, בקרב ארגוני ואנשי מקצוע בתחום שירותי הבריאות;

(ד) התמיכה ביישום ניהול סיכונים שיטתי בקרב ארגוני בריאות;

(ה) מתן מענה לצרכי הביטחון המזוהים במצבי שירותי בריאות נפוצים;

(ו) הקטנת ההוצאות התפעוליות על ידי קידום השימוש בטכנולוגיות באופן בטוח, מאובטח ומנוהל נכון התומך בפעילות שירותי הבריאות השוטפת – אך אינו מגביל אותה.

[3] בנוסף לחובות על פי דין, קיים מידע בהיקף עצום בנושא החובות האתיים הנוגעים למידע בריאות, לדוגמה הקוד האתי של ארגון הבריאות העולמי. חובות אתיים אלה יוכלו, בנסיבות מסוימות, להיות בעלות השלכות על מדיניות ביטחון מידע הבריאות.

(ז) השמירה על אמון הציבור בארגוני הבריאות ובמערכות המידע עליהן מתבססים ארגונים אלה;

(ח) ההקפדה על סטנדרטים מקצועיים ואתיים כפי שאלה נקבעו על ידי ארגוני בריאות (כל אימת שביטחון המידע שומר על סודיותו ושלמותו של מידע הבריאות);

(ט) ההפעלה של מערכות מידע בריאות אלקטרוניות בסביבה המוגנת כיאות מפני איומים;

(י) קידום התפקוד ההדדי המתואם בין מערכות בריאות, מאחר ומידע הבריאות זורם יותר ויותר בין ארגונים שונים, וחוצה גבולות שיפוט וחקיקה (במיוחד כאשר שיתוף הפעולה התפעולי דלעיל שם לעצמו כדגש את הטיפול הנכון במידע בריאות כדי להבטיח את סודיותו, שלמותו וזמינותו המתמשכות).

5.2. ביטחון מידע כחלק מן השליטה על המידע[4]

בשנים האחרונות הפכה סוגית השליטה על המידע לנושא קריטי בעבור ארגונים מכל הסוגים, זאת בעקבות החקיקה הרגולאטורית שקודמה על ידי פקודת Sarbanes Oxley האמריקאית, פקודת האחריות לביטוח הבריאות, להסכמי באזל II האירופיים, לקוד Turnbull הבריטי, ולפקודת הבקרה והשקיפות בניהול עסקים של הרפובליקה הפדראלית של גרמניה. כמו כן, הסתמכותם ההולכת וגוברת של ארגונים על מידע ועל הטכנולוגיות התומכות בו הופכים את השליטה על המידע למרכיב חשוב של תהליכי ניהול הסיכונים התפעוליים.

תחומים רבים בניהול המידע, כגון הסמכה והגנה על נתונים, יכולים להיחשב כנכללים בתוך הטווח של השליטה על המידע. חשוב ביותר כי טווח השליטה על המידע יכלול את ההשלטה השוטפת של ביטחון המידע, ואף יסייע בידה, כך שתשומת הלב הראויה תופנה בכל עת להקפדה על סודיותו, שלמותו וזמינותו של המידע. אין ספק באשר לכך, כי ביטחון המידע הוא מרכיב ראשון במעלה בחשיבותו המסייע ליישומם של ההיבטים הרחבים יותר של השליטה על המידע.

5.3. שליטה על המידע כמרכיב בשליטה הארגונית והקלינית

בעוד שארגוני בריאות יוכלו לאמץ גישות שונות בכל הנוגע לשליטה הקלינית והארגונית, חשוב כי מעמדה המרכזי של השליטה על המידע, לרבות שילובה בארגון והטיפול בה, יהיו מעבר לכל ויכוח ויובנו כמרכיב תמיכה חיוני לשני היבטי השליטה שצוינו לעיל. ככל שארגוני בריאות הופכים יותר ויותר תלויים במערכות מידע כדי לתמוך בהענקת שירות הבריאות (לדוגמה, על ידי ניצול של טכנולוגיות תמיכה בהחלטות ותמיכה במגמות, לקראת שירות בריאות "מבוסס ראיות" יותר מאשר "מבוסס ניסיון"), ברור לכל כי אירועים בהם מתרחשים אובדן של סודיות, שלמות או זמינות עלולים לגבות מחיר קליני משמעותי, כאשר הבעיות המתעוררות מהשלכה מעין זו יתפסו כאי עמידה בחובות האתיים והחוקיים הגלומות ב"חובת הטיפול הרפואי."

אין ספק בכך כי בכל מדינה ותחום שיפוט יימצא חקר אירוע שבו הפרות מעין אלה הובילו לאבחון שגוי, למקרי מוות, או להתאוששות ארוכה מן הרגיל. לכן, חייבות מסגרות השליטה הקלינית להתייחס ליעילותו של ניהול סיכוני המידע כאל שווה בחשיבותו כמו תוכניות הטיפול עצמן, אסטרטגיות ניהול זיהומים, או סוגיות "ליבה" קליניות אחרות.

5.4. מידע בריאות החייב בהגנה

קיימים מספר סוגי מידע שסודיותם, שלמותם וזמינותם[5] חייבות בהגנה:

(א) מידע בריאות אישי;

(ב) נתונים שעברו פסאודונימיזציה והנגזרים ממידע בריאות אישי באמצעות מתודולוגיה כלשהי לזיהוי על בסיס פסבדונים.

(ג) מידע סטטיסטי ומידע מחקר, לרבות מידע אנונימי הנגזר ממידע בריאות אישי על ידי הסרתם של מרכיבי הזיהוי האישי;

(ד) ידע קליני/רפואי שאינו קשור למטופל ספציפי כלשהו של שירות בריאות, לרבות נתוני תמיכה בהחלטה קלינית (כגון מידע באשר לתגובות שליליות למינון תרופות);

---

[4] במדינות מסוימות ההתייחסות לניהול המידע היא כאל ביטחון המידע.

[5] דרגת הזמינות תלויה בשימושים המיועדים של המידע.

(ה) מידע על אודות אנשי מקצוע בתחום הבריאות, צוותי עובדים ומתנדבים.

(ו) מידע הקשור בפיקוח על בריאות הציבור;

(ז) נתונים בדבר נתיב ביקורת, המיוצרים על ידי מערכות מידע הכוללות מידע בריאות אישי, או מידע לאחר תהליך פסאודונימיזציה הנגזר ממידע בריאות אישי, או מידע הכולל פרטים בדבר צעדיהם של משתמשים בכל הנוגע למידע בריאות אישי;

(ח) מידע בטיחות מערכת בעבור מערכות מידע בריאות, לרבות מידע בדבר בקרת גישה ומידע תצורה אחר, הנוגע לביטחון, בעבור מערכות מידע בריאות.

ההיקף בו הסודיות, השלמות והזמינות של המידע חייבות בהגנה תלוי בטיב המידע, השימושים שלו והסיכונים לו הוא חשוף. לדוגמה, מידע סטטיסטי (סעיף (ג) להלן) לא חייב בהכרח להיות סודי, ואולם השמירה על שלמותו עשויה להיות חיונית. באותו האופן, מידע נתיב ביקורת (סעיף (ז) להלן) לא בהכרח יחייב זמינות גבוהה (העברה תכופה לארכיב עם משך זמן למשיכת מידע הנמדד בשעות ולא בשניות יוכל להספיק ביישום כזה או אחר), ואולם תוכנו עשוי להיות סודי ביותר. הערכת סיכון יכולה לקבוע באופן נאות את דרגת המאמץ הנחוצה לשמירה על סודיות, שלמות וזמינות המידע (ראה 6.4.4). תוצאותיה של הערכת סיכונים שגרתית וקבועה חייבות להיות מותאמות לסדרי העדיפויות ולמשאבים של הארגון המבצע את ההערכה.

5.5. איומים וחשיפה לפגיעות בתחום ביטחון מידע הבריאות

קיימים סוגים רבים של איומים וחשיפות לפגיעות בביטחון המידע, והגדרותיהם מגוונות באותה המידה. בעוד שאף אחד מהם אינו באמת ייחודי לשירותי הבריאות, מה *שכן* ייחודי בתחום שירותי הבריאות הוא מגוון הגורמים הרחב עליו יש לתת את הדעת כאשר מעריכים איומים וחשיפות לפגיעות.

מטבעם, ארגוני בריאות פועלים בסביבה בה לא ניתן לעולם להוציא לחלוטין את גורמי המבקרים והציבור בכללו מזירות ההתרחשות. בארגוני שירותי בריאות גדולים, כמויות בני האדם הנעים דרך אזורי התפעול הן משמעותיות עד מאוד. גורמים אלה מגבירים את חשיפתן של המערכות לאיומים פיסיים. הסבירות לכך, כי סיכונים מעין אלה יתממשו עשויה לעלות כאשר בסביבה נמצאים מטופלים בלתי יציבים מבחינה רגשית או נפשית, או קרובי משפחתם.

ארגוני שירותי בריאות סובלים דרך קבע מתקצוב חסר, כאשר צוותיהם נדרשים לעיתים לעבוד תחת מצבי לחץ משמעותי. השלכות אחרות של צמצום זה של משאבים כוללות מערכות המתוכננות, מיושמות ומופעלות באופן שטחי יתר על המידה, או מערכות הנשמרות תפעוליות זמן רב אחרי שהן היון למעשה חייבות להיות מוחלפות במערכות חדישות יותר. הגורמים דלעיל עלולים להגביר את הסיכון להתממשותו של איום כזה או אחר ולהחמיר את החשיפה לפגיעות. מאידך, הטיפול הקליני מהווה עדיין תהליך בו מעורב טווח רחב של צוותי עובדים מקצועיים, טכניים, מינהלים, מסייעים, נלווים ומתנדבים, כאשר רבים מהם רואים בעבודתם שליחות. מסירותם וניסיונם המגוון של העובדים יכולים לסייע לעיתים קרובות בהקטנת החשיפה להיפגעות מסוגים שונים. כמו כן, רמת ההכשרה הגבוהה לה זוכים צוותי שירותי הבריאות שמה את התעשייה הזו ברמה נפרדת ממגזרי תעשייה רבים אחרים, בכך שהיא מקטינה את שכיחותם של האיומים הפנים-ארגוניים.

החשיבות המכרעת של הזיהוי הנכון של מטופלים ושל התאמתם הנכונה לרישומי הבריאות שלהם מובילה ארגוני בריאות לאיסוף מידע זיהוי מפורט. מרשמי מטופלים אזוריים או חוקיים אחרים (כגון מרשמי מטופלים) מהווים לעיתים את מאגרי המידע רחבי ההיקף והמעודכנים ביותר של מידע זיהוי הזמין באזור מסוים. מידע זיהוי זה יכול להיות בעל ערך פוטנציאלי רב לאלה העשויים לעשות בו שימוש לגניבת זהויות, ועל כן יש חובה להגן עליו בקפידה.

יש חובה, על כן, להתייחס לסביבת שירותי הבריאות, על איומיה וחשיפתה להיפגעות הייחודיים, בתשומת לב מיוחדת. נספח א' כולל רשימה לידיעה של סוגי האיומים שאותם חייבים ארגוני שירותי בריאות לשקול כאשר הם מעריכים את הסיכונים הקיימים לסודיותו, שלמותו וזמינותו של מידע הבריאות, כמו גם לשלמות והזמינות של מערכות המידע הקשורות בו.

6. תוכנית פעולה מעשית ליישום תקן ISO/IEC 27002

6.1 הטקסונומיה של תקני ISO/IEC 27002 ו- ISO/IEC 27001

תקן ISO/IEC 27002 מציע רשימת תיוג סטנדרטית לנושאים לביקורת באחד עשר תחומים הכוללים 39 קטגוריות ביטחון עיקריות, כאשר כל אחת מהן כוללת תאור של בקרת ביטחון אחת או יותר. המיישמים של תקן זה בסביבת שירותי הבריאות יגלו כי מרבית יעדי הבקרה חלים על כמעט מלוא המצבים. עם זאת, על משתמשי התקנים בתחום שירותי הבריאות לזהות גם מצבים אשר בהם יוכלו להידרש מטרות בקרה נוספות. זה לעיתים קרובות המקרה כאשר תהליכים קליניים משתלבים עם מכשור מתמחה, כגון סורקים, מכונות אינפוזיה, ועוד, גם אם בקרות הביטחון מתייחסות רק לשמירה על שלמותו של המכשור. אזורים גיאוגראפיים שונים יאמצו גם מסגרות חוקיות שונות העשויות לשנות את הטווח הדרוש של פעילות הציות.

תקן ISO/IEC 27001 מציע את המושג של "**מערך ניהול ביטחון המידע** (**ISMS**)" ומתאר את הצורך הקיים במסגרת מפורטת זו של בקרות כאשר ננקט מאמץ לעמוד ביעדי ביטחון שזוהו כרלוונטיים בתהליך הערכת הסיכונים בארגון. הניסיון הבינלאומי ועקרונות ההתנהלות המיטבית בתחום ביטחון המידע מצביעים על כך, כי הציות המתמשך להנחיותיו של תקן ISO/IEC 27002 יכול להיות מובטח באופן המיטבי על ידי יישומו של מערך הניהול המתואר בתרשים 1 להלן.

סדרת מסמכים לתהליך ISMS	תהליך תיעוד "תהליכים"	אירועים
▪ מדיניות ביטחון המידע ▪ תצהיר טווח ▪ תצהיר ישימות/רלוונטיות ▪ מלאי נכסי מידע ומערכות החייב בהגנה ▪ הערכת סיכונים ▪ נהלים ותקנים ישימים ▪ חוזים (הסכמי רמת שירות, הסכמי שימוש מותר, ועוד).	תהליכים עסקיים	▪ אירועי ביטחון ▪ חולשות נתפסות ▪ תקלות ▪ הערות ביקורת ▪ ממצאי בדיקות ▪ ממצאי בדיקות מדגמיות
סקירה ועדכון של ISMS	רישום וניתוח	"תיעוד ראייתי"
	דיווח לפורום/ים	

תרשים 1 – מערך ניהול ביטחון המידע

מומלץ לארגוני שירותי בריאות, ככל שהדבר אפשרי, לכלול את תהליך ISMS לעיל בתהליכי השליטה על המידע שלהם המתוארים בסעיפים 5.2 וגם 5.3, ואף לתת את הדעת להנחיה הנכללת בסעיפים 6.2 עד 6.7.

טעות נפוצה, המבוצעת בעיקר על ידי ארגוני שירותי בריאות ציבוריים, בהם על פי רוב אין בנמצא דרישה להסמכה או אישור רשמיים, היא לתאר את הציות בהנחיות תקן ISO/IEC 27002 כעניין של אימוץ רשימת תיוג בלבד. על מנת לעמוד בציות במלוא מובן המילה, ארגונים חייבים להיות מסוגלים להדגים את הטמעתו של תהליך ISMS הכולל בקרות נאותות על תהליכי הציות. ציות זה עולה יפה עם הדרישות הרגולטוריות תחתן פועלים רבים מארגוני שירותי בריאות אלה. ראה גם 7.12.

6.2 התחייבות ההנהלה ליישום תקן ISO/IEC 27002

חיוני הוא כי ארגון המעניק שירותי בריאות ייהנה מן התמיכה הברורה של הדרג הניהולי לפני שהוא ינסה להטמיע בקרבו את הציות להנחיותיו של תקן זה. אין ספק כי מעורבותה הפעילה ותמיכתה של ההנהלה הן חיוניות להצלחה. מעורבות זו חייבת לכלול הצהרות בכתב ובעל פה באשר למחויבותו של הדרג הניהולי לחשיבות נושא ביטחון המידע ולהכרה ביתרונות הנגזרים ממנו.

היישום של תהליך הערכת הסיכונים בארגון מביא עמו את הפוטנציאל של גילוי סיכונים חמורים, המחייבים לעיתים עריכת שינויים מהותיים בתהליכים קיימים על מנת שסיכונים אלה ימותנו. נכונותו האישית של הדרג הניהולי להכפיף, הן את עצמו והן את הארגון, לשינויים תהליכיים, ולשמש חלוצים בהטמעתם של השינויים המתחייבים, חייבת להיות גלויה וברורה לעיני כל.

מבלי שיינקטו הצעדים דלעיל, תהיה התחייבותם של גורמים אחרים בארגון לוקה בחסר. חשדות מיותרים יוכלו להיות מועלים על ידי בעלי עניין באשר ל"מטרה האמיתית" של התוכנית (כגון, "האם היא נועדה להגביר את יעילות ביטחון המידע, או אולי להקטין את מספר העובדים הנחוץ בארגון"?).

יתרה מזו, חייב הדרג הניהולי להיות מוכן לקראת האפשרות הסבירה כי העלייה בהוצאות בטווח הקצר הנובעת מן המעבר למשטר החדש תעורר הערות שליליות, בייחוד במגזר שירותי הבריאות. הערות מעין אלה יהיו עלולות להתבסס על תפיסות מעורבות באשר למטרות והתוכניות של הארגון. מסירותו הברורה והחד-משמעית של הדרג הניהולי בארגון לשינויים המתחייבים תהיה עשויה להקטין את היקפן של בעיות אלה.

6.3 ההקמה, תפעול, שמירה ושיפור של מערך ניהול ביטחון המידע

סעיפי המשנה 6.4 עד 6.7 להלן מציעים הנחיה באשר להקמתו, ולתפעולו לאחר מכן, של מערך ניהול ביטחון המידע בסביבת שירותי בריאות. הדבר דורש נקיטת סדרה של צעדים, כמתואר בתרשים 2.

בעלי עניין	1. **תכנון:** קבע את מאפייני מערך ניהול ביטחון המידע (**ISMS**) (ראה 6.4)	2. **עשה:** יישם והפעל את ISMS (ראה 6.5)	**בעלי עניין**
מחזור החיים של מערך ניהול ביטחון המידע **הקמה, יישום, פיקוח ושיפור**			
דרישות וציפיות ביטחון המידע	3. **בדוק:** פקח על ISMS ועדכן אותו (ראה 6.6)	4. **פעל:** שמר ושפר את ISMS (ראה 6.7)	ביטחון מידע מנוהל

תרשים 2 – סקירת תהליך מערך ניהול ביטחון המידע

נספח ב' למסמך זה מציע דוגמאות לצעדים הכרוכים בדרך כלל בכל אחד משלבי מחזור החיים, יחד עם דוגמאות לסוגי המסמכים הקשורים לכל שלב.

6.4 תכנון: הקמתו של מערך ניהול ביטחון המידע

6.4.1 בחירה והגדרה של טווח הציות

6.4.1.1 כללי

באופן תיאורטי, ניתן ליישם את תקן ISO/IEC 27002 בארגונים שלמים. עם זאת, הניסיון שהצטבר מן היישום בבריטניה ובמקומות אחרים הראה כי יחידות גדולות מאוד נאבקות כדי להשלים את העבודה הכרוכה בכך וכדי להשיג את רמת הציות הנדרשת במהלכו של ניסיון אחד.

טווחי הציות הכוללים לא יותר מאשר שניים עד שלושה אתרים, או 50 עובדים בקירוב, או לחילופין עשרה תהליכים, נמצאו כפועלים היטב. מסיבה זו, נהלי טיפול רפואי עיקריים, קליניקות, צוותי ביקורי בית, תחומי מומחיות בבתי חולים וכדומה, מהווים כולם טווחים יעילים ליישום הציות. תהליך הדרגתי והחוזר על עצמו, יהיה, אם כן, באופן אופייני השלב הראשון שאחריו יבוא הכיסוי המלא של ניהול ביטחון המידע, על מלוא יתרונותיו. יש לעשות ניסיון שלא לפגום בסיכויו של מהלך מעין זה על ידי בחירה של טווח ציות רחב יתר על המידה. עם זאת, במקומות בהם מועסקים ספקי צד שלישי של שירותי טכנולוגית מידע, נבחר בעבר "הניהול של אספקת שירותי טכנולוגית המידע" כטווח ראוי ליישום הציות בתקן, עם הצלחה הראויה לציון.

בארגוני שירותי בריאות, בדומה למתרחש בארגונים אחרים, נעה פעילות ביטחון המידע בשנים האחרונות בהצלחה מהיותה עיסוק טכני של "המשרד האחורי" לעבר תפיסת מקום חשוב באחריות התאגידית.

בתחום שירותי הבריאות, התלות ההדדית הניכרת של התפקידים והמשימות הופכת את הגדרת טווח הציות לאתגר של ממש. מסיבה זו, חשוב ביותר כי הדבר ייעשה באופן נכון.

6.4.1.2. הקריטריונים להגדרת טווח הציות

על מנת שיתאפשר איזון נכון בין "יכולת היישום" של הציות לבין היתרון ברמת הארגון, הגדירו ארגונים רבים בשירות הציבורי, ובכללם ארגוני שירותי בריאות, כטווח ראשוני את **"האספקה הבטוחה של שירותי טכנולוגיות מידע"**. למרות היותו קרוב יותר לתשתית מאשר לתהליכים עסקיים, טווח זה מעניק יתרונות ארגוניים מוחשיים, ובנוסף ממלא אחר משימות קריטיות, לרבות הבטחתה של התשתית בכללותה, תוך המרצת הצורך ביישומם של כל סוגי העדכונים הנחוצים לתהליכי הביטחון הארגוניים, שיפור ניהול הזהות, המודעות לביטחון המידע, ושיפור המשכיות הניהול העסקי. על פי רוב יצמחו לארגון יתרונות ברבים מן התחומים דלעיל, החורגים באופן משמעותי מן הטווח הספציפי שנבחר.

חיוני, על כן, כי ייעשה שימוש בקריטריונים להגדרתו של טווח הציות. הקריטריונים הם בדרך כלל "רכים" בטיבם, והם מכסים נושאים כגון:

(א) טווח הנראות המבוקש;

(ב) האיזון בין המעורבות העסקית והטכנית לו שואפים;

(ג) דרגת הרלוונטיות המקומית או המרכזית לה שואפים;

(ד) מידת יכולת או גמישות הניהול שהטווח יביא עמו.

6.4.1.3 ניתוח פערים פוטנציאלי תמציתי תוך כדי הגדרת טווח הציות

לפני שמבוצעת בחירתו הסופית של הטווח, יתכן ויהיה ראוי לנקוט בניתוח פערים, על בסיס מדגמי, על מנת לקבל "תחושה" באשר לכמות העבודה שתהיה כרוכה בכל אחד מן התחומים. האם ייבחר תחום פעילות "קשה" או "קל" הוא בגדר החלטה של הארגון, ואולם באופן הגיוני יצמחו לארגון באופן יחסי יותר יתרונות מטיפול בהיבטים ה"קשים" של הטווח.

6.4.1.4 מעורבות/הכללה מבוקרת של צדדים שלישיים

תחום נוסף בו מבוצעות לעיתים קרובות טעויות הוא פרשנותו של הטווח. הטווח כולל את השירותים הניתנים על ידי צדדים שלישיים ואת אספקתם של תהליכי תמיכה נדרשים, ואולם לא הקביעה כיצד תהליכי תמיכה אלה מסופקים לארגון.

6.4.1.5 הסכמי רמת שירות וחוזים מסייעים בקביעת טווח הציות

הסכמי רמת שירות (SLA) וחוזים יכולים אף הם לסייע בקביעת הטווח, שכן כלים אלה מגדירים באופן יעיל את

גבולות הטווח. גם אם הם אינם עושים זאת במקרים אחדים, סקירתם תוכל להתברר כמועילה בקביעת סדרי העדיפויות הדורשים שיפור.

6.4.1.6 ניסוחו והפצתו של תצהיר הטווח

יש צורך לנסח תצהיר טווח פורמאלי בכתב, במיוחד אם השאיפה היא לקבל אישור על פי תקן ISO/IEC 27001. על התצהיר יהיה להיות מופץ באופן נרחב בארגון, וחיוני הוא כי הוא יגדיר את גבולות פעולות הציות במונחי אנשים, תהליכים, מקומות, פלטפורמות ויישומים.

במקרה של ארגוני שירותי בריאות, חשוב כי תצהיר זה יופץ באופן נרחב, ואף כי הוא ייסקר ויאומץ על ידי גורמי השליטה על המידע, השליטה הקלינית והארגונית הפועלים בקרבם. ואכן, ידוע כי ארגוני שירותי בריאות מסוימים ביקשו לקבל הערות לתצהיר הטווח לציות שלהם מישויות רגולציה קליניות מקצועיות, העשויות להיות מעודכנות באשר למתרחש בקרב ארגונים דומים אחרים השואפים אף הם להטמיע ציות או לזכות באישור ליישומו של התקן.

ראה סעיף 7.3.2.1 להלן באשר לדרישות המינימום בנוגע לתצהירי טווח.

6.4.2 ניתוח פערים

ברגע בו נבחר הטווח, השלב הבא של תהליך התכנון הוא לנקוט בניתוח פערים הכולל דרגה גבוהה של הערכת הציות. הנהלים המיטביים הצביעו על כך, כי ניתוח זה חייב להתמקד בהיבטי האחריות הארגונית, וביישום והתיעוד של נהלי הביטחון והראיות בהם נעשה שימוש כדי לתמוך בניתוח. הדבר עולה באופן ברור

בקנה אחד עם נהלי עבודה בתחומי הבריאות בהם מיומנויות, רישומים ונהלים נאותים הם כולם בעלי חשיבות מכרעת.

כשל נפוץ של ניתוחים מעין אלה מתבטא בכך כי הם אינם משיגים נקודות ראות השוואתיות לצד אימות. האדם המבצע את הניתוח מסתכן בקבלת הערות, העלולות לבטא את שאיפותיהם של אנשים יחידים מסוימים בלבד, במקום שיבטאו ראייה עקבית של נהלי העבודה השוטפים בארגון. זמן מספיק נדרש על מנת לראיין אנשי מקצוע בתחומי הבריאות ומנהלים כדי לאמץ עמדה רחבה וכוללת בנושא זה.

מטרתו של ניתוח הפערים היא להעניק הנחיה ראשונית באשר לשיפורים הנדרשים, בכפוף ללימוד מפורט של הערכת הסיכונים (ראה 6.4.5.1) ושל הטיפול בסיכון (ראה 6.4.5.2). כמו כן, ניתוח הפערים יוכל להציע גם סדר עדיפויות ראשוני להטמעתם של שיפורים בארגון.

6.4.3 הקמתו או חיזוקו של פורום ביטחון מידע בריאות

חובה להקים פורום ביטחון מידע בריאות מתאים בלב תהליך מערך ניהול ביטחון המידע (ISMS), שתפקידו יהיה לפקח על ביטחון המידע ולכוונו. מה יש להבין כ"מתאים" בהקשר זה, שונה מארגון לארגון, ועשוי להשתנות גם בקרב תחומי שירותי הבריאות השונים.

הקמתו של הפורום וגיבושו יהיו מאתגרים, שכן יהיה צורך לתת מענה לדעות הרבות של בעלי העניין מחד, ושל החובות הרגולטוריות מאידך. בעוד שאת סמכויות הפורום לא ניתן להאציל או לפזר מבלי שהוא יאבד מיעילותו, אין להתייחס להקמתו של פורום זה כאל הקמתה של "עוד וועדה." על פי רוב עדיף להרחיב את סמכויותיה של וועדה קיימת, לדוגמה של וועדה המטפלת בסיכונים או בשליטה על המידע.

החברות בפורום תהיה חייבת לכלול את מלוא משימות טווח ביטחון המידע והשליטה עליו, כמו גם נציגים של קהילות המשתמשים השונות ונציגים של תפקיד המפתח בתמיכה בארגון. נציגי ביקורת הפנים ומשאבי האנוש בארגון יהיו בדרך כלל מיוצגים אף הם.

על קצין ביטחון המידע של הארגון (בין אם ווירטואלי ובין אם ממשי) יהיה לדווח, בין שאר חובותיו, לפורום ולספק לו שירותי מזכירות, כמו גם לשאת באחריות לתאום והפרסום של ההערות המתקבלות מחברי הפורום ולפרסומן.

כפי שמצוין בסעיפים 5.2 וגם 5.3 לעיל, תפקידו המרכזי של ביטחון המידע בנושא הרחב של השליטה על המידע הופך את הצבתו של פורום ביטחון המידע בתוך מבנה השליטה על המידע בארגון למהלך הגיוני ביותר, אך זאת, רק בכפוף לכך כי פעילותו של הפורום אכן תהיה מוטמעת בתוך מבנה השליטה הקלינית. השליטה הקלינית מטפלת בסוגיות של בטיחות המטופל, ואלה קרובות במקרים רבים לסוגיות ביטחון המידע החייבות בטיפול על ידי גורמי השליטה על המידע בארגון.

אימוצה של גישת שליטה על המידע מדגישה את טיבו הקריטי של ביטחון המידע ומאפשרת גם תהליך שלם, הכולל תשומות של ניתוח סיכונים, והמזין באופן ישיר את השליטה הקלינית. הסרתה של מנטאליות ה"סילו" המפרידה בין ביטחון מידע, הגנה על נתונים, חופש המידע וכדומה, יכולה רק לסייע להסיר כפילויות בעלויות ולהעניק ביטחון מוגבר בשלמותם של התהליכים המתקיימים בארגון.

6.4.4 הערכת הסיכונים הכרוכים במידע הבריאות

6.4.4.1 כללי

הערכת סיכונים הוא המנגנון לפיו יש לזהות את מסגרת הבקרות העומדת ביסוד יעדי הבקרה של תקן ISO/IEC 27002. תהליך זה מתועד היטב בנוהל ISO/IEC/TR 13335-3.

בזירת שירותי הבריאות קיימים מספר שיקולים ייחודיים הראויים לדיון.

6.4.4.2 תפקידה של הערכת הסיכונים של ביטחון המידע במגזר שירותי הבריאות

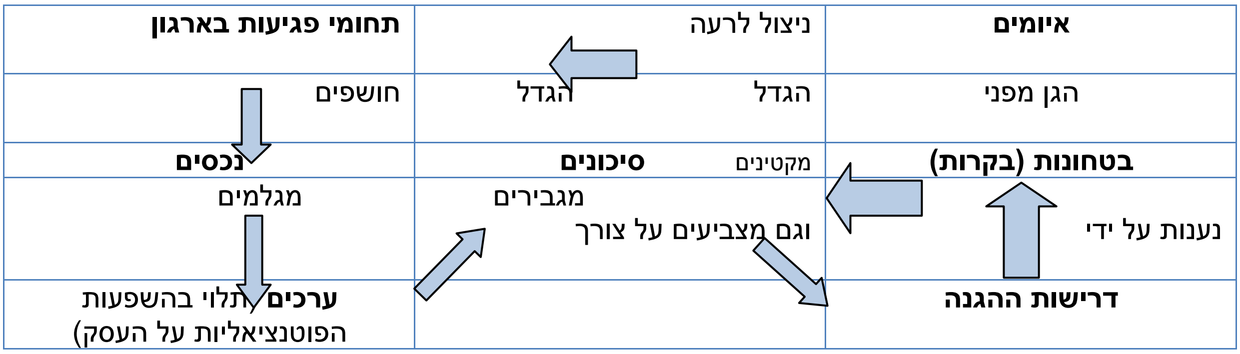
מגזר שירותי הבריאות טומן בחובו באופן ברור סיכונים גבוהים, במיוחד בתחומים כמו מעבדות, מחלקות רפואה דחופה וחדרי ניתוח. לכן, יש מקום להטיל ספק בממצא המעלה סיכון נמוך בפעילות מידע בריאות בתחומים שנמנו לעיל, למרות שיש להיזהר מן המלכודת, לפיה מניחים כי כל פעילות מידע בריאות קשורה ישירות לאספקת שירות בריאות, הנחה שתהיה שגויה באותה המידה.

מן הראוי כי הערכות הסיכונים של ביטחון המידע בתחום שירותי הבריאות ישקלו הן גורמים איכותיים והן גורמים כמותיים. אין להפוך את ההפסדים הכספיים לשיקול העיקרי, ואולם ניתן לקחת אותם בחשבון במקומות בהם קיימות ראיות לסכומי כסף גבוהים המשולמים בעקבות מעשים של הזנחה. בהקשר הנוכחי

יהיה צורך בהגדרה זהירה של הנחיות ההערכה הרלוונטיות לתחום שירותי הבריאות, לדוגמה של הנחיות המכירות בחשיבותה של בטיחות המטופל, באספקה הבלתי מופרעת של שירותי חירום, בהסמכה המקצועית וברגולציה הקלינית.

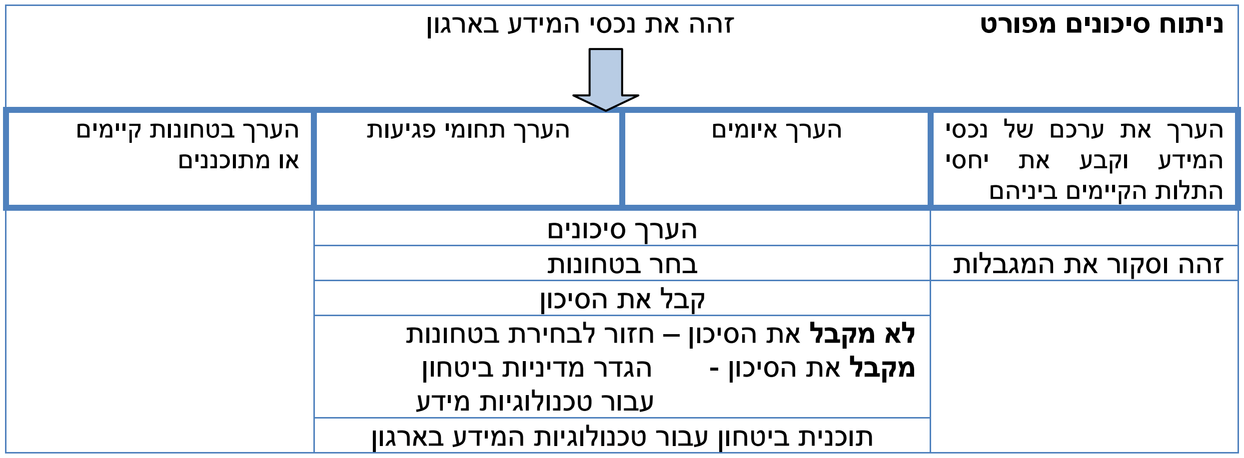
6.4.4.3 מאפייני הערכת הסיכונים עם דוגמאות מתחום שירותי הבריאות והתייחסות לתקן ISO/IEC 13335

סיכון מורכב מיחס חופשי, או אקראי, הקיים בין מספר מקורות סיכון. תרשים 3 להלן מצביע על היחס הקיים בין סיכונים לבין מקורות סיכון בתקן ISO/IEC 13335, תוך הבהרה כי ערך סיכון נקבע על בסיס ערכי הנכסים, האיומים וההיפגעות הסובבים אותו.



תרשים 3 – היחס בין סיכונים ומקורות סיכון במודל סיכון פשוט

הערכת הסיכונים בביטחון המידע, ושלבי ניהול הסיכונים בהמשך התהליך האופייניים מוצגים בתרשים 4 להלן:



תמצית מתוך מסמך ISO/IEC TR 13335-3

תרשים 4 – ניהול סיכונים העושה שימוש בניתוח סיכונים מפורט

הן תקן ISO/IEC 27002 והן ISO/IEC TR 13335-3 מגדירים את מרכיבי ניתוח וניהול הסיכונים כדלקמן:

(א) הזיהוי של נכסים עסקיים, איומים ותחומי חשיפה להיפגעות;

(ב) הערכת ההשלכה העסקית;

(ג) הערכת הסבירות והחשיפה להיפגעות;

(ד) זיהוין של בקרות ביטחון מומלצות;

(ה) ההשוואה על בקרות קיימות, תוך זיהוי תחומים בהם קיים עדיין סיכון;

(ו) חלופות לטיפול בסיכונים, לרבות ניהול ישיר, קבלה ומניעה של סיכונים, ניהול העברה, וכדומה;

(ז) תוכניות הערכת סיכונים ותוכניות טיפול בסיכונים;

(ח) מיפוי החלטות המתקבלות נגד רשימת הבקרות המפורטת בתקן ISO/IEC 27002.

כל המרכיבים דלעיל הם ישימים בתחומי שירותי הבריאות, למרות ש"הערכת ההשלכה העסקית" חייבת לכלול באופן ברור את מקצועות הבריאות הרבים והמגוונים. הערכות סיכוני ביטחון מידע הננקטות על ידי ארגוני שירותי בריאות יוכלו לראות יתרונות מאימוצו של מודל זה.

בנוסף לרשימה דלעיל, חשוב לקבוע גם, או לחילופין להבטיח כי מתקיימת, הבנה באשר לתלותם של תהליכים עסקיים בשירותי טכנולוגיות המידע, בחומרה, תוכנה, המדיה והמיקומים. מבלי שהבנה זו תושג בעקבות ניתוח ההשלכה העסקית, יהיה זה כמעט בלתי אפשרי להבין את תרחישי הכישלון שיהיו הרלוונטיים. הבנתם של יחסי התלות האלה היא חיונית לאור השלכתם המהותית על ארגוני שירותי הבריאות.

6.4.4.4 מיומנויות דרושות ותרומות לתהליך

ניתוח הסיכונים אינו יכול להתבצע, על פי רוב, על ידי אדם יחיד, למעט בהיקף בו אותו אדם רשאי להמציא את השקפתו האישית. תחת זאת, מדובר בפעילות השואפת להשיג הסכמה רחבה בארגון, כך שכלל ההשקפות אכן נאספות ומכובדות. המציאות היא כי לאנשים שונים יש דעות והשקפות שונות, כמו גם דרגות סובלנות שונות, בכל הנוגע לסיכונים. אתגרים, גם היפותטיים ובלתי סבירים, יידרשו ככל הנראה בארגון על מנת לגבש את "תרחישים החמורים ביותר" למקרים של השלכות, סבירותם של איומים והחשיפות להיפגעות.

באופן טבעי, אירועים שקרו בפועל בעבר נתפסים כמציאותיים, ואולם הם אינם בהכרח מהווים את התרחיש הגרוע ביותר. לעומתם, תרחישים המאופיינים בתצהירי "אם" רבים, נוטים שלא להיות מציאותיים. אנשי מקצוע בתחום שירותי הבריאות יראו בדרך כלל תועלת בהכללתם של אנשי מקצוע מתחומי טכנולוגיות המידע אשר יהיו מסוגלים לזהות כשלים ותרחישים הדורשים הערכה.

הערכת סיכונים יעילה בתחום ביטחון המידע דורשת כי יהיו בנמצא המיומנויות והידע שלהלן:

(א) ידע בתהליכים קליניים ובתהליכי סיעוד, לרבות בפרוטוקולים של טיפול רפואי ומהלכיו;

(ב) הכרת הפורמטים של המידע הקליני ושל היכולות הקיימות לניצולם לרעה;

(ג) הכרת גורמים סביבתיים חיצוניים העלולים להחמיר, או לחילופין למתן, את כל אחד מרכיבי הסיכון שתוארו לעיל;

(ד) מידע בדבר מאפייני משכור טכנולוגיות המידע והמכשור הרפואי, כמו גם הכרת מאפייני ביצוע וכשל;

(ה) הכרת אירועים שהתרחשו בפועל, כמו גם הכרה של תרחישי השלכה שונים שאירעו בפועל.

(ו) הכרה של ארכיטקטורות המערכות לפרטיהן;

(ז) היכרות עם תוכניות ניהול שינוי שיעלה בידן לשנות רכיבים אחדים, או את כלל הרכיבים, של הסיכונים.

6.4.4.5 תפוקות נדרשות

ISO/IEC TR 13335-3 מגדיר את התפוקות האופייניות הבאות:

(א) דו"ח הערכת סיכונים;

(ב) תוכנית טיפול בסיכונים;

בנוסף, יהיה על ארגוני שירותי בריאות לייצר גם:

(ג) מודלים לנכסים/יחסי תלות (לתמיכה בהערכת הסיכונים);

(ד) דוחות התקדמות באשר לבקרות;

(ה) דוחות סיכום בדבר הטיפול בסיכונים (כדי לתמוך בניתוח הפערים ובתצהיר הישימות).

מאחר ומגזר שירותי הבריאות הוא מגזר חשוב המתאפיין בחובות ציות משמעותיות, (הן משפטיות/חוקיות והן מקצועיות), תפוקה המאגדת בתוכה הערכות של סיכונים הקשורים אלה באלה, הערוכה על ידי דיסציפלינות שונות או קבוצות תפעוליות שונות, תוכל להיחשב ככלי עזר מועיל לשליטה על המידע, כמו גם להבטחת שלמותן של הערכות סיכונים פרטניות.

6.4.5 ניהול סיכונים

6.4.5.1 הערכת סיכונים

הערכת הסיכונים אמורה להוות אמצעי לקראת השגתה של מטרה. אסור לה להוות יעד כשלעצמה, אך זה מה שאכן מתרחש מפעם בפעם. הדבר נכון במיוחד באשר לסביבות המתאפיינות במשאבים מצומצמים, כגון אלה בהן אנו נתקלים לעיתים קרובות בארגוני שירותי בריאות. ניהול הסיכונים נותן מענה לתהליך ההערכה על ידי זיהוין של אותן הבקרות שיש לחזק, של אלה העושות כבר את מלאכתן באופן יעיל, ושל הבקרות הנוספות להם זקוק הארגון כדי להפחית את רמת הסיכון הנותרת לכדי רמה שהיא מקובלת.

הקשר ההדדי וההולך וגובר בין מערכות מידע בריאות הופך את ניהול הסיכונים בתחום שירותי הבריאות למאתגר במיוחד, שכן רק ארגונים מעטים יכולים לפעול כאילו מערכותיהם הן איים מבודדים של מידע. הערכת הסיכונים במגזר הבריאות מרבה להעלות שאלות באשר לשמירתו של המידע, הבעלות עליו, והאחריות החלה לגביו. ניהול סיכונים יעיל חייב להבטיח את התאמתה של האחריות על ביטחון המידע עם הסמכות לקבל החלטות בתחום ניהול הסיכונים.

6.4.5.2 טיפול בסיכונים

על מנת להבחין באופן ברור בין תהליך ניהול הסיכונים בכללותו ובין צעדי הניהול של סיכונים מזוהים, חידש התקן האוסטרלי והניו-זילנדי AS/NZ 4360 את המונח "טיפול בסיכון." מושג זה אומץ עקב כך על ידי תקן ISO/IEC 27001.

המונח "טיפול בסיכון" בא להדגיש את הפעילות המתבטאת בהקטנת הסיכון לכדי ממדים מתקבלים על הדעת (ההכרה בכך כי משאבים מספיקים לעולם לא יהיו זמינים כדי לנסות אפילו הימנעות כוללת מן הסיכון). הטיפול בסיכון הולם במיוחד ארגוני שירותי בריאות, שכן הוא מביא עמו את מונחי ה"טפל, העבר או סבול" בקשר עם הסיכונים המזוהים.

ההגדרה של מה מתקבל על הדעת, ויכול להישאר כזה, היא ייחודית לארגון ולצוות עובדיו. עליה לשקף את נכונותו של הארגון לשאת בסיכונים, ולכן יש לעשות בה שימוש כדי להבטיח כי הוצאת כספים על שיפור ביטחון המידע מוצדקת, ומציגה לעיני הכלל שימוש מושכל במשאבים הכספיים המוגבלים ממילא.

6.5.4.3 קריטריונים לקבלת סיכונים

מומלץ כי ארגוני שירותי בריאות יגדירו ויתעדו את הקריטריונים שלהם לקבלתם של סיכונים. הגורמים שיש לקחתם בחשבון הם רבים ומגוונים, ואולם יש לשקול את הכללתם של אלה המפורטים להלן:

(א) תקני מגזר או תעשיית הבריאות, או תקנים ארגוניים;

(ב) עדיפויות קליניות או אחרות;

(ג) התאמה תרבותית;

(ד) תגובותיהם של מטופלים;

(ה) עקביות והתאמה עם אסטרטגיות תאגידיות לקבלת סיכונים בתחומי טכנולוגיות המידע, התחום הקליני והארגוני;

(ו) עלות;

(ז) יעילות;

(ח) סוג ההגנה;

(ט) מספר האיומים המכוסים;

(י) דרגת הסיכון בה הבקרות הופכות למוצדקות;

(יא) דרגת הסיכונים שהובילה להעברת ההמלצה;

(יב) החלופות שקיימות זה מכבר;

(יג) יתרונות נגזרים נוספים.

כאשר הם נלקחים יחד, הגורמים דלעיל יפיקו הערכת עלות-תועלת שתהיה מסוגלת להוות בסיס להמצאת בקשה להקצאת המשאבים למקרה העסקי הנדון.

החלטה המתקבלת, בדרך כלל על ידי פורום ביטחון המידע, שלא ליישם בקרה מסוימת היא לגיטימית לחלוטין, ואולם יש לתעד אותה באופן פורמאלי לצורך בחינתה התקופתית ולהערכה מחדש בבוא העת.

על ארגוני שירותי בריאות יהיה לתעד את הסיכונים המקובלים עליהם.

6.4.5.4 תוכניות להתמודדות עם תחומים המאופיינים בסיכונים חריגים

התהליך שתואר לעיל יהיה חייב לכלול הסכם באשר למועד בו יטופל הסיכון המזוהה על ידי יישומה של הבקרה (למרות שגם "לעולם לא" יוכל להיות מקובל במקרה הזה).

תוכנית שיפור הביטחון של הארגון תהיה חייבת לשקף את נקיטתם של צעדי יישום עתידיים.

6.4.6 תכנון שיפור הביטחון

הסמכות לעיצובה של תוכנית לשיפור הביטחון בארגון צריכה להילקח על ידי נושא המשרה האחראי על ביטחון המידע, האחראי על ההגנה על המידע או מנהל הסיכונים, בשם הפורום לביטחון המידע, או לחילופין על ידי נושא משרה דומה בארגון.

כאשר הם מנוסחים לעיתים קרובות כתרשים מסוג גאנט, יש להעביר את התוכניות לעיונם של עובדים בתחומים הקליניים ובתחומים אחרים, שכן הן בדרך אינן מהוות מסמך סודי. ואכן, מסמכים אלה יכולים להתגלות לעיתים קרובות כמועילים בהצבעה על התקדמות שהושגה לצד שיפור בתהליכים.

תוכניות אלה ישיגו מידה מרבית של יעילות ושל היעדר הפרעה לפעילותו השוטפת של הארגון אם יעלה בידן לשלב בין שיפורי ביטחון מידע לבין שינויים מתוכננים בהענקתן של טכנולוגיות המידע ושירותי הבריאות בארגון. כמו כן, חלה חובה כי תוכניות אלה יזהו תקופות של פעילות שירותי בריאות חריגה, כגון קליטתן של קבוצות חדשות של מתמחים או מתלמדים.

6.4.7 תצהיר הישימות

ניתן לראות בתצהיר הישימות תמצית מנהלים על אודות מצבו של ביטחון המידע בארגון, על פרשנותו לצרכי הביטחון, וגם בדבר האסטרטגיה שלו ליישומם של פתרונות ביטחון. כאשר הוא מנוסח ומעודכן על ידי האחראי על ביטחון המידע בארגון בשם פורום ניהול ביטחון המידע, יש להמציא את המסמך לנושאי התפקידים בתחומי השליטה הקלינית והתאגידים כדי שהוא יהפוך למרכיב קבוע של סדרת התיעוד השליטה בארגון. פורמט המסמך יהיה בדרך כלל מועיל גם ככלי להערכה או ראייה התומך בביקורת חיצונית, בבקרת הביטחון הקליני ובביקורות רגולאטוריות מסוגים אחרים.

6.4.8 סדרת מסמכי מערך ניהול ביטחון המידע

מודל ISMS המפורט בסעיף 6.1 לעיל מפרט את התיעוד הנדרש (ראה תרשים 1). המסמכים החיוניים הם כדלקמן:

(א) מדיניות ביטחון המידע של הארגון;

(ב) תצהיר טווח יישום;

(ג) תצהיר ישימות;

(ד) מלאי נכסי מידע ומערכת החייב בהגנה;

(ה) תוכניות ודוחות להערכת סיכונים;

(ו) נהלים ותקנים מוסכמים;

(ז) הסכמים חוזיים (לרבות הסכמי רמת שירות והסכמי שימושים מקובלים).

בנוסף, ניתן להקל על עמידתו של פורום ניהול ביטחון המידע ביעדים הקליניים ובסדרי העדיפויות, אם סדרי עדיפויות אלה מתועדים על ידי נושאי המשרות בתחום השליטה הקלינית והתאגידים, כדי שיהפכו לאחר מכן לחלק קבוע של התיעוד של הפורום. מסמך זה מעניק אז גיבוי לטובת החלטות לקבלת סיכונים המתקבלות על ידי פורום ניהול ביטחון המידע.

נספח ב' כולל את סדרת מסמכי מערך ניהול ביטחון המידע, ומסמכים הקשורים לצעדים השונים הדרושים להקמתו או הרחבת פעילותו של המערך דלעיל.

6.4.9 פוטנציאל לקידום על ידי שימוש בכלים

תהליך הציות להנחיותיו של תקן ISO/IEC 27002 כולל סדרה של צעדים המייצרים כמות משמעותית של מידע ותיעוד. עם זאת, ארגוני שירותי הבריאות פועלים בסביבה דינאמית בה הסיכונים משתנים ובקרות חדשות מיושמות מעת לעת. שלמותו הכוללת של מידע זה ושל תיעודו חייבת, אם כן, להישמר בכל עת.

יתרה מזו, אופיים המדורג, המורכב, המתגבר, מתרחב והחוזר על עצמו של התהליכים הנוגעים בדבר, פירושם הוא כי המידע נתון שוב ושוב למניפולציה ולשימוש חוזר בתהליכים מרובים, כאשר כתוצאה מכך תהליך מאוחר דורש לא אחת שינויים או תיקונים החייבים להתבצע במסגרתו של תהליך מוקדם יותר. לבסוף, החלטות יתקבלו בדרך כלל לאור סדרת גורמים שידרשו פעילות הצלבה בסדרי גודל ניכרים.

מומלץ כי ארגוני שירותי בריאות ישקלו את אימוצם של כלים שיסייעו בידם לציית להנחיות של תקן ISO/IEC 27002. נספח ג' כולל דיון אינפורמטיבי על אודות היתרונות הפוטנציאליים של כלים אלה, לרבות המאפיינים הנדרשים מהם.

6.5 עשייה: יישום ותפעול מערך ניהול ביטחון המידע

יישומו של מערך ניהול ביטחון המידע כרוך בנקיטתם של מספר צעדים, כמפורט להלן:

(א) **ניסוח תוכנית טיפול בסיכונים**: לאחר שהסיכונים זוהו באמצעות הערכת הסיכונים, הם חייבים להיבחן ולהתקבל על ידי דרג הניהול הבכיר, או ממותנים כאשר הסיכון נחשב לבלתי מקובל על הארגון. תוכנית טיפול בסיכון מבהירה את הפעילויות שבהן יש לנקוט על מנת להקטין את הסיכונים שהוגדרו כבלתי מקובלים. היא כוללת תוכנית ליישומן של בקרות הביטחון שנבחרו (על בסיס תוצאות הערכת הסיכונים) כמתאימות כדי להקטין או למתן סיכונים בלתי מקובלים אלה. פורום ניהול ביטחון המידע בארגון הוא האחראי לוודא כי התוכנית שאומצה אכן מוצאת אל הפועל הלכה למעשה. באופן האידיאלי, תכלול תוכנית הטיפול בסיכונים לוחות זמנים, סדרי עדיפויות ותוכניות עבודה מפורטות, והיא גם תקצה תחומי אחריות ליישומן של בקרות הביטחון. בתחום שירותי הבריאות יכול האישור של תוכניות מעין אלה לכלול הן תפקידי שליטה על מידע והן שליטה קלינית.

(ב) **הקצאת משאבים**: משימה חיונית של הדרג הניהולי היא הקצאתם של המשאבים הדרושים (כוח אדם, מערכות ומימון) הנחוצים להבטחת הביטחון של נכסי ביטחון המידע.

(ג) **הבחירה והיישום של בקרות ביטחון:** סעיף 7 סוקר את כל אחד מאחד עשר סעיפי הביטחון של תקן ISO/IEC 27002, ומעניק ייעוץ והנחיה באשר לבחירה המתאימה של בקרות הביטחון בסביבת שירותי הבריאות.

(ד) **הדרכה והכשרה**: סעיף המשנה 7.5.2.2 דן בדרישות להדרכתו והכשרתו של כלל צוות העובדים, הקבלנים, אנשי המקצוע בתחומי הבריאות, ושל אחרים שהם בעלי גישה למערכות מידע בריאות ולמידע בריאות אישי.

(ה) **ניהול התפעול**: התפעול השוטף והמוכשר של מערך ניהול ביטחון המידע הוא חיוני אם הארגון שואף לשמר את סודיותו, שלמותו וזמינותו של מידע הבריאות ושל מערכות המידע בכללותן. סעיף המשנה 7.7 דן בהיבטי שירותי הבריאות של ניהול התפעול.

(ו) ניהול משאבים: ביטחון מידע יעיל עשוי להיות יקר, וכוח אדם מוכשר עלול להיות נדיר. להבטחת הניהול היעיל השוטף נדרשים קביעת סדרי עדיפויות יעילה ונכונה על ידי פורום ניהול ביטחון המידע, בשילוב עם ניהולם הזהיר של אנשים ומשאבים.

(ז) ניהול אירועי ביטחון: כדי להקטין למינימום את ההשלכות של תקרית ביטחון חשוב כי התקרית תאותר באופן הנכון וכי יינקטו צעדי תיקון. יש צורך להכין, ולעדכן באופן שוטף, מסמכי הדרכה להתמודדות עם תקריות ביטחון. חשוב במיוחד להגדיר תחומי אחריות וצעדים מעשיים ליישום בשלב התגובה הראשוני, שכן אירועים עלולים להתפתח במהירות, כאשר אופיין הקריטי של מערכות המידע בתחום שירותי הבריאות אינו מותיר זמן להרהורים בעוד אירוע כזה או אחר מתפשט בארגון. נהלי דיווח ברורים למקרה של תקרית ביטחון חיוניים אף הם כך שניתן יהיה לשמר את אמונם של בעלי העניין, ועל מנת שידווח על כל תקרית משמעותית, ועל השלכותיה, לנושאים באחריות לשליטה התאגידית והקלינית בארגון. סעיף המשנה 7.10 כולל דיון מפורט בנושא ניהול תקריות ביטחון.

6.6 בדיקה: פיקוח על מערך ניהול ביטחון המידע וסקירתו

6.6.1 הצורך בביטחון שוטף

הארגון, מערך ניהול ביטחון המידע, ובתוכו הפורום לניהול ביטחון המידע יזדקקו לביטחון באשר למידת יעילותם הן באשר לשמירה על רמת הביטחון הנוכחית הקבועה בארגון, והן באשר לשיפורה המתמשך בהתאם לאסטרטגית ביטחון המידע המותאמת ליעדיו של הארגון.

קיים מגוון אפשרויות להשגתה של מידת הביטחון דלעיל, וניתן לעשות בהן שימוש משולב. החלופות היקרות פחות יציעו באופן טבעי דרגה פחותה של ביטחון, תוך שהן ישקפו את המידה המוגבלת של קפדנות ועצמאות שהן מציעות. חשוב כי ארגוני שירותי בריאות ינסחו תוכניות ביקורת על מידת הציות, אשר יעשו שימוש משולב בין טכנולוגיות לבין גישות.

6.6.2 הערכת הציות

6.6.2.1 הערכה עצמית

ברמה הבסיסית ביותר, ובמיוחד במקומות בהם יישומו של תקן ISO/IEC 27001 נועד למטרות פנים-ארגוניות בלבד, הערכה הננקטת על ידי צוות מצומצם הפעיל בתחום אחר של הארגון תוכל להעניק אינדיקציה מסוימת באשר ליעילותו של מערך ניהול ביטחון המידע. עם זאת, גישה זו יכולה לסבול לא אחת מנאמנויות של קבוצות עמיתים או מפאת חובות אישיות או ארגוניות הדדיות שונות.

6.6.2.2 סקירת עמיתים

חלופה דומה מאוד היא הארגון של סקירה על ידי עמיתים, בה הנאמנויות הארגוניות השונות של הסוקרים יוכלו להוביל להגדלת מידת האובייקטיביות והביטחון של הסקירה המבוקשת.

6.6.2.3 תהליך ביקורת עצמאית

ביקורות עצמאיות יכולות להיות מבוצעות על ידי גורמים שונים, כגון חברות ביקורת וייעוץ ארגוני, או על ידי מבקרי הפנים של הארגון עצמו, בעלות קטנה יותר. סביר יהיה להניח כי הדו"ח שיופק יהיה אמין ובאיכות גבוהה יותר, וכי הוא ישקף בדרך כלל דרגת מומחיות גבוהה יותר. ביקורות מעין אלה מביאות עמן גם מידה של "מידוד," שכן הצוות המעורב בהן על פי רוב ביצע כבר בעבר ביקורות עצמאיות אחרות היכולות לשמש לו כלי להשוואה.

6.6.2.4 ביקורת אישור לתקן ISO/IEC 27001

ביקורת אישור כוללות באופן אופייני ישיבת טווח, מסמך סקירה ולאחריהם את ביקורת הציות עצמה.

מומלץ כי ארגוני שירותי בריאות יערבו את המבקרים שלהן החל מן הרגע בו הם החליטו כי הם מבקשים לקבל את האישור, זאת על בסיס ניסיון שנצבר בקרב ארגונים מורשים אחרים. במקרה זה הופך המבקר יותר לשותף בביצוע, והציות יכול היות מושג בהדרגה, דהיינו על ידי הסכמה התחלתית באשר לכך כי תצהיר הטווח הנדון בסעיף 6.4.1 מוגדר נכונה ובאופן מעשי. עם זאת, כדאי לשקול גם את יישומה של סקירת עמיתים או של ביקורת עצמאית אחרת בשלב ביניים כדי להגביל עוד יותר כל פוטנציאל לכישלון.

אי הבנה נפוצה מתבטאת בכך כי האישור ניתן רק כאשר ביטחון המידע שנצפה הוא "מושלם." הדרישות הן בסך הכל כי הארגון יקיים מערך ניהול ביטחון מידע הפעיל זה מכבר, הבנה ברורה של הסיכונים והחשיפות, ותוכנית הנהלה שנועדה לצמצם חשיפות אלה לכדי רמה המתקבלת על הדעת. ואכן, תהליך הביקורת יוכל לזהות מספר מוגבל של כשלים אשר, בכפוף למהותם, לא יהוו מכשול בפני הענקת אישור העמידה בתקן.

קיימת גם תפיסה שגויה באשר לכך כי תהליך האישור צורך זמן. עם זאת, הניסיון הראה כי ביקורות אישור עמידה בתקן בקרב ארגוני שירותי בריאות לוקחים אך במקרים נדירים יותר מחמישה או שישה ימי עבודה של איש הביקורת.

הביקורת העצמאית החשובה היא זו המבוצעת על פי ההנחיות של תקן ISO 27001, כפי שהיא מבוצעת על ידי גוף מקצועי, מוסמך ועצמאי, כפי שהדבר נקבע זה מכבר במדינות רבות. ביקורת זו תהיה היסודית ביותר מבין אלה שנמנו לעיל, שכן היא תבוצע על ידי מבקר מוסמך, אשר יהיה חייב להכיר גם את תחומי טכנולוגיות המידע וביטחון המידע. לכן, מידת הקפדנות ומידוד העבודה שניתן לצפות מביקורת מעין זו היא גבוהה. על אף כל זאת, הניסיון הצביע על כך כי עלותה של ביקורת מעין זו היא עדיין בגדר המתקבל על הדעת.

למשתמשים בתקן הבינלאומי הבוחרים לנקוט במהלך זה, מומלץ מאוד לערב את הישות המבקרת כבר בתחילת התוכנית שלהם, שכן תמיכתם של אנשי הביקורת מושגת בהדרגה, עובדה התורמת להגברת הסיכוי לעמידה ביעד הסופי, כאשר לא צפויות "הפתעות" בשלב הביקורת הסופי.

6.7 פעולה: שמירה על מערך ניהול ביטחון המידע ושיפורו

תוצאותיה של פעילות הפיקוח המתוארת בסעיף 6.6 לעיל חייבות להיות מוחזרות לפורום לניהול ביטחון המידע הנושא באחריות להבטיח כי הליקויים מתוקנים וכיח מערך ניהול ביטחון המידע נותר יעיל בתפקודו.

תצהיר הישימות המתואר בסעיף משנה 6.4.7 יכול להוות כלי מועיל לעדכונם השוטף של הנושאים באחריות לשליטה התאגידית והקלינית באשר למצבו השוטף של מערך ניהול ביטחון המידע. בנוסף, הפורמט הטיפוסי של תצהיר זה מתאים ככלי הערכה או ראייה לתמיכה בביקורת חיצונית, בביטחון הקליני ובביקורות רגולאטוריות אחרות.

תוכנית שיפור הביטחון המתוארת בסעיף משנה 6.4.6 מהווה גם היא כלי חשוב להצגת התקדמות ושיפור תהליכי בארגון.

7 השלכות תקן ISO/IEC 27002 על שירותי הבריאות

7.1 כללי

סעיף זה כולל ייעוץ ספציפי באשר לאחד עשר סעיפי בקרת הביטחון ושלושים ותשע קטגוריות הביטחון העיקריות המתוארות בתקן ISO/IEC 27002.

הגישה הכללית הננקטת על ידי ISO/IEC 27002 היא עידודו של כל ארגון לשקול ולפרש את אותו המסמך בהקשר שלו עצמו ועל פי הדרישות העסקיות והחוקיות הרלוונטיות בעבורו. עם זאת, הניסיון שנצבר במספר מדינות כגון אוסטרליה, קנדה, צרפת, הולנד, ניו זילנד, דרום אפריקה ובריטניה הראה כי קיים צורך בקיום מספר סעיפי ביקורת וקטגוריות ביקורת בכל מקום בו עולה הצורך להבטיח את מידע בריאות אישי. על בסיס ניסיון זה, התקן מציין דרישות מינימום כאשר הדבר מתבקש, ובנוסף, במקרים אחדים, מפורטות הנחיות נורמטיביות המתארות את היישום הנכון של בקרות ביטחון מסוימות הנכללות בתקן הבינלאומי ISO/IEC 27002 ואשר נועדו להגן על מידע הבריאות. דרישות מינימום אלה הן כה חיוניות להגנה על מידע הבריאות האישי, עד כי לא ניתן לומר על ארגון בריאות כלשהו שאינו עומד בהן, כי הוא עומד בהוראותיו של תקן בינלאומי זה.

בכל סעיף משנה המצוין בהמשך מהווה ההנחיה המפורטת בו השלמה, אך לא תחליף, להנחיה הכלולה בתקן ISO/IEC 27002.

7.2 מדיניות ביטחון המידע

7.1 מסמך מדיניות ביטחון המידע

<u>בקרה</u>

ארגונים המעבדים מידע בריאות, לרבות מידע בריאות אישי יהיו **חייבים** להחזיק מדיניות ביטחון מידע בכתב המאושרת על ידי ההנהלה, המפורסמת ולאחר מכן מדווחת לכלל עובדי הארגון ולגורמי החוץ הרלוונטיים.

<u>הנחיית יישום</u>

בנוסף לעמידה בהנחיות המפורטות בתקן ISO/IEC 27002 באשר למה חייב להיכלל במדיניות ביטחון המידע, תהיה מדיניות זו **חייבת** לכלול תצהירים בנושאים שלהלן:

(א) הצורך ביישום ביטחון מידע בריאות;

(ב) יעדיה של מדיניות מידע בריאות;

(ג) טווח הציות, כמתואר בסעיף המשנה 6.4.1.6;

(ד) דרישות חקיקה, רגולאטוריות ודרישות חוזיות, לרבות אלה הדרושות להגנה על מידע הבריאות האישי, כמו גם פירוט האחריות בתחומים החוקיים והאתיים של אנשי המקצוע בתחום הבריאות בכל הנוגע להגנה על מידע זה.

(ה) הסדרים באשר לדיווח על תקריות ביטחון מידע, לרבות קיומו של ערוץ להעלאת דאגות באשר לשמירה על סודיות, ללא חשש מפני הטלת אשמה או נקיטה בענישה.

באופן מיטבי, העדכון של תוכן המדיניות יתבסס על הממצאים של הערכת הסיכונים בהם נקט הארגון, זאת למרות שהמדיניות נדרשת לקבוע כיוון פעולה כללי בלבד, לקבוע קרונות ולהפנות לעבר מסמכים אחרים בהן ניתן למצוא התייחסויות מפורטות יותר הכפופות לשינויים או עדכונים תכופים יותר.

בבואן לנסח את מסמך מדיניות ביטחון המידע שלהן, יידרשו ארגוני שירותי הבריאות לשקול באופן ספציפי את הגורמים המפורטים להלן, הייחודיים למגזר הבריאות:

(ו) רוחבו של מידע הבריאות

(ז) זכויותיו חובותיו האתיים של צוותי העובדים, כמוסכם בהוראות החוק, וכמקובל על חברי הארגונים המקצועיים;

(ח) זכויותיהם של מטופלים, כאשר הנושא רלוונטי, לפרטיות ולגישה לרישומים על אודותיהם;

(ט) חובותיו של הצוות בתחום הקליני להשיג את הסכמתם של מטופלים לשימוש במידע האישי שלהם, ובאשר להקפדה על ההגנה על סודיותו של מידע זה;

(י) הצרכים הלגיטימיים של עובדים בתחומים הקליניים ושל ארגוני שירותי בריאות להיות מסוגלים להתגבר על פרוטוקולי ביטחון רגילים כאשר עדיפויות הטיפול הרפואי, הקשורות לעיתים קרובות בחוסר יכולתו של מטופל לבטא את העדפותיו, מחייבות עקיפות מעין אלה; כמו כן, הנהלים הדרושים ליישום במצבים מעין אלה;

(יא) חובותיהם של ארגוני שירותי הבריאות, כמו גם של המטופלים, כאשר הטיפול הרפואי מוענק על בסיס "טיפול משותף" או "טיפול מורחב;"

(יב) הפרוטוקולים והנהלים שיש ליישם לצורך שיתוף במידע למטרות מחקר וניסויים קליניים;

(יג) סידורים מתאימים בעבור עובדים זמניים, כגון ממלאי מקום, סטודנטים וצוותים "לפי דרישה," לרבות גבולות הסמכות שלהם;

(יד) סידורים מתאימים בנושא הגישה למידע בריאות אישי על ידי מתנדבים וצוותי תמיכה כגון אנשי דת וארגוני צדקה למיניהם, לרבות גבולות הסמכות שלהם;

ארגוני בריאות רבים נוכחו לדעת, כי יש יתרון בהעברת המסמך לידיעתם ועיונם של צוותי העובדים באמצעים אלקטרוניים באמצעות אזור מידע בטוח הנכלל ברשת האינטראנט הפנים-ארגוני.

כאשר ארגון שירותי הבריאות זוכה לתמיכה או סיוע מצדדים שלשיים, או משתף פעולה עם ארגוני צד שלישי, ובמיוחד כאשר הוא מקבל סיוע מאזורים גיאוגראפיים אחרים, קיימת **חובה** לכלול במסגרת המדיניות מדיניו, בקרות ונהלים מתועדים המכסים פעילות הדדית זו והמפרטים את תחומי האחריות של כל אחד מן הצדדים.

במקרים שבהם מידע אישי חוצה גבולות לאומיים או שיפוטיים, יש חובה ליישם את הנחיותיו של תקן ISO 22857.

7.2.2 סקירת מסמך מדיניות ביטחון המידע

<u>בקרה</u>

חלה **חובה** על כך כי מדיניות ביטחון המידע של הארגון תהיה כפופה לסקירה שוטפת וכוללת בפרקי זמן קבועים, כך שהמדיניות כולה תיבחן לכל הפחות פעם אחת מדי שנה. חלה **חובה** לבחון את פרטי המדיניות אחרי תקרית ביטחון משמעותית.

<u>הנחית יישום</u>

בנוסף לעמידה בהנחיות המפורטות בתקן ISO/IEC 27002, **חייבת** סקירה זו לכלול התייחסות לנושאים שלהלן:

(א) טיבן המשתנה של פעילות ארגוני שירותי הבריאות והשינויים הנובעים מכך בפרופיל הסיכונים ובצרכי ניהול הסיכונים;

(ב) השינויים שנערכו בתשתית טכנולוגיות המידע של הארגון, והשינויים הנובעים מהם בפרופיל הסיכונים של הארגון;

(ג) השינויים שזוהו בסביבה החיצונית המשפיעים גם הם על פרופיל הסיכונים של הארגון;

(ד) דרישות והסדרי הבקרות, הציות והביטחון העדכניים הנדרשים על פי החקיקה התקפה, או על בסיס חקיקה או רגולציה חדשה;

(ה) ההנחיות וההמלצות המעודכנות מארגוני שירותי בריאות מקצועיים כמו גם מישויות האחראיות על שמירת פרטיות המידע באשר להגנה על מידע בריאות אישי;

(ו) תוצאותיהם של מקרים משפטיים שנדונו בערכאות משפטיות, אשר קבעו, או לחילופין שללו, תקדימים או נהלים מקובלים בארגון;

(ז) אתגרים וסוגיות הנוגעים למדיניות, כפי שאלה מבוטאים בפני הארגון על ידי צוותי עובדיו, המטופלים ושותפיהם ומטפליהם, חוקרים וממשלות (כגון ישויות הנושאות באחריות לשמירת פרטיות המידע).

7.3 ארגון ביטחון המידע

7.3.1 כללי

הנהלתו של ארגון שירותי בריאות היא הנושאת באחריות לביטחון מידע הבריאות האישי ולביטחון של מידע בריאות קשור אחר המטופל על ידי הארגון. האמור לעיל חשוב במיוחד בעבור ארגונים הסומכים על שירותים מנוהלים המוענקים על ידי צדדים שלישיים. תאום יעיל מהווה גם הוא מרכיב חיוני בשמירה על ביטחון המידע. שתי המשימות דורשות כי בארגון תתקיים ותפעל תשתית ברורה ואיתנה של ניהול ביטחון מידע.

7.3.2 ארגון פנימי

7.3.2.1 מחויבות הדרג הניהולי לביטחון המידע, תאום ביטחון המידע והקצאת תחומי אחריות בביטחון המידע

בקרה

על ארגונים המעבדים מידע בריאות אישי חלה **החובה**:

(א) להגדיר באופן ברור ולהקצות תחומי אחריות בנושא ביטחון המידע;

(ב) לקיים פורום ניהול ביטחון מידע בארגון על מנת להבטיח כי מתקיימות הנחיה והכוונה ברורות של הדרג הניהולי בנושא יוזמות ביטחון הנוגעות לביטחון מידע הבריאות האישי, כמתואר בסעיף משנה 6.4.3.

לכל הפחות אדם אחד **חייב** לשאת באחריות לביטחון מידע הבריאות בתוך הארגון.

פורום ביטחון מידע הבריאות יהיה **חייב** להתכנס באופן סדיר, על בסיס חודשי או קרוב לחודשי. (בדרך כלל יהיה זה יותר יעיל להתכנס באמצע התקופה שבין ישיבות גוף השליטה לו מדווח הפורום. הדבר יאפשר לטפל בסוגיות דחופות בישיבה מוסדרת תוך פרק זמן קצר).

תחול **חובה** לנסח תצהיר טווח המגדיר את גבולות פעילות הציות במונחי אנשים, תהליכים, מקומות, פלטפורמות ויישומים.

הנחיית יישום

בנוסף להנחיות הנכללות בתקן ISO/IEC 27002, חשוב לציין את טיבה החיוני של אחריות הדרג הניהולי בארגונים השומרים בקרבם מידע בריאות אישי, כמתואר בסעיף 6.2 לעיל. הנשיאה באחריות והתאום יוכלו להישמר בטווח הארוך רק אם הארגון הקים תשתית ניהול ביטחון מידע ברורה ומפורשת.

ללא קשר למבנה הארגוני המאומץ, חשוב באופן קריטי כי הוא יתוכנן כך שהוא יקדם את הגישה על ידי המטופלים (למשל כדי להמציא בקשות לקבלת מידע בריאות אישי), כי הוא יקדם את הדיווח בתוך המבנה הארגוני, וכי הוא יבטיח את המסירה בזמן של מידע.

כמצוין בסעיף משנה 6.4.3, חלה **חובה** על קצין ביטחון המידע של הארגון (בין אם ווירטואלי ובין אם ממשי), בין שאר חובותיו, לדווח לפורום ולהעניק לו שירותי מזכירות. הקצין יישא באחריות לאיסוף והפרסום של הדוחות המתקבלים מחברי הפורום ולהנפקת הערות בגינם.

על ארגוני שירותי בריאות חלה **חובה** לפרסם פרסום מקיף בארגוניהם את תצהיר הטווח, ולסקור אותו בשלב מאוחר יותר תוך שהם מוודאים כי הוא מאומץ על ידי קבוצות שליטת המידע, והשליטה הקלינית והתאגידית בארגון.

7.3.2.2. תהליך האישור לאמצעי עיבוד המידע

לא קיימת הנחיה נוספת בנושא זה לניהול ביטחון המידע במגזר הבריאות.

7.3.2.3 הסכמי סודיות

בקרה

בנוסף לעמידה בהנחיות הנכללות בתקן ISO/IEC 27002, ארגונים המעבדים מידע בריאות אישי **חייבים** להחזיק בהסכם סודיות המפרט את טיבו הסודי של מידע זה. ההסכם **חייב** להיות מיושם על כלל כוח האדם שהוא בעל גישה למידע בריאות.

הנחיית יישום

חלה **חובה** כי ההסכם דלעיל יכלול התייחסות לענישה האפשרית כאשר מזוהה הפרה של מדיניות ביטחון המידע.

7.3.2.4 קשר עם רשויות, קבוצות בעלות אינטרס מיוחד, וסקירה עצמאית של ביטחון המידע

לא קיימת הנחיה נוספת בנושא זה לניהול ביטחון המידע במגזר הבריאות.

7.3.3 צדדים שלישיים

7.3.31 זיהוי סיכונים הקשורים לצדדים חיצוניים

<u>בקרה</u>

חלה **חובה** על ארגונים המעבדים מידע בריאות להעריך את הסיכונים הכרוכים בגישתם של צדדים חיצוניים למערכות אלה או למידע שהם כוללים, והם יפעלו ליישומן של בקרות ביטחון שיהיו נאותות ומתאימות לרמת הסיכון שזוהתה ולטכנולוגיות הנמצאות בשימוש.

<u>הנחיית יישום</u>

הערכת סיכונים היא מהלך חיוני לניהול היעיל של גישתם של צדדים שלישיים למערכות הכוללות מידע בריאות, ובייחוד מידע בריאות אישי. חשוב להגן על זכויות המטופל, גם כאשר גורם חיצוני עם פוטנציאל גישה למידע בריאות אישי נמצא בתחום שיפוט אחר מזה שבו נמצאת הישות השולטת על המטופל או על ארגון שירותי הבריאות.

7.3.3.2 טיפול בסוגיות ביטחון במסגרת הקשר עם לקוחות

לא קיימת הנחיה נוספת בנושא זה לניהול ביטחון המידע במגזר הבריאות.

7.3.3.3 טיפול בסוגיות ביטחון במסגרת הסכמים עם צדדים שלישיים

<u>בקרה</u>

ארגוני שירותי בריאות הנעזרים בשירותיהם של צדדים שלישיים, כאשר שירותים אלה כוללים עיבוד של מידע בריאות אישי, **חייבים** לעשות שימוש בחוזים פורמאליים המפרטים, כדלקמן:

(א) את טיבו וערכו הסודי של מידע הבריאות האישי;

(ב) צעדי הביטחון אשר עומדים להיות מיושמים ו/או שיחול ציות להם;

(ג) ההגבלות החלות על צדדים שלישיים בגישה לשירותים אלה;

(ד) רמות השירות שיש להשיג בשירותים המוענקים;

(ה) הפורמט והתדירות של הדיווח לפורום ניהול ביטחון המידע בארגון;

(ו) ההסדר שסוכם באשר לייצוגו של הצד השלישי בישיבות וקבוצות העבודה המוסדרות של ארגון שירותי הבריאות;

(ז) הסידורים שננקטו באשר לביקורת הציות בקרב הצדדים השלישיים;

(ח) הענישה אשר תיושם בכל מקרה של כשל על פי המפורט לעיל.

<u>הנחיית יישום</u>

בנוסף להנחיות הנכללות בתקן ISO/IEC 27002, הדרישה דלעיל נועדה להבטיח כי נשמרות הסודיות, השלמות והזמינות של מידע הבריאות האישי כאשר המידע זורם מעבר לתחום שליטתו הישיר של ארגון שירותי הבריאות. כאשר המידע זורם מעבר לגבולות תחומי שיפוט, ראה הנחיות נוספות בתקן ISO 22857.

כאשר צד שלישי אינו מעבד מידע בריאות אישי, יתכן ועדיין יהיה מקום לנסח קטע מתאים מתוך סעיפי החוזה שפורטו לעיל. מומלץ ליישם הסכם המפרט סדרה מינימאלית של בקרות בכל מקרה של אספקת שירות על ידי צד שלישי.

7.4 ניהול נכסים

7.4.1 אחריות לנכסי מידע הבריאות

<u>בקרה</u>

בנוסף להנחיות הנכללות בתקן ISO/IEC 27002, חלה **חובה** על ארגונים המעבדים מידע בריאות אישי, כדלקמן:

(א) לתעד את נכסי מידע הבריאות ולעקוב אחריהם (כגון ניהול מלאי של נכסים מעין אלה);

(ב) למנות שומר מוגדר לנכסי מידע בריאות אלה;

(ג) לנסח ולקיים כללים לשימוש בנכסים אלה, המזוהים, מתועדים ומיושמים.

<u>הנחיית יישום</u>

על ארגונים המעבדים מידע בריאות חלה **החובה** לנסח כללים שנועדו לקיים את המטבע של הנכסים דלעיל (כגון המטבע של מאגר נתונים של תרופות), כמו גם את שלמותם של הנכסים (לדוגמה השלמות התפקודית של מכשירים רפואיים הרושמים או מדווחים נתונים).

מכשירים הרושמים או מדווחים נתונים יכולים להיות כפופים לשיקולי ביטחון מיוחדים בקשר עם הסביבה בה הם פועלים, ולקרינה האלקטרו-מגנטית המתרחשת במהלך הפעלתם. חלה **חובה** לזהות מכשירים אלה בנפרד.

7.4.2 סיווג מידע הבריאות

7.4.2.1 הנחיות סיווג

<u>בקרה</u>

בנוסף להנחיות הנכללות בתקן ISO/IEC 27002, חלה **חובה** על ארגוני שירותי בריאות המעבדים מידע בריאות אישי לסווג את המידע דלעיל באופן גורף כסודי.

<u>הנחיית יישום</u>

קביעתן של רמות הגנה לנכסי מידע בתחום שירותי הבריאות היא מלאכה מורכבת, והשוואות עם סיווג מידע ממשלתי או צבאי עלולות להתברר כמטעות. הנקודות המפורטות להלן מהוות מאפיינים חשובים של נכסי מידע בתחום שירותי הבריאות.

(א) סודיותו של מידע הברירות האישי הוי לעיתים קרובות סובייקטיבית בעיקרה. במילים אחרות, רק האדם המהווה את מושא המידע (לדוגמה: המטופל) יכול לקבוע באופן נאות באשר לסודיותן היחסית של קבוצות או מקבצי מידע שונים. לדוגמה, אדם הנמלט מקשר נצלני יוכל להיות סבור כי פרסום כתובתו ומספר הטלפון החדשים שלו הם סודיים הרבה יותר מאשר הנתונים הקליניים הנוגעים לזרועו השבורה.

(ב) סודיותו של מידע הבריאות האישי הוא תלוי הקשר. לדוגמה, שמו וכתובתו של מטופל המופיעים ברשימת קבלת מטופלים לבית חולים לא ייחשבו לסודיים במיוחד על ידי אותו המטופל, ואולם אותם הפרטים המופיעים ברשימת הקבלה לקליניקה לטיפול באין אונות יוכלו להיחשב לסודיים ביותר על ידי אותו המטופל.

(ג) סודיותו של מידע הבריאות האישי יכולה להשתנות במהלך תקופת חייו של רשומת הבריאות של אדם יחיד. לדוגמה, השינוי בגישות חברתיות שחל בעשרים השנים האחרונות הוביל מטופלים רבים לכך כי הם אינם מעריכים את האוריינטציה המינית שלהם כנושא סודי. אם לציין מקרה הפוך, הגישות המעודכנות לשימוש בסמים ובאלכוהול הביאו מטופלים מסוימים לראות במידע הייעוץ האישי שלהם כסודי היום הרבה יותר ממה שהוא היה בכל עת במהלך עשרים השנים האחרונות.

מכיוון שלא ניתן לחזות את רגישותו של מרכיב זה או אחר של מידע הבריאות האישי לאורך כלל שימושיו, ועל פני כל שלבי מחזור חייו, **חייב** כל מידע הבריאות האישי להיות כפוף להגנה זהירה מתאימה בכל עת. יש לציין, כי למרות העובדה כי כלל מידע הבריאות האישי חייב להיות מסווג באופן אחיד כסודי, שיקולים מעשיים עשויים לדרוש כי יזוהו פרטיו של מטופל שיהיו בסיכון גישה גבוה על ידי מי שאינו צריך להכירם. יחידים בעלי רשומות המידע אלה כוללים את עובדי הארגון (בייחוד אם מצבם הוא כזה המפיק תגובה רגשית כזו או אחרת), ראשי ממשלות, ידוענים, פוליטיקאים, יוצרי חדשות, וחברי קבוצות המתמודדות עם סיכונים גבוהים במיוחד (כגון אלה הסובלים ממחלות מין מדבקות, או כאלה שמידע הבריאות האישי שלהם כולל מידע על נטיות גנטיות לסבל ממחלות קשות). יתכן ויהיה צורך לתייג את נתוניהם של אנשים אלה באופן מיוחד, כך שניתן יהיה לעקוב מקרוב אחר כל גישה למידע זה. עם זאת, יש ליישם זהירות רבה ביישום נהלים מעין אלה שכן תיוג מעין זה עלול להחמיר דווקא את הבעיה שהוא נועד למנוע, כלומר, הוא עלול למשוך תשומת לב לנתונים הספציפיים הנתונים לתיוג המיוחד. חשוב להדגיש גם כי בעוד שמטופלים יחידים עשויים להימצא

בסיכון מוגבר, אין הדבר מחייב כי מידע הבריאות האישי שלהם יהיה סודי יותר מאשר זה של מטופלים אחרים. כל מידע בריאות אישי הוא סודי ויש להתייחס אליו בהתאם. ראה גם את הדיון בסעיף משנה 7.5.2.1.

הזיהוי (והתיוג, כאשר הדבר מתאים) של נכסי המידע כנכסים סודיים עשוי להוות כלי חשוב בהדרכת הצוותים ובציות למדיניות. הדבר פועל באופן מיטבי כאשר הסיווג פועל כאינדיקאטור לנהלים הדרושים לטיפול במידע הספציפי. יתרה מכך, הסיווג יכול לשמש מרכיב חשוב של הסכמי הגנה על המידע בין תחומי שיפוט שונים ועם ארגוני צדדים שלישיים ועובדיהם. הזיהוי והתיוג של נכסי מידע הוא מרכיב חיוני גם של תקן ISO/IEC 27702.

7.4.2.2 תיוג מידע וטיפול במידע

<u>בקרה</u>

חלה **חובה** על כלל מערכות מידע הבריאות המעבדות מידע בריאות אישי לעדכן את המשתמשים על אודות סודיותו של מידע הבריאות האישי הזמין דרך המערכת (לדוגמה על ידי כניסה למערכת עם סיסמה), וחלה עליהם **חובה** לציין כסודי כל מסמך מודפס כאשר הוא כולל מידע בריאות אישי.

<u>הנחיית יישום</u>

לא כל מידע הבריאות הוא סודי, ולא כל מערכות מידע הבריאות מאפשרות למשתמשים גישה למידע בריאות אישי. המשתמשים של מערכות מידע בריאות חייבים לדעת מתי המידע לו הם ניגשים כולל מידע בריאות אישי.

7.5 ביטחון משאבי אנוש

7.5.1 לפני ההעסקה

7.5.1.1 תפקידים ואחריות

<u>הנחיית יישום</u>

בנוסף לעמידה בהנחיות הנכללות בתקן ISO/IEC 27002, חלה **חובה** על ארגונים אשר עובדיהם עוסקים בעיבוד מידע בריאות אישי לתעד את מעורבותם זו של העובדים במידע במסמכי תיאורי תפקיד רלוונטיים.

גם תפקידי הביטחון ותחומי האחריות כפי שהם מוגדרים במדיניות ביטחון המידע של הארגון **חייבים** להיות מתועדים בתיאורי התפקידים הרלוונטיים.

תשומת לב מיוחדת חייבת להיות מוקדשת לתפקידים ותחומי האחריות של צוותי עובדים זמניים או לטווח קצר כגון ממלאי מקום, סטודנטים, מתמחים וכדומה.

7.5.1.2 סינון

<u>בקרה</u>

בנוסף לעמידה בהנחיות הנכללות בתקן ISO/IEC 27002, חלה **חובה** על ארגונים אשר צוותי העובדים, הקבלנים או מתנדביהם מעבדים (או צפויים לעבד) מידע בריאות אישי, **לכל הפחות**, לוודא את זהותם, כתובתם המעודכנת ומקום העבודה הקודם של אותם צוותי עובדים, עובדי קבלן או מתנדבים במועד פנייתם לקבלה לעבודה בארגון.

<u>הנחיית יישום</u>

חשוב לדעת כיצד והיכן ליצור קשר עם צוות רופאי מקצועי, למרות שלנוכח העובדה כי צוותים רפואיים מחליפים מקומות עבודה לעיתים מזומנות, עלול לכתובות להיות ערך מוגבל בלבד. לכן, מומלץ כי ארגוני שירותי בריאות ישקלו לאסוף מספר סביר של המלצות ולנקוט בדיקות מסוגים אחרים, לדוגמה כאלה הננקטים על ידי גופים מקצועיים וישויות אקדמיות.

בכל מקרה בו הדבר אפשרי, חלה **חובה** לבדוק האם קיים רקע פלילי. ראה גם .7.8.2.1

7.5.1.3 תנאי ההעסקה

<u>הנחיית יישום</u>

בנוסף לעמידה בהנחיות הנכללות בתקן ISO/IEC 27002, חלה חובה על ארגונים המעבדים מידע בריאות אישי לכלול תצהיר בדבר אחריותו של העובד לביטחון המידע במסגרת תנאי העסקתם של עובדים העתידים לעבד מידע בריאות אישי.

חלה **חובה** על תנאי ההעסקה לכלול:

(א) התייחסות לענישה האפשרית במקרה של זיהוי הפרה של מדיניות ביטחון המידע של הארגון;

(ב) פסקה המציינת כי התנאים הנוגעים לסודיותו של מידע הבריאות האישי שורדים את סיום ההעסקה לנצח.

בכל הנוגע לצוות עובדים קליניים, חלה **חובה** על תנאי העסקתם לפרט את תנאי הגישה המוענקים לצוותים אלה לנתוני המטופלים, כמו גם את תנאי גישתם למערכות מידע בריאות קשורות למקרה של תביעות שיועלו על ידי צדדים שלישיים.

אם חלף זמן רב בין מועד הקבלה לעבודה ותחילת העבודה בפועל, חלה **חובה** לשקול ברצינות חזרה על תהליך הסינון, או על מרכיבי המפתח שלו.

7.5.2 במהלך תקופת ההעסקה

7.5.2.1 תחומי אחריות של ההנהלה

<u>הנחיית יישום</u>

בנוסף לעמידה בהנחיות הנכללות בתקן ISO/IEC 27002, חשוב לציין את הדגש המיוחד שיש לשים על רצונותיהם של מטופלים שאינם מעוניינים כי מידע הבריאות האישי שלהם יהיה נגיש לעובדי מגזר הבריאות המהווים שכנים, עמיתים למקצוע או קרובי משפחה. דאגות אלה מהוות לעיתים קרובות אחוז גבוה של התלונות המגיעות מאותם מטופלים המודאגים באשר לסודיותו של מידע הבריאות האישי שלהם. באופן דומה, עובדים יכולים להימצא במצב בו הם אינם מעוניינים להימצא ללא צורך במצב בו הם נאלצים לסקור מידע על חברים, קרובי משפחה או שכנים. ניהול יעיל של מערכות מידע בריאות חייב לתת את הדעת להיבטים אישיים אלה.

7.5.2.2 מודעות לביטחון מידע, חינוך והדרכה

<u>בקרה</u>

בנוסף לעמידה בהנחיות הנכללות בתקן ISO/IEC 27002, חלה **חובה** על ארגונים המעבדים מידע בריאות אישי להבטיח כי ניתנים חינוך והדרכה בנושאי ביטחון המידע כבר בשלב ההעסקה הראשון, וכי עדכונים שוטפים מוצעים לעובדים בנושאי מדיניות הביטחון התאגידית והנהלים הקשורים אליה, כמו גם, כאשר הדבר רלוונטי, לקבלני צד שלישי, חוקרים, סטודנטים ומתנדבים המעבדים מידע בריאות אישי.

7.5.2.3 הליך משמעתי

<u>הנחיית יישום</u>

בנוסף לעמידה בהנחיות הנכללות בתקן ISO/IEC 27002, חלה **חובה** על ארגונים המעבדים מידע בריאות אישי לוודא, כי ההליכים המשמעתיים בקשר עם הפרות של מדיניות ביטחון המידע ישקפו את המדיניות, ואי לכך יהיו מוכרים ליחיד הכפוף להליך המשמעתי. בנוסף לעמידתם בחקיקה הקיימת, חלה חובה כי ההליכים דלעיל יעלו בקנה אחד גם עם ההסכמים הקיימים בין אנשי המקצוע בתחום הבריאות והגופים המקצועיים הפועלים בתחום זה.

7.5.3 סיום או שינוי העסקה

7.5.3.1 אחריות בעת סיום העסקה והחזרת נכסים

<u>הנחיית יישום</u>

בנוסף לעמידה בהנחיות הנכללות בתקן ISO/IEC 27002, חשוב לציין כי בתחום שירותי הבריאות עוברים סוגים שונים של עובדים, כגון רופאים ואחיות דרך קבע דרך תוכניות הכשרה והדרכה ו"רוטציות" מסוגים אחרים, כאשר זכויות הגישה שלהם יכולות להשתנות בהתאם בכל אחד מן המצבים דלעיל. על מנת להבטיח את סיומן של זכויות קודמות שאינן נחוצות עוד לתפקידים, מומלץ לטפל בשינויי העסקה מעין אלה באופן זהה לאופן בו מטופלת עזיבתם של עובדים את הארגון.

7.5.3.2 הסרת הרשאות גישה למידע

בקרה

חלה **חובה** על ארגונים המעבדים מידע בריאות אישי לבטל, מהר ככל האפשר, את הרשאות היתר של המשתמש לגישה למידע בעבור כל עובד, קבלן צד שלישי או מתנדב המסיים את התקשרותו עם הארגון, מיד עם סיום ההעסקה, ההתקשרות החוזית או פעילות ההתנדבות.

הנחיית יישום

בנוסף לעמידה בהנחיות הנכללות בתקן ISO/IEC 27002, חשוב לציין כי קיימות דוגמאות רבות במגזר שירותי הבריאות למקרים של סטודנטים, מתמחים וממלאי מקום אשר שמרו על הרשאות הגישה שלהם לאחר סיום תפקידיהם בארגון. במיוחד בבתי חולים, כמויות גדולות של צוותי עובדים זמניים ייהנו בדרך כלל מגישה קצרת טווח למידע בריאות אישי. חלה חובה לנהל את הרשאות הגישה של עובדים מעין אלה באופן קפדני. בה בעת, במגזר שירותי הבריאות מתבצעות העברות מידע זמן ניכר אחרי מועד הענקת הטיפול הרפואי (לדוגמה, החתימה או השלמה של רישומים רפואיים). עובדה זו עלולה לסבך באופן משמעותי את תהליך הסרת הרשאות הגישה במועד מתאים, וחלה **חובה** לקחת העברות נתונים אלה בחשבון העת התכנון והיישום של נהלים העוסקים בהסרתן של הרשאות גישה למידע.

חלה **חובה** על ארגוני שירותי בריאות לשקול ברצינות את הסיום המיידי של הרשאות גישה בעקבות המצאתה של הודעת התפטרות, וכו', בכל מקום בו קיימת הערכה בדבר סיכון מוגבר הכרוך בהמשך קיומה של הרשאת הגישה.

7.6 ביטחון פיסי וסביבתי

7.6.1 אזורים בטוחים

7.6.1.1 אזור ביטחון פיסי

בקרה

על ארגונים המעבדים מידע בריאות אישי חלה **החובה** להגדיר אזורי ביטחון שנועדו להגן על אתרים הכוללים מתקני עיבוד מידע התומכים ביישומי הבריאות. אזורים בטוחים אלה **חייבים** להיות מוגנים באמצעות הגנות כניסה נאותות כדי שיובטח כי רק עובדים מורשים נהנים מגישה אליהם.

הנחיית יישום

בנוסף לעמידה בהנחיות הנכללות בתקן ISO/IEC 27002, חשוב להכיר בכך כי באתרי שירותי בריאות רבים כרוכה ההקמה של אזורים בטוחים בקושי מיוחד. אזורים תפעוליים רבים מוצפים במטופלים, ואכן, יתכן ולא קיים עוד מגזר תעשייתי שבו יש לציבור הרחב גישה כה נרחבת לאזורים תפעוליים כמו במגזר שירותי הבריאות. בה בעת, יש צורך לדאוג לסביבה בטוחה המשמרת את הבטיחות הפיסית ואת ביטחונם של מטופלים, כמו גם את אלה של המידע והמערכות שיתכן ויהיו נגישים באותה הסביבה.

בשונה מן המתרחש במגזרים אחרים, הלקוחות במגזר שירותי הבריאות לעיתים קרובות אינם מסוגלים, מן הבחינה הפיסית, לדאוג לבטיחותם וביטחונם האישי. חלה **חובה** לתאם בין צעדי הביטחון פיסי בעבור המידע לבין צעדי הביטחון והבטיחות הנדרשים בעבור המטופלים. על ארגוני שירותי הבריאות חלה החובה להגן על שניהם.

7.6.1.2 בקרות כניסה פיסיות; אבטחת משרדים, חדרים ומתקנים; הגנה מפני איומים חיצוניים וסביבתיים; עבודה באזורים בטוחים

הנחיית יישום

בנוסף לעמידה בהנחיות הנכללות בתקן ISO/IEC 27002, חלה **חובה** על ארגונים המעבדים מידע בריאות אישי לנקוט בצעדים הגיוניים כדי להבטיח כי הציבור הרחב נמצא בקרבתו של ציוד טכנולוגיות מידע (דהיינו שרתים, מתקני אחסון מידע, מסופים ותצוגות) רק באופן בו אין ברירה אחרת בעקבות מגבלה פיסית, וכפי שהתהליכים הקליניים השונים דורשים זאת בלבד.

7.6.1.3 גישה ציבורית, אזורי אספקה וטעינה

הנחיית יישום

בנוסף להנחיות הנכללות בתקן ISO/IEC 27002, חשוב לציין כי הענקת שירות הבריאות כוללת נסיבות ייחודיות שבהן הציבור (המטופלים, ומלוויהם או תומכיהם) מתקבל באופן פיסי לאזורים המתאפיינים בכמות גדולה של מידע רגיש (כגון ביצוע בדיקות מעבדה באזור בו זרימת העבודה עשויה להכתיב את איסוף המידע ממטופלים באותו האזור שבו מטופלים אחרים זוכים בו לטיפול; טיפולי חדר מיון בהם מלווים או קרובי משפחה יוכלו, באופן פוטנציאלי, להיות חשופים לכמויות משמעותיות של מידע מילולי או חזותי על אודות מטופלים אחרים; תחנות עבודה/סיעוד הצמודות למיטת המטופל והממוקמות בקרבת חדרי מטופלים). חלה **חובה**, אם כן, ליישם השגחה נוספת על אזורים אלה בשירותי הבריאות האוספים מידע בריאות באמצעות ראיונות/שיחות, והכוללים מידע המוצג על גבי מסכים.

על מנת להבטיח כי נשמרת פרטיותם של מטופלים,נדרש לעיתים קרובות במגזר שירותי הבריאות כי יוצבו הודעות על גבי מעליות או דלתות שמאחוריהן מתקיימים ראיונות, ובאזורים נוספים. הודעות אלה משמשות כתזכורת לצורך להמעיט בדיון על מקרים של מטופלים בשטחים הציבוריים.

7.6.2 ביטחון הציוד

7.6.2.1 מיקום הציוד וההגנה עליו

<u>הנחיית יישום</u>

בנוסף לעמידה בהנחיות הנכללות בתקן ISO/IEC 27002, חלה **חובה** על ארגונים המעבדים מידע בריאות אישי למקם כל תחנת עבודה המאפשרת גישה למידע בריאות אישי באופן המונע עיון בלתי מכוון בנתונים, או את הגישה אליהם על ידי המטופלים או הציבור הרחב.

מכשור רפואי הרושם נתונים או המדווח עליהם עשוי לדרוש שיקולי ביטחון מיוחדים בקשר עם הסביבה בה הוא פועל, והקרינה האלקטרו-מגנטית המתרחשת במהלך הפעלתו. ארגוני שירותי בריאות, ובמיוחד בתי חולים, **חייבים** להבטיח כי המיקום והנחיות ההגנה החלות על מכשור טכנולוגיות המידע מקטינים למינימום את החשיפה לקרינה מעין זו.

7.6.2.2 אמצעי תמיכה, בטיחות כבלים ותחזוקת ציוד

<u>הנחיית יישום</u>

בנוסף לעמידה בהנחיות הנכללות בתקן ISO/IEC 27002, חלה **חובה** על ארגונים המעבדים מידע בריאות אישי לשקול ברצינות את הסיכון של רשתות ושל חיווט אחר באזורים המאופיינים בקרינה גבוהה ממכשור רפואי.

7.6.2.3 ביטחון הציוד שאינו נמצא באתר

<u>בקרה</u>

בנוסף לעמידה בהנחיות הנכללות בתקן ISO/IEC 27002, חלה **חובה** על ארגונים המעבדים מידע בריאות אישי להבטיח כי כל שימוש הנעשה מחוץ למתחם הפיסי שלהם במכשור רפואי הרושם או מדווח נתונים רפואיים הוא מורשה. חלה **חובה** כי האמור לעיל יכלול ציוד המשמש עובדי חוץ, גם במקום בו שימוש מעין זה הוא קבוע (לדוגמה, במקרים שבהם הוא מהווה חלק חשוב מתפקידו של העובד, כגון צוותי אמבולנסים, תראפיסתים, ועוד).

7.6.2.4 סילוק בטוח של ציוד או שימוש חוזר בו

<u>בקרה</u>

בנוסף לעמידה בהנחיות הנכללות בתקן ISO/IEC 27002, חלה **חובה** על ארגונים המעבדים מידע בריאות אישי לשכתב באופן בטוח רשומות קודמות, או לחילופין להשמיד כל מדיה הכוללת תוכנת אפליקציית מידע בריאות, או מידע בריאות אישי, כאשר המדיה אינה נדרשת עוד לשימוש.

7.6.2.5 סילוק נכס קבוע

<u>בקרה</u>

בנוסף לעמידה בהנחיות הנכללות בתקן ISO/IEC 27002, חלה **חובה** על ארגונים המספקים ציוד, נתונים או תוכנה, או המשתמשים בהם, שנועדו לתמוך ביישום בתחום שירותי הבריאות הכולל מידע בריאות אישי, למנוע מצב בו ציוד, נתונים, או תוכנה אלה יורחקו מן האתר, או יוצבו במקום אחר, מבלי שהתקבלה ההסכמה של הארגון לכך.

7.7 ניהול התקשורת והתפעול

7.7.1 נהלים ותחומי אחריות תפעוליים

7.7.1.1 נהלי תפעול מתועדים

לא קיימות הנחיות נוספות לניהול ביטחון המידע בתחום הבריאות.

7.7.1.2 ניהול שינוי

בקרה

בנוסף לעמידה בהנחיות הנכללות בתקן ISO/IEC 27002, חלה **חובה** על ארגונים המעבדים מידע בריאות אישי לבקר את השינויים החלים במתקני עיבוד המידע המעבדים מידע בריאות אישי, באמצעות יישומו של תהליך שינוי פורמאלי ומובנה, זאת כדי להבטיח בקרה נאותה של יישומי מחשב מארחים ומערכות אחרות, כמו גם את המשכיותו של הטיפול הרפואי במטופל.

הנחיית יישום

חשוב לציין כי שינויים בלתי ראויים, כאלה שלא נבדקו כיאות או שינויים שגויים בכל הקשור לתהליך העיבוד של מידע בריאות אישי עלולים להביא להשלכות הרות אסון הן לטיפול הרפואי והן לבטיחות. תהליך השינוי **חייב** לתעד באופן מפורש ולהעריך את הסיכונים הכרוכים בשינוי.

7.7.1.3 הפרדת חובות

הנחיית יישום

בנוסף לעמידה בהנחיות הנכללות בתקן ISO/IEC 27002, חלה **חובה** על ארגונים המעבדים מידע בריאות אישי, כאשר הדבר הוא בר-ביצוע, להפריד בין חובות ותחומי אחריות על מנת להקטין על ידי כך את אפשרויות השינוי הבלתי מורשה, או הניצול לרעה, של מידע הבריאות האישי.

על ארגונים המעבדים מידע בריאות אישי חלה **החובה** להבטיח כי מערכות טכנולוגיות המידע כוללות מנגנונים מובנים מסוימים האוכפים, כאשר הדבר נדרש, את האישור של תהליכים קליניים על ידי בעלי תפקידים שונים בארגון.

7.7.1.4 הפרדה בין מתקני פיתוח, ניסוי ותפעול

בקרה

בנוסף לעמידה בהנחיות הנכללות בתקן ISO/IEC 27002, חלה **חובה** על ארגונים המעבדים מידע בריאות אישי להפריד (בין אם פיסית ובין אם באופן ווירטואלי) את סביבות הפיתוח והניסוי בעבור מערכות המידע התומכות במידע דלעיל מן הסביבות התפעוליות המארחות את מערכות המידע האלה. כללים באשר לנדידה של תוכנה מסטאטוס של פיתוח לעבר סטאטוס תפעולי יהיו **חייבים** להיות מוגדרים ומתועדים על ידי הארגון המארח את יישום/מי המחשב הנוגעים בדבר.

7.7.2 ניהול אספקת שירותי צדדים שלישיים

הנחיית יישום

ניהול אספקת השירותים על ידי צדדים שלישיים הופך פשוט באופן ניכר, כאשר מאומץ הסכם פורמאלי המפרט סדרה מינימאלית של בקרות שיש ליישם.

7.7.3 תכנון וקבלה של מערכות

7.7.3.1 ניהול יכולת

לא קיימות הנחיות נוספות לניהול ביטחון המידע בתחום הבריאות.

7.7.3.2 קבלת מערכת

בקרה

בנוסף לעמידה בהנחיות הנכללות בתקן ISO/IEC 27002, חלה **חובה** על ארגונים המעבדים מידע בריאות אישי לקבוע קריטריונים שיחולו על מערכות מידע חדשות מתוכננות, כמו גם לעדכונים ולגרסאות חדשות.

חלה **חובה** לערוך גם ניסויים מתאימים במערכות אלה לפני הטמעתן בארגון.

<u>הנחיית יישום</u>

חלה **חובה** לקבוע את היקפם ואת דרגת הקפדנות של ניסויים אלה בהתאמה לסיכונים המזוהים ככרוכים בשינוי. ראה גם סעיף משנה 7.7.1.2.

7.7.4 הגנה מפני קוד זדוני ונייד

7.7.4.1 בקרות מפני קוד זדוני

<u>בקרה</u>

בנוסף לעמידה בהנחיות הנכללות בתקן ISO/IEC 27002, חלה **חובה** על ארגונים המעבדים מידע בריאות אישי ליישם בקרות מניעה, איתור ותגובה נאותות כאמצעי הגנה מפני תוכנה זדונית, וכמו כן חלה עליהם **החובה** ליישם הדרכה להשגת מודעות משתמשים נאותה לתופעה זו.

7.7.4.2 בקרות מפני קוד נייד

לא קיימות הנחיות נוספות לניהול ביטחון המידע בתחום הבריאות.

7.7.5 גיבוי מידע הבריאות

<u>בקרה</u>

בנוסף לעמידה בהנחיות הנכללות בתקן ISO/IEC 27002, חלה **חובה** על ארגונים המעבדים מידע בריאות אישי לגבות כל מידע בריאות אישית, ולאחסנו בסביבה בטוחה מבחינה פיסית כדי להבטיח את זמינותו העתידית.

כדי להגן על סודיותו, חלה **חובה** לגבות מידע בריאות אישי בפורמט מקודד.

7.7.6 ניהול ביטחון רשת

7.7.6.1 בקרות רשת

לא קיימות הנחיות נוספות לניהול ביטחון המידע בתחום הבריאות.

7.7.6.2 ביטחון שירותי הרשת

<u>הנחיית יישום</u>

בנוסף לעמידה בהנחיות הנכללות בתקן ISO/IEC 27002, חלה **חובה** על ארגונים המעבדים מידע בריאות אישי לשקול בזהירות מה עלולה להיות ההשלכה של אובדן זמינות שירות הרשת על תהליכי העבודה הקלינית בארגון. ראה גם 7.11.

7.7.7 טיפול במדיה

7.7.71 ניהול של מדיית מחשב הניתנת להסרה

<u>הנחיית יישום</u>

בנוסף לעמידה בהנחיות הנכללות בתקן ISO/IEC 27002, חלה **חובה** על ארגונים המעבדים מידע בריאות אישי להבטיח כי כלל מידע הבריאות האישי המאוחסן במדיה הניתנת להסרה הוא:

(א) מקודד כל אימת שהמדיה שלו נמצאת במעבר, או

(ב) מוגן מפני גניבה כל אימת שהמדיה שלו נמצאת במעבר.

7.7.7.2 השמדת מדיה

<u>בקרה</u>

בנוסף לעמידה בהנחיות הנכללות בתקן ISO/IEC 27002, חלה **חובה** למחוק באופן בטוח כל מידע בריאות אישי, או לחילופין להשמיד את המדיה, כאשר אין הוא נדרש עוד לשימוש.

<u>הנחיית יישום</u>

ההשמדה הבלתי נאותה של מדיה ממשיכה להוות מקור להפרות חמורות של פרטיות מטופלים. חשוב במיוחד לציין בהקשר זה כי יש ליישם בקרה זו לפני התיקון או ההשמדה של כל ציוד נלווה או קשור. דרישה זו מתייחסת גם למכשור רפואי הרושם או מדווח נתונים.

7.7.7.3 נהלי טיפול במידע

<u>בקרה</u>

בנוסף להנחיות הנכללות בתקן ISO/IEC 27002, חלה **חובה** להגן על מדיה הכוללת מידע בריאות אישי באופן פיסי, או לחילופין לדאוג כי המידע הנכלל בה יקודד. הסטאטוס ומיקומה של מדיה הכוללת מידע בריאות אישי שאינו מקודד יהיה **חייב** להיות כפוף לפיקוח.

7.7.7.4 ביטחון תיעוד מסמכים

לא קיימות הנחיות נוספות לניהול ביטחון המידע בתחום הבריאות.

7.7.8 החלפת מידע

7.7.8.1 מדיניות ונהלי החלפת מידע והסדרי החלפה

<u>הנחיית יישום</u>

בנוסף להנחיות הנכללות בתקן ISO/IEC 27002, ניתן למצוא הנחיות ספציפיות בנושא מדיניות החלפת מידע הבריאות בתקן ISO 22857. למרות שהתקן דלעיל מתייחס ספציפית לזרימה חוצת הגבולות של מידע בריאות אישי (כאשר בהקשר זה הכוונה לגבולות היא תחומי שיפוט בתחום שירותי הבריאות, ולא בהכרח גבולות לאומיים), חלק גדול מן הייעוץ הנכלל בו ניתן להתאמה, כאשר הדבר נדרש, כדי לטפל בהחלפת מידע בין מספר ישויות.

על ארגונים תחול **החובה** להבטיח כי הביטחון של החלפות מידע מעין אלה ייבדק במסגרת ביקורת פיתוח מדיניות וציות בארגון (ראה סעיף 7.12).

ניתן לסייע באופן ניכר לביטחון של החלפת המידע על ידי שימוש בהסכמי החלפות מידע המפרטים מידה מינימאלית של בקרות ליישום על ידי הנוגעים בדבר.

7.7.8.2 מדיה פיסית במעבר

לא קיימות הנחיות נוספות לניהול ביטחון המידע בתחום הבריאות.

7.7.8.3 הודעות אלקטרוניות

<u>הנחיית יישום</u>

בנוסף לעמידה בהנחיות הנכללות בתקן ISO/IEC 27002, חלה **חובה** על ארגונים השולחים מידע בריאות אישי באמצעות הודעות אלקטרוניות לנקוט בצעדים אשר יבטיחו את סודיותו ושלמותו של המידע. מן הראוי לציין, כי הביטחון של הודעת דואר אלקטרוני ושל הודעות מיידיות הכוללות מידע בריאות אישי עלול להיות כרוך בנהלים שיחולו על צוותי עובדי שירותי הבריאות, ואשר לא ניתן יהיה להחילם על מטופלים ועל הציבור הרחב.

הודעות דואר אלקטרוני בין אנשי מקצוע בתחומי הבריאות, והכוללות מידע בריאות אישי, חייבות להיות מקודד בשלבי המעבר. גישה אחת בנושא זה כוללת את השימוש באישורים דיגיטליים. ראה את הביבליוגרפיה באשר לרשימת תקנים הקשורה לשימוש באישורים דיגיטליים בסביבות שירותי בריאות.

ראה גם את סעיף המשנה 7.12.2.2 לדיון בהסכמה הנדרשת קודם לקיום תקשורת אל מחוץ לארגון.

7.7.8.4 מערכות מידע בריאות

לא קיימות הנחיות נוספות לניהול ביטחון המידע בתחום הבריאות.

7.7.9 מערכות מידע בריאות אלקטרוניות

7.7.9.1 מסחר אלקטרוני ועסקאות מקוונות

הנחיית יישום

בנוסף להנחיות הנכללות בתקן ISO/IEC 27002, חשוב לציין כי יש לנהוג בזהירות כאשר קובעים האם המידע הנכלל בסחר אלקטרוני ובעסקאות מקוונות (online) כוללים מידע בריאות אישי. אם הם אכן כוללים מידע מעין זה, הוא חייב להיות מוגן כיאות. חשובים במיוחד במגזר שירותי הבריאות הם נתונים הנוגעים לחיובים כספיים, תביעות רפואיות, חשבוניות, דרישות ומידע סחר אלקטרוני מסוגים אחרים אשר ממנו ניתן לגזור מידע ביראות אישי.

7.7.9.2 מידע בריאות הזמין לכלל

בקרות

חלה **חובה** לשמור בארכיב מידע בריאות הזמין לכלל הציבור (להבדיל ממידע בריאות אישי).

חלה **חובה** להגן על שלמותו של מידע בריאות הזמין לציבור כדי למנוע את שינויו הבלתי מורשה.

חלה **חובה** לציין את פרטי המחברים של מידע בריאות הזמין לציבור, כמו גם להגן על שלמותו.

7.7.10 פיקוח

7.7.10.1 כללי

מבין כלל דרישות הביטחון להגנה על מידע בריאות אישי, אלה הנוגעות לביקורת ולתיעוד שוטף הן מן החשובות ביותר. דרישות אלה מבטיחות נשיאה ברורה באחריות בעבור המטופלים המפקידים את המידע האישי שלהם במערכות רישום בריאות אלקטרוניות, ובנוסף הן מהוות תמריץ חזק למשתמשים במערכות דלעיל כדי לעמוד בפרטי המדיניות באשר לשימוש המקובל במערכות אלה. ביקורת ותיעוד שוטף יעילים עשויים לסייע לגלות ניצול לרעה של מערכות מידע בריאות, או לחילופין של מידע הבריאות האישי עצמו. בנוסף, יכולים תהליכים אלה לסייע לארגונים ולמטופלים כאחד לזכות בהגנה מפני האפשרות בה משתמשים ינצלו לרעה את הרשאות הגישה שלהם למידע.

7.7.10.2 תיעוד שוטף ביומן פעילות (logging) למטרת ביקורת

הנחיית יישום

בנוסף לעמידה בהנחיות הנכללות בתקן ISO/IEC 27002, חלה **חובה** על ארגונים השולחים מידע בריאות אישי ליצור קובץ יומן פעילות שוטפת מאובטח, כל אימת שמשתמש ניגש למידע בריאות אישי, או לחילופין מעדכן או מאחסן אותו באמצעות המערכת. חלה **חובה** כי יומן הפעילות השוטף (log) יזהה באופן ייחודי את המשתמש, את נושא המידע (כגון המטופל), את המשימה המבוצעת על ידי המשתמש (יצירת רשומה, גישה, עדכון וכדומה), ולציין את השעה והמועד בו בוצע הצעד דלעיל.

כאשר מעודכן מידע בריאות אישי, חלה **חובה** לשמר רשומה של התוכן הקודם של המידע ושל רשומת הביקורת הקשורה (כגון פרטים על אודות מי נכנס למידע, ובאיזה תאריך).

מערכות תמסורת בהן נעשה שימוש על מנת להעביר הודעות הכוללות מידע בריאות אישי **חייבות** לנהל יומן פעילות של העברת המסרים (יומן פעילות מעין זה יהיה **חייב** לכלול את נתוני הזמן, התאריך, המקור והיעד של ההודעה, אך לא את תוכנה).

על הארגון חלה **חובה** לשקול ולקבוע בזהירות המתחייבת את תקופות השמירה של יומני פעילות אלה, תוך התייחסות מיוחדת לתקנים קליניים מקצועיים ולחובות הקיימים על פי חוק, על מנת שניתן יהיה לבצע חקירות עתידיות אם הדבר יידרש, ולהמציא ראיות בדבר ניצול אפשרי לרעה.

7.7.10.3 פיקוח על השימוש במערכת

הנחיית שימוש

בנוסף לעמידה בהנחיות הנכללות בתקן ISO/IEC 27002, חלה **חובה** כי פונקצית יומן הפעילות השוטפת (logging) של מערכת מידע הבריאות תמשיך להיות תפעולית בכל עת, כל אימת שהמערכת הכפופה לביקורת זמינה לשימוש.

חלה **חובה** כי מערכות הכוללות מידע בריאות אישי יכללו יכולות לניתוח יומני פעילות ונתיבי ביקורת, המסוגלות:

(א) לאפשר את זיהויים של כל משתמשי המערכת אשר להם הייתה גישה למערכת, או ששינו רשומה/ות כלשהי/הן של מטופל על פני פרק זמן נתון;

(ב) לאפשר את זיהויים של כלל המטופלים שהתבצעה גישה לרישומיהם, או אשר רישומיהם שונו על ידי מערכת כזו או אחרת במהלך תקופת זמן נתונה.

7.7.10.4 הגנה על מידע יומן הפעילות

בקרה

חלה **חובה** לשמר רשומות ביקורת כאשר הן בטוחות ומוגנות לחלוטין מפני פריצה מכל סוג. הגישה לכלי הביקורת של המערכת ולנתיבי הביקורת תהיה חייבת להיות מאובטחת כדי למנוע כל ניצול לרעה או סיכון.

הנחיית יישום

בנוסף לעמידה בהנחיות הנכללות בתקן ISO/IEC 27002, חשוב לציין כי ראיית שלמותם של רישומי הביקורת יכולה למלא תפקיד מרכזי בהליכים שונים, כגון חקירותיהם של חוקרי מקרי מוות, בחקירות בחשד למקרים של רשלנות רפואית, ובהליכים משפטיים או דומים אחרים. בהליכים דלעיל נקבעים מעשיהם של אנשי המקצוע בתחומי הבריאות, ועיתוי האירועים, לעיתים על ידי בדיקתם של השינויים והעדכונים שבוצעו ברשומות של מידע הבריאות האישי של מטופל.

7.7.10.5 יומני פעילות של מנהל ומפעילי המערכת

לא קיימות הנחיות נוספות לניהול ביטחון המידע בתחום הבריאות.

7.7.10.6 יומן פעילות לתיעוד ליקויים

לא קיימות הנחיות נוספות לניהול ביטחון המידע בתחום הבריאות.

7.7.10.7 סנכרון שעון

בקרה

מערכות מידע בריאות התומכות בפעילות טיפול רפואי משותפת המתאפיינת בזמנים קריטיים, יהיו **חייבות** להמציא שירותי סנכרון זמן כדי לתמוך במעקב ובשחזור של צירי הזמן של הפעילות, במקומות בהם הדבר יידרש.

הנחיית יישום

בנוסף להנחיות הנכללות בתקן ISO/IEC 27002, חשוב לציין כי עיתוי האירועים כפי שהוא נרשם באמצעים אלקטרוניים במידע הבריאות האישי, וברשומות הביקורת, עשוי למלא תפקיד חיוני בהליכים שונים, כגון חקירותיהם של חוקרי מקרי מוות, בחקירות שיתנהלו בחשד למקרים של רשלנות רפואית, ובהליכים משפטיים או דומים אחרים בהם חיוני לקבוע באופן מדויק את סדר ההתרחשויות הקליני של האירועים.

7.8 בקרת גישה

7.8.1 דרישות לביקורת גישה בתחום הבריאות

7.8.1.1 כללי

בקרה

על ארגונים המעבדים מידע בריאות אישי חלה **החובה** לבקר את הגישה למידע דלעיל. באופן כללי, חלה **חובה** על משתמשי מערכות מידע הבריאות לגשת למידע בריאות אישי רק:

(א) כאשר מתקיים קשר של טיפול רפואי בין המשתמש ורשומת המידע (המטופל שמידע הבריאות האישי שלו כפוף לגישה);

(ב) כאשר המשתמש מבצע פעילות בשם המטופל;

(ג) כאשר קיים צורך בנתון ספציפי כדי לתמוך בפעילות זו.

7.8.1.2 מדיניות ביקורת הגישה

<u>בקרה</u>

על ארגונים המעבדים מידע בריאות אישי חלה **החובה** לשמר מדיניות ביקורת גישה השולטת על הגישה לפועל למידע דלעיל.

מדיניות הארגון בנושא ביקורת הגישה **חייבת** להיקבע על בסיס תפקידים מוגדרים מראש עם סמכויות קשורות העולות בקנה אחד עם הצרכים של אותו התפקיד, ובו זמנית מוגבלים אליו.

קיימת **חובה** כי מדיניות ביקורת הגישה, כמרכיב של מדיניות ביטחון המידע הרחבה יותר המתוארת בסעיף משנה 7.2.1, תשקף דרישות מקצועיות, אתיות, חוקיות ואת אלה הקשורות למטופל. בנוסף, תהיה המדיניות **חייבת** לקחת בחשבון את המשימות הננקטות על ידי אנשי המקצוע בתחום הבריאות ואת תזרימי העבודה הרלוונטיים.

<u>הנחיית יישום</u>

בנוסף להנחיות הנכללות בתקן ISO/IEC 27002, חשוב לציין כי על מנת למנוע מאספקת שירותי הבריאות עיכוב או מכשול, קיימות דרישות גבוהות יותר מן המקובל לקיום מדיניות ותהליך ברורים, עם הרשאות קשורות, שיש ביכולתן "לדרוס" את כללי ביקורת הגישה הרגילים בעת מצבי חירום.

מומלץ כי ארגוני שירותי בריאות ישקלו את יישומו של פתרון ניהולי מאוחד לסוגיות הזיהוי והגישה, תוך הכרה ביתרון הנוסף הפוטנציאלי וצמצום הוצאות המנהלה שצעד מעין זה עשוי לתרום למדיניות בקרת הגישה. בנוסף, מהלך מעין זה יתמוך בתהליכי ביטחון גישה ברמה גבוהה יותר, כגון גישה המבוססת על כרטיס חכם ויכולת "כניסה יחידה" למערכות.

7.8.2 ניהול גישת משתמש

7.8.2.1 רישום משתמש

<u>בקרה</u>

הגישה למערכות מידע בריאות המעבדות מידע בריאות אישי תהיה **חייבת** להיות כפופה לתהליך רישום משתמש פורמאלי. נהלי רישום המשתמש יהיו **חייבים** להבטיח כי רמת האימות הנדרשת מזהות המשתמש הנטענת עולה בקנה אחד עם רמת/ות הגישה שתהפוך זמינה למשתמש.

פרטי רישום המשתמש יהיו **חייבים** להיות נתונים לסקירה תקופתית כדי להבטיח כי הם שלמים, מדויקים, וכי הגישה למידע עדיין נדרשת.

<u>הנחיית יישום</u>

בנוסף להנחיות הנכללות בתקן ISO/IEC 27002, חשוב להבין בהקשר זה כי משימת הזיהוי והרישום של משתמשי מערכות מידע הבריאות כוללת את כל המטלות שלהלן:

(א) הרישום המדויק של זיהויו של משתמש (שם מלא, תאריך לידה, וכתובתו המעודכנת);

(ב) הרישום המדויק, לאחר בדיקתו, של הרקע המקצועי המתמשך של משתמש (כגון "ד"ר חיים כהן, קרדיולוג") ו/או של תפקידו (כגון "רות לוי, פקידת קבלה רפואית");

(ג) הקצאת זיהוי משתמש שאינו משתמע לשתי פנים.

יצוין כי מטופלים בדרך כלל אינם משתמשי מערכת, למרות שאלה המסוגלים לגשת למידע האישי שלהם, כולו או חלקו, באמצעים מקוונים, (לדוגמה דרך פורטל אונליין), אכן ייחשבו למשתמשים (על אף שיהיו בעלי גישה מוגבלת). יש לציין גם, כי קיימים יישומי בריאות בהם עשוי המשתמש לחפש עצה ומידע בעלי אופי כללי. בעוד

שבקשה מעין זו לקבלת מידע עשויה להירשם, המשתמש הניגש למידע יוותר אנונימי. אתרי אינטרנט רבים המציעים מידע בדבר הריון, מחלת האיידס או נושאי בריאות אחרים, פועלים בדרך זו. המשתמשים של אתרים מעין אלה בדרך כלל אינם נדרשים להירשם, ולכן הם אינם נכללים בדיון שינוהל להלן. ראה גם 7.5.1.2.

7.8.2.2 ניהול זכויות יתר

מספר אסטרטגיות ביקורת גישה למידע מפורטות להלן, היכולות לסייע באופן משמעותי להבטיח את סודיותו ושלמותו של מידע הבריאות האישי. אסטרטגיות אלה הן:

(א) ביקורת גישה מבוססת תפקיד, הנסמכת על המיומנות המקצועית ועל תפקידיהם של משתמשים הנקבעים במהלך שלב הרישום, ואשר נועדה להגביל את הענקת זכויות היתר רק לאלה הזקוקים להן מכוח תפקיד אחד, או יותר, המוגדר היטב;

(ב) ביקורת גישה מבוססת קבוצות עבודה, המתבססת על הקצאתם של משתמשים לקבוצות עבודה שונות (כגון צוותים קליניים), על מנת לקבוע לאלו רישומים משתמשים אלה זכאים לגשת;

(ג) ביקורת גישה על פי שיקול דעת, המאפשרת למשתמשי מערכות מידע בריאות המחזיקים ביחס לגיטימי למידע הבריאות האישי של מטופל כלשהו (כגון רופא המשפחה), להעניק גישה למשתמשים אחרים אשר להם אין, עד למועד ההוא, יחס מוכר כלשהו למטופל ולמידע הבריאות האישי שלו (כגון רופא מומחה).

<u>הנחיית יישום</u>

בנוסף לעמידה בהנחיות הנכללות בתקן ISO/IEC 27002, חלה **חובה** על מערכות מידע בריאות הכוללות מידע בריאות אישי לתמוך בביקורת גישה מבוססת תפקיד המסוגלת לשייך כל משתמש לתפקיד אחד, או יותר, כמו גם כל תפקיד לפונקציה אחת, או יותר, במערכת.

משתמש במערכת מידע בריאות הכוללת מידע בריאות אישי יהיה **חייב** לגשת לשירותיה של המערכת דלעיל בתפקיד יחיד (לדוגמה, משתמשים שנרשמו ביותר מתפקיד אחד יהיו **חייבים** להגדיר תפקיד אחד יחיד במהלך כל מהלך של גישה למערכת המידע).

מערכות מידע בריאות **חייבות** לקשור בין משתמשים (לרבות אנשי מקצוע בתחום הבריאות, צוותים תומכים ואחרים) לבין רישומי מטופלים, ולאפשר גישה עתידית על בסיס קשר זה.

הנחיות נוספות בנושא ניהול זכויות יתר במגזר שירותי הבריאות ניתן למצוא בתקנים ISO/TS 22600-1, ISO/TS 22600-2.

7.8.2.3 ניהול סיסמת משתמש

לא קיימת בנושא זה הנחייה נוספת לניהול ביטחון המידע במגזר שירותי הבריאות, ואולם מן הראוי לציין כי אילוצי זמן המתרחשים במצבי אספקת שירותי בריאות עלולים להפוך את השימוש היעיל בסיסמאות למסובך ליישום. ארגוני שירותי בריאות רבים שקלו זה מכבר את האימוץ של טכנולוגיות אימות חלופיות כדי להתמודד עם בעיה זו.

7.8.2.4 סקירת זכויות גישת המשתמש למערכת

<u>הנחיית יישום</u>

בנוסף להנחיות הנכללות בתקן ISO/IEC 27002, תשומת לב מיוחדת חייבת להיות מוקדשת לנושא המשתמשים אשר קיימת ציפייה סבירה לגביהם, כי הם יעניקו שירותי רפואה דחופה, שכן הם עשויים להידרש לגשת למידע בריאות אישי בעת מצבי חירום, כאשר מטופל עלול להיות מנוע מלתת את הסכמתו לכך.

7.8.3 תחומי אחריות של המשתמש

<u>הנחיית יישום</u>

בנוסף לעמידה בהנחיות הנכללות בתקן ISO/IEC 27002, חלה **חובה** על ארגונים המעבדים מידע בריאות אישי, בבואם לקבוע את תחומי האחריות של משתמשים, לכבד את הזכויות ואת תחומי האחריות האתיים של אנשי המקצוע במקצועות הבריאות, כמפורט בחוק וכמקובל על חבריהם של ארגוני בריאות מקצועיים.

7.8.4 ביקורת גישה לרשת ולמערכות הפעלה

לא קיימות הנחיות נוספות לניהול ביטחון המידע בתחום הבריאות.

7.8.5 ביקורת גישה ליישומים ולמידע

7.8.5.1 הגבלת גישה למידע

בקרה

על מערכות מידע בריאות המעבדים מידע בריאות אישי חלה **החובה** לאמת משתמשים, **והחובה** לעשות כן באמצעות כלי אימות הכוללים לכל הפחות שני גורמים.

הנחיית יישום

בנוסף להנחיות הנכללות בתקן ISO/IEC 27002, יש להעניק תשומת לב מיוחדת לצעדים הטכניים שעל בסיסם מאומת מטופל באופן בטוח כאשר הוא עצמו ניגש למידע שלו, כולו או חלקו, (באותן מערכות מידע המאפשרות גישה מעין זו). דגש דומה יש לשים לקלות השימוש בצעדים אלה, בייחוד בעבור מטופלים בעלי מוגבלות כזו או אחרת, כמו גם להוראות גישה על ידי מקבלי החלטות חלופיים.

7.8.5.2 בידוד של מערכת רגישה

לא קיימות הנחיות נוספות לניהול ביטחון המידע בתחום הבריאות.

7.8.6 מחשוב נייד ועבודה באמצעות רשת תקשורת

7.8.6.1 מחשוב נייד ותקשורת

הנחיית יישום

בנוסף לעמידה בהנחיות הנכללות בתקן ISO/IEC 27002, חלה **חובה** על ארגונים המעבדים מידע בריאות אישי לנהוג כדלקמן:

(א) להעריך באופן ספציפי את הסיכונים הכרוכים במחשוב נייד בתחום שירותי הבריאות;

(ב) לנסח מדיניות באשר לאמצעי הזהירות בהם יש לנקוט כאשר עושים שימוש במכשירי מחשוב ניידים, לרבות מכשירים אלחוטיים;

(ג) לדרוש מן המשתמשים שלהם בכלי מחשוב ניידים לעמוד במדיניות זו.

כמצוין בתקן ISO/IEC 27702, קשרי רשת ניידים אלחוטיים, למרות היותם דומים לאלה של רשתות מקוונות, נושאים בחובם מספר הבדלים חשובים מן ההיבט של ביטחון המידע. מספר פרוטוקולים של קידוד אלחוטי נמצאים עדיין בשימוש, כגון WEP, למרות חסרונותיהם הברורים ההופכים אותם לבלתי יעילים על פי רוב. יתרה מכך, המידע הנשמר במכשירים ניידים עלול שלא להיות מגובה בכל עת (לדוגמה בגלל רוחב פס מוגבל, או מכיוון שהמכשירים אינם מחוברים בזמנים בהם מתוכננים להתבצע הגיבויים).

7.8.6.2 עבודה באמצעות רשת תקשורת

הנחיית יישום

בנוסף לעמידה בהנחיות הנכללות בתקן ISO/IEC 27002, חלה **חובה** על ארגונים המעבדים מידע בריאות אישי לנהוג כדלקמן:

(א) לנסח מדיניות באשר לאמצעי הזהירות בהם יש לנקוט כאשר עובדים באמצעות רשת תקשורת;

(ב) להבטיח כי משתמשי רשתות תקשורת במגזר שירותי הבריאות מקיימים מדיניות זו הלכה למעשה.

מספר תחומי שיפוט לאומיים (כגון גרמניה) כבר הטילו מגבלות על עבודתם של עובדי מגזר שירותי הבריאות באמצעות רשתות תקשורת.

חשוב לתת את הדעת לכך כי במגזר שירותי הבריאות יכולה עבודה המושתת על רשתות תקשורת לחצות גבולות, ואף להתרחש על גבי מטוסים או אוניות המצויים מחוץ לכל ריבונות לאומית. רופאים כבר מעבירים דרך קבע תמונות או תרשימים באמצעות הדואר האלקטרוני מעבר לגבולות ארצותיהם על מנת לקבל חוות דעת של מומחים.

צוותים בינלאומיים שיעסקו בעתיד בטיפול באסונות טבע, יוכלו להתבסס על מערכות מידע בריאות בתחומי שיפוט שלא יהיו ארצות מושבם הקבוע. יש לקחת בחשבון את ההשלכות החוקיות והאתיות של עבודה בעלת מאפיינים אלה כאשר מתכננים ומיישמים מערכות מידע בתחומי שירותי הבריאות (בייחוד מערכות לאומיות) שניתן יהיה ליישמן באופן זה. ראה גם סעיפי משנה 7.7.7.1, 7.7.8.3.

7.9 רכש, פיתוח ואחזקה של מערכות מידע

7.9.1 דרישות ביטחון ממערכות מידע

לא קיימת הנחייה נוספת בעבור ניהול ביטחון המידע במגזר שירותי הבריאות.

7.9.2 עיבוד נכון ביישומים

7.9.2.1 זיהוי ייחודי של מטופלים

בקרה

חלה **חובה** על מערכות מידע המעבדות מידע בריאות אישי:

(א) להבטיח כי כל מטופל יכול להיות מזוהה באופן ייחודי בתוך המערכת;

(ב) להיות מסוגלת למזג רשומות כפולות או מרובות, אם נקבע כי נוצרו רשומות מרובות שלא במתכוון בעבור אותו המטופל, או במהלכו של מצב חירום רפואי.

הנחיית יישום

הענקת שירותי רפואה דחופה ומצבים אחרים בהם יתכן והזיהוי המתאים של מטופלים לא היה אפשרי, יובילו באופן בלתי נמנע למקרים של רשומות מרובות בעבור אותו המטופל. יכולת כלשהי חייבת להיות קיימת בכל מערכת מידע בריאות כדי למזג מקרים מרובים של רשומות מטופל לכדי רשומה אחת יחידה. צעד זה של מיזוג מחייב נקיטת מירב הזהירות, ולכן הוא דורש לא רק כוח אדם המיומן בסוג זה של תהליך, כי אם גם כלים טכניים שיסייעו לקדם את אינטגרציית המידע מן הרשומות המקוריות לכדי קובץ שלם ומאוחד.

חלה **חובה** על ארגוני שירותי בריאות המעבדים מידע בריאות אישי להבטיח כי מידע אשר ממנו ניתן לגזור זיהוי אישי נשמר אך ורק במקומות בהם נחוץ לעשות זאת, וכי נעשה שימוש נאות בטכניקות מחיקה, אנונימיזציה ופסבדונימיזציה בהיקף המרבי האפשרי, זאת על מנת להקטין למינימום את הסיכון של גילוי שלא במתכוון של מידע אישי.

7.9.2.2 אימות מידע נכנס

לא קיימת הנחייה נוספת בעבור ניהול ביטחון המידע במגזר שירותי הבריאות.

7.9.2.3 ביקורת תהליכי עיבוד פנימיים

לא קיימת הנחייה נוספת בעבור ניהול ביטחון המידע במגזר שירותי הבריאות.

7.9.2.4 שלמות מסרים

לא קיימת הנחייה נוספת בעבור ניהול ביטחון המידע במגזר שירותי הבריאות.

7.9.2.5 אימות מידע יוצא

בקרה

חלה **חובה** על ארגוני שירותי בריאות המעבדים מידע בריאות אישי להמציא מידע מזהה אישי שנועד לסייע לאנשי המקצוע בתחום הבריאות לאשר כי רשומת הבריאות האלקטרונית הנמשכת מן המאגר תואמת את פרטיו של המטופל הנמצא תחת טיפולם.

הנחיית יישום

בנוסף להנחיה הניתנת בתקן ISO/IEC 27002, יש להתחשב במספר גורמים חשובים נוספים. לפני שהם מתבססים על מידע בריאות אישי המסופק על ידי מערכת מידע, **חייבים** אנשי המקצוע בתחום הבריאות להיחשף לכמות מספקת של מידע על מנת שיהיו בטוחים כי המידע שנמשך תואם את המטופל שלהם. ההתאמה בין מטופל לבין רשומה קיימת יכולה להתברר כמשימה כלל לא פשוטה. מערכות מסוימות מדגישות

את היבט הביטחון על ידי הוספת זיהוי באמצעות צילום לכל קובץ מידע של מטופל. דגשים אלה עלולים כשלעצמם ליצור בעיות פרטיות , שכן הם מאפשרים, באופן פוטנציאלי, את גילוי מאפייני פניו של המטופל, כגון גזעו, אשר אינם נכללים כשדות מידע. הדרישות לזיהוי מטופלים ולזמינות המידע בו נעשה שימוש לתמיכה בזיהוי זה עשויות להשתנות ממדינה למדינה. יש **חובה** להפעיל זהירות יתרה בעיצובן של מערכות מידע בריאות כדי להבטיח כי אנשי המקצוע הנעזרים בהן יוכלו לסמוך על כך כי המערכת מעניקה את המידע הנדרש כדי לאשר כי כל רשומה המועלית אכן תואמת לפרט הנמצא בטיפול.

מערכות מידע בריאות **חייבות** לאפשר לבדוק כי תדפיסים הם שלמים (לדוגמה, על ידי ציון המילים "עמוד 3 מתוך 5").

7.9.3 ביקורות קידוד

7.9.3.1 מדיניות בדבר השימוש בביקורת קידוד וניהול מפתחות

<u>הנחיית יישום</u>

בנוסף להנחיה הניתנת בתקן ISO/IEC 27002, ניתן למצוא הנחיות בנושא המדיניות להנפקה והשימוש של אישורים דיגיטליים במגזר שירותי הבריאות ובנושא ניהול מפתחות בתקן ISO 17090-3.

7.9.3.2 ניהול מפתחות

לא קיימת הנחייה נוספת בעבור ניהול ביטחון המידע במגזר שירותי הבריאות.

7.9.4 ביטחון קבצי מערכת

7.9.4.1 ביקורת תוכנה תפעולית

לא קיימת הנחייה נוספת בעבור ניהול ביטחון המידע במגזר שירותי הבריאות.

7.9.4.2 הגנה על נתוני בדיקה של מערכת

בנוסף לעמידה בהנחיות הניתנות בתקן ISO/IEC 27002, על ארגונים המעבדים מידע בריאות אישי חל **איסור** לעשות שימוש במידע בריאות אישי בפועל כבנתוני בדיקה.

7.9.4.3 בקרת גישה לקוד המקור של תוכנית

לא קיימת הנחייה נוספת בעבור ניהול ביטחון המידע במגזר שירותי הבריאות.

7.9.5 ביטחון בתהליכי פיתוח ותמיכה, וניהול פגיעות טכנית

לא קיימת הנחייה נוספת בעבור ניהול ביטחון המידע במגזר שירותי הבריאות.

7.10 ניהול תקרית ביטחון מידע

7.10.1 דיווח על אירועי וחולשות ביטחון מידע

<u>הנחיית יישום</u>

בנוסף לעמידה בהנחיות הניתנות בתקן ISO/IEC 27002, על ארגונים המעבדים מידע בריאות אישי חלה **החובה** להגדיר תחומי אחריות ונהלים בנושא ניהול תקריות ביטחון, על מנת:

(א) להבטיח תגובה מהירה, יעילה ומסודרת לתקריות ביטחון;

(ב) להבטיח כי קיים נתיב הסלמה יעיל לתקריות, כך שניתן יהיה להפעיל את ניהול המשברים וניהול המשכיות הפעילות העסקית בנסיבות הנכונות ובעיתוי הנכון;

(ג) לאסוף ולשמר נתונים הקשורים לתקריות ביטחון כגון נתיבי ביקורת, יומני פעילות וראיות אחרות.

תקריות ביטחון מידע כוללות את ההשחתה, או הגילוי שלא במתכוון, של מידע בריאות אישי, או את אובדן זמינותן של מערכות מידע הבריאות, במקרים בהם אובדן הזמינות פוגם בטיפול הרפואי במטופל, או גורם לאירועים קליניים שליליים.

על ארגונים חלה **החובה** לעדכן את המטופל בכל מקרה בו מידע בריאות אישי נחשף שלא במתכוון.

על ארגונים חלה **החובה** לעדכן את המטופל בכל מקרה בו היעדר הזמינות של מערכות מידע בריאות עלול לפגום בטיפול הרפואי שלהם.

קיימת נטייה בארגוני בריאות להפריד באופן מלאכותי בין תקריות ביטחון מידע לבין סוגי תקריות אחרים, הן בכל הנוגע לטיפול בהן, והן בדיווח על אודותיהן. מתוך הכרה בעובדה כי פריצה למאגר המידע עלולה הייתה להוביל לגניבה של חומרת מחשוב (ובעקבותיה להפרת סודיות), או שהוצתה אש כדי להסוות ניצול לרעה של ציוד מחשוב, או בכך כי שימוש בלתי מזוהה או שגוי במערכת עלול היה להוביל להשלכות קליניות, חלה **חובה** לקיים הערכת ביטחון, בין אם של כלל התקריות בארגון, ובין אם של תקריות מדגמיות אחדות, על מנת שניתן יהיה להעריך לעומק את יעילותן של הבקרות הקיימות ושל הערכת הסיכונים שהובילה ליישומן.

7.10.2 ניהול תקריות ושיפורים

7.10.2.1 אחריות ונהלים

לא קיימת הנחייה נוספת בעבור ניהול ביטחון המידע במגזר שירותי הבריאות.

7.10.2.2 לימוד מתקריות

לא קיימת הנחייה נוספת בעבור ניהול ביטחון המידע במגזר שירותי הבריאות.

7.10.2.3 איסוף ראיות

<u>הנחיית יישום</u>

בנוסף לעמידה בהנחיות הניתנות בתקן ISO/IEC 27002, ארגונים המעבדים מידע בריאות אישי עשויים להידרש לשקול את ההשלכות של איסוף ראיות למטרות קביעת רשלנות מקצועית, ואף עשויים להידרש לשקול דרישות בין-מדינתיות, כאשר מערכות מידע הבריאות הן זמינות מעבר לגבולות מדינתיים.

7.11 היבטי ביטחון מידע של ניהול ההמשכיות העסקית

<u>הנחיית יישום</u>

בנוסף להנחיות הניתנות בתקן ISO/IEC 27002, השיקולים המפורטים להלן הם חשובים במגזר שירותי הבריאות. ניהול ההמשכיות העסקית, הכולל התאוששות מאסונות, זוכה להכרה הולכת וגוברת כדרישה מארגוני שירותי בריאות, והעדיפות לו הוא זוכה ממשיכה להתגבר. כאשר הדבר משקף את דרישות הזמינות הקפדניות הקיימות במגזר שירותי הבריאות, יש לנקוט במאמץ מיוחד בניסוח הסדרי גמישות ויתירות, לא רק בגלל הטכנולוגיה עצמה, כי אם גם למען ההדרכה הצולבת של צוותי הבריאות.

תכנון ההמשכיות העסקית במגזר שירותי הבריאות מאתגר במיוחד בעבור איש המקצוע בתחום ביטחון המידע, שכן יהיה צורך לשלב כל תוכנית באופן נאות עם תוכניות הארגון לטיפול בכשלי אספקת חשמל, ביקורת זיהומים והטיפול במצבי חירום קליניים אחרים. ואכן, הטיפול בכל אחד מאלה צפוי להוביל ישירות לטיפול בתוכנית ההמשכיות העסקית של הארגון, ולו רק כדי להעניק תמיכה רבה יותר מעבר לזו שכבר קיימת. עם זאת, תקריות אחרונות כגון התפרצותה של מחלת SARS הראו, כי תקריות בסדר גודל גדול עלולות לגרום למחסור בכוח אדם, היכול כשלעצמו להגביל את היכולת להפעיל תוכניות להמשכיות עסקיות.

ארגוני שירותי בריאות חייבים להבטיח כי תוכניות ההמשכיות העסקית שלהם כוללות תכנון ניהול משברי בריאות.

כמו כן, נדרשים ארגוני שירותי בריאות לוודא כי התוכניות שהם מפתחים נבדקות על בסיס "פרוגרמאתי." הבדיקות הנכללות בתוכנית זו חייבות להיבנות זו על זו, החל מבדיקה על גבי שולחן העבודה, דרך בדיקה מודולארית ועד לסינתזה של זמני ההתאוששות הצפויים, ועד לחזרות הלכה למעשה, ובהיקף מלא, בסוף התהליך. תוכנית מעין זו היא, לכן, בעלת סיכון נמוך ומציעה שיפור משמעותי ברמת המודעות הכללית בקרב אוכלוסיית המשתמשים שלה.

7.12 ציות

7.12.1 כללי

<u>הנחיית יישום</u>

בנוסף לעמידה בהנחיות הניתנות בתקן ISO/IEC 27002, חלה **חובה** על ארגוני בריאות לנסח תוכנית ביקורת על הציות המטפלת במזור הפעילות השלם, דהיינו לא רק בתהליכים המזהים נושאים, אלא גם סוקרת תוצאות או תקופות, ומחליטה על עדכונים של מערך ניהול ביטחון המידע בארגון.

חלה **חובה** כי תוכניות הביקורת של ארגוני הבריאות יהיו מובנות באופן פורמאלי כדי שהן יכסו את כלל מרכיביו שלך תקן בינלאומי זה, את כלל תחומי הסיכונים, כמו גם את כל הביקורות המיושמות, תוך תקופה מחזורית כוללת של 12 עד 18 חודשים.

בסביבה הכפופה עד מאוד לרגולציה ולביקורת של ארגוני שירותי בריאות רבים, חייב פורום ניהול ביטחון המידע לקבוע לעצמו למטרה את ביסוסה של מסגרת ביקורת ציות מאורגנת, אשר שכבת היסוד שלה תהיה ביקורת עצמית על ידי מפעילי ומנהלי התהליכים השונים. לפיכך, הביקורת של מערך ניהול ביטחון המידע, בשם הפורום לניהול ביטחון המידע, כמו גם ביקורת הפנים, הערכות ביטחון הבקרות וביקורות חוץ חייבים כולם להיות מוגדרים באופן כזה המאפשר לכל רובד לסמוך על הרבדים המצויים תחתיו.

7.12.2 הציות לדרישות חוקיות

7.12.2.1 זיהוי החקיקה הרלוונטית, זכויות קניין רוחני וההגנה על רשומות ארגוניות

לא קיימת הנחייה נוספת בעבור ניהול ביטחון המידע במגזר שירותי הבריאות.

7.12.2.2 הגנה על המידע ופרטיות המידע האישי

<u>בקרה</u>

בנוסף לעמידה בהנחיות הניתנות בתקן ISO/IEC 27002, חלה **חובה** על ארגוני בריאות המעבדים מידע בריאות אישי לנהל את הסכמתם של מטופלים בכל הנוגע למידע האישי שלהם.

בכל מקרה בו הדבר אפשרי, יש **חובה** לקבל את הסכמתו של המטופל לפני שמידע הבריאות האישי שלו נשלח באמצעות דואר אלקטרוני, פקסימיליה, או מדווח בשיחה טלפונית, או נחשף בדרך אחרת לצדדים חיצוניים לארגון שירותי הבריאות.

<u>הנחיית יישום</u>

ההמלצה של מועצת אירופה R (97) 5 *בדבר ההגנה על מידע רפואי*, שטרסבורג, 12 בפברואר 1997, מהווה דוגמה לחקיקה או רגולציה הדורשת הסכמה על אודות מידע ממטופלים. להלן עיקרי נוסח המסמך:

לפני ביצועו של ניתוח גנטי, יש לעדכן את המטופל באשר למטרותיו של הניתוח והסיכוי לממצאים שאינם ניתנים לצפייה מראש.

המטופלים חייבים להיות מעודכנים באשר לממצאים שלא ניתן לחזותם אם:

א. הדבר אינו אסור על פי החקיקה המקומית

ב. האדם עצמו ביקש לקבל לידיו את המידע

ג. המידע אינו צפוי לגרום נזק משמעותי:

1. לבריאותו/ה

2. לקרובי משפחתו בקרבת דם או קרבה רחמית, לחבר של משפחתו/ה החברתית, או לאדם אחר לו יש קשר ישיר לקו הגנטי שלו/ה.

ד. מידע זה הוא בעל חשיבות ישירה למטופל בקשר עם הטיפול או המניעה.

דוגמה אחרת להנחיה מקצועית אתית הדורשת את הסכמת המטופל היא הצהרת הלסינקי של ארגון הבריאות העולמי העוסקת במחקר רפואי בבני אדם.

7.12.2.3 מניעת ניצול לרעה של מידע – ביקורות על מתקני עיבוד ועל הסדרת אמצעי קידוד מידע

לא קיימת הנחייה נוספת בעבור ניהול ביטחון המידע במגזר שירותי הבריאות.

7.12.3. ציות למדיניות ולתקני ביטחון וציות טכני

הנחיית יישום

תשומת לב מיוחדת מוסבת לציות למטרת התפעול הטכני ההדדי (משולב), שכן מערכות מידע בריאות גדולות מורכבות בדרך כלל ממערכות רבות הפועלות באופן משולב אלה עם אלה.

7.2.14 שיקולי ביקורת של מערכות מידע בסביבת שירותי בריאות

לא קיימת הנחייה נוספת בעבור ניהול ביטחון המידע במגזר שירותי הבריאות.

נספח א'

(לידיעה)

איומים על ביטחון מידע הבריאות

האיומים לסודיות, השלמות והזמינות של נכסי מידע הבריאות כוללים את כל אלה המפורטים להלן.

(1) **התחזות על ידי גורמי פנים** (לרבות התחזות על ידי אנשי מקצוע בתחום הבריאות וצוות תמיכה)

ההתחזות על ידי גורמי פנים היא השימוש במערכת על ידי גורמים העושים שימוש בחשבונות שאינם שלהם.

צעד זה כשלעצמו מהווה קריסה של ביטחון הליך אימות המשתמש. מקרים רבים של התחזות על ידי גורמי פנים מתבצעים מן הסיבה השפוטה שהדבר מקל על אנשים לבצע את מלאכתם. לדוגמה, כאשר איש מקצוע אחד מחליף את רעהו בתחנת עבודה וממשיך לעבוד על רשומת מטופל הפעילה כבר, קיימת נטייה חזקה לדלג על חוסר הנוחות הכרוך ביציאה מן המערכת של המשתמש הראשון וכניסתו של המשתמש השני, המחליף אותו במשימתו. עם זאת, התחזות על ידי גורמי פנים מהווה גם מקור להפרות חמורות של סודיות המידע. ואכן, מרבית הפרות הסודיות מבוצעות על ידי גורמים פנימיים בארגון. התחזות על ידי גורמי פנים עלולה להתרחש גם מתוך כוונה לכסות על מקרים בהם נגרמו נזקים.

(2) **התחזות על ידי ספקי שירותים** (לרבות צוותי עובדי קבלן המבצעים עבודות אחזקה, כגון מהנדסי תוכנה, טכנאי חומרה ואחרים העשויים להחזיק במניע לגיטימי *פרו פורמה* לגישתם למערכות ומידע)

ההתחזות על ידי ספקי שירותים מתבטאת בעובדי קבלן העושים שימוש בזכות היתר שלהם לגישה למערכות (לדוגמה בעת בדיקות באתר הפעילות, או תוך כדי תיקון תקלות), כדי להשיג גישה בלתי מורשית למידע. מדובר, למעשה, בהפרה – או לחילופין בכשל – של הסדרי מיקור חוץ בטוחים בארגון. למרות שתופעה זו היא נדירה יותר מאשר התחזות על ידי גורמי פנים, יכולה גם היא להוות מקור להפרות חמורות של סודיותו של מידע הבריאות האישי.

(3) **התחזות על ידי גורמי חוץ** (לרבות פורצי מחשבים)

התחזות על ידי גורמי חוץ מתרחשת כאשר צדדים שלישיים בלתי מורשים זוכים לגישה לנתוני או מקורות המערכת, בין אם תוך התחזות למשתמש מורשה, ובין אם על ידי הפיכה למשתמש מורשה בדרך של מרמה (באמצעות, לדוגמה, מה שמכונה "הנדסה חברתית"). בנוסף לפורצי מחשבים, ההתחזות של גורמי חוץ מבוצעת גם על ידי עיתונאים, חוקרים פרטיים או פורצי מחשבים הפועלים כביכול בשם קבוצות לחץ פוליטיות כאלה ואחרות. ההתחזות על ידי גורמי חוץ מהווה כשל באחת, או יותר, מבקרות הביטחון שלהלן:

(א) זיהוי משתמש;

(ב) אימות משתמש;

(ג) אימות מקור;

(ד) ניהול בקרת גישה וזכויות יתר.

(4) **שימוש בלתי מורשה ביישום מידע בריאות**

זה עשוי להיות מפתיע עד כמה זה פשוט להשיג גישה בלתי מורשית ליישום (אפליקציה) מידע בריאות (לדוגמה, כאשר מטופל ניגש לתחנת עבודה בלתי מאוישת במשרדו של רופא ומעלעל במסך). גם משתמשים מורשים עלולים לבצע פעולות *בלתי* מורשות, כגון שינוי נתונים בזדון. בבריטניה ניסה הד"ר הרולד שיפמן להסתיר את הרצח של עשרות ממטופליו על ידי שינוי הנתונים שהיו שמורים במחשב שלו.

החשיבות הקריטית הנודעת לזיהוי הנכון של מטופלים, ולהתאמה הנכונה בינם לבין רשומות הבריאות שלהם, מובילה ארגוני שירותי בריאות לאסוף מידע זיהוי מפורט על אודות המטופלים המצויים תחת חסותם.

מידע זיהוי זה טומן בחובו פוטנציאל רב לאלה שהיו רוצים לעשות בו שימוש כדי לבצע גניבת זהות, ועל כן יש הכרח לשמור עליו בקפדנות.

בראייה כוללת, השימוש הבלתי מורשה ביישומי מידע הבריאות מהווה כשל של אחד, או יותר, מן הנושאים המפורטים להלן:

(א) ביקורת הגישה של קבוצות עבודה (לדוגמה, על ידי כך שמאפשרים למשתמש גישה לנתוני מטופל עמו הוא אינו מקיים כל קשר לגיטימי);

(ב) בקרת נשיאה באחריות ובקרת הביקורת (לדוגמה, על ידי כך שמאפשרים לצעדים בלתי ראויים להתרחש מבלי שהם יעוררו תגובה);

(ג) ביטחון כוח האדם (לדוגמה, על ידי הענקת הדרכה בלתי מתאימה למשתמשים,

או אי ההבהרה כי גישתם למידע כפופה לביקורת וסקירה).

(5) הכנסת תוכנה מזיקה או משחיתה (לרבות וירוסים, תולעים ו"תוכנה זדונית אחרת)

מרבית תקריות הביטחון הקשורות לטכנולוגיות המידע קשורות בווירוסי מחשבים. ההחדרה של תוכנה מזיקה או משחיתה מהווה כשל בהגנה מפני וירוסים, או בבקרת החלפת תוכנה. בעוד שהם נמצאים בדרך כלל ברשתות מחשבים, הריבוי של תולעי וגם ווירוסי הדואר האלקטרוני, כמו גם הניצול של חולשות תוכנות שרתי המחשבים על ידי פורצי מחשבים, הפכו יחד את הצעדים הנדרשים למניעת החדרתה של תוכנה מזיקה או משחיתה למערכות המידע למסובכים עד מאוד.

(6) ניצול לרעה של מקורות המערכת

איום זה כולל את השימוש של מערכות ושירותי מידע בריאות לצרכי עבודה אישית. משתמשים המורידים מידע מן האינטרנט שאינו קשור לתחום עבודתם למחשבים המיועדים באופן בלעדי לתמיכה במערכות מידע הבריאות, ההקמה של מאגרי מידע על ידי משתמשים, או של יישומים אחרים בנושאים שאינם קשורים לעבודתם, או דוגמאות של משתמשים הפוגעים בזמינותן של מערכות מידע הבריאות על יד כך, לדוגמה, שהם משתמשים ברוחב פס הרשת על מנת להוריד קבצי ווידיאו או שמע לשימושם הפרטי. ניצול לרעה מעין זה מהווה כשל באכיפה של הסכמי שימוש מקובלים, או כשל בחינוכם של משתמשים באשר לחשיבות השמירה על שלמותם וזמינותם של מקורות מידע הבריאות.

(7) הסתננות למערך התקשורת

הסתננות לתקשורת אלקטרונית מתרחשת כאשר יחיד (כגון פורץ מחשבים) מטפל בזרימת המידע הרגילה המתקיימת ברשת תקשורת מסוימת. התוצאה הנפוצה ביותר היא התקפת מניעת שירות (אשר במהלכה שרתים או מקורות רשת מופלים באופן יעיל), ואולם יתכנו גם צורות אחרות של הסתננות לתקשורת (כגון התקפת הילוך חוזר, בה הודעה תקפה אך ישנה נשלחת שוב, באופן בו היא נתפסת כעדכנית). הסתננות לתקשורת מהווה כשל באיתור הפריצה הבלתי מורשית ו/או בבקרות הגישה לרשת, ו/או בניתוח הסיכונים (בייחוד של ניתוח הפגיעות), ו/או כשל של ארכיטקטורת המערכת (החייבת להיות מתוכננת כך שתכלול הגנה מפני התקפות מניעת שירות).

(8) הפרעה לתקשורת

אם המידע אינו עובר קידוד במהלך שידורו, עלולה הסודיות שלו להיות מוסרת על ידי היירוט של התשדורת. מדובר במהלך פשוט יותר ממה שהוא נשמע, שכן כל גורם ברשת מקומית עלול באופן פוטנציאלי להתקין את מה שקרוי "מריח מידע" בתחנת העבודה שלו, ולנטר באמצעותו את מרבית התנועה העוברת ברשת המקומית שלו, לרבות קריאת הודעות דואר אלקטרוני תוך כדי מעברן. כלי פריצה זמינים בקלות יחסית כדי להפוך את מרביתו של תהליך זה לאוטומטי ופשוט למדי. הפרעה לתקשורת מהווה כשל בתקשורת בטוחה.

(9) התכחשות

איום זה כולל משתמשים המכחישים כי הם שלחו הודעה כזו או אחרת (הכחשת המקור), ומשתמשים המכחישים כי הם קיבלו הודעה (הכחשת קבלה). הקביעה שאינה משתמעת לשתי פנים האם מידע בריאות אישי זרם מספק שירות בריאות אחד למשנהו, יכולה להוות מרכיב חיוני בחקירות על חשדות לרשלנות מקצועית. התכחשות יכולה להוות כשל ביישומן של בקרות כגון חתימות דיגיטליות על מרשמים אלקטרוניים (דוגמה להכחשת מקור), או תוצאה של הכשל ליישם בקרות כקבלות קריאה בהודעות דואר אלקטרוני (דוגמה של הכחשת קבלה).

(10) כשל בקיום קשר (לרבות כשלים של רשתות מידע בריאות)

כל הרשתות כפופות לתקופות הפסקת שירות תקופתיות. איכות השירות היא גורם מרכזי באספקת שירותי רשת במגזר שירותי הבריאות. כשל בקיומה של תקשורת יכול לנבוע גם מניהול כושל של שירותי הרשתות (לדוגמה, שינוי בזדון של טבלאות ניתוב הגורם לתנועה ברשת לזרום לכיוון בלתי רצוי). כשלים בקיום קשר עלולים לתרום לגילוי מידע סודי על ידי כך שהם מאלצים את המשתמשים לשלוח הודעות באמצעות מנגנון בטוח פחות, כגון הפקסימיליה או האינטרנט.

(11) הטמעת קוד זדוני

איום זה כולל ווירוסים המופצים באמצעות הודעות דואר אלקטרוני, כמו גם קוד נייד עוין. למרות שהוא כמובן אינו ייחודי בשום דרך למגזר שירותי הבריאות, השימוש הגובר בטכנולוגיות אלחוטיות וניידות על ידי ספקי שירותי בריאות מגביר את הפוטנציאל לנזק הטמון באיום זה. ההטמעה של קוד זדוני מהווה כשל ביישום בקרות בצורת תוכנות אנטי-ווירוס, או ביישום הגנות יעילות מפני פריצה.

(12) הפנייה מוטעית מקרית

איום זה כולל את האפשרות בה מידע יוכל להימסר לכתובת שגויה כאשר הוא נשלח על גבי רשת תקשורת. הפנייה מוטעית מקרית עלולה להוות כשל בהדרכת משתמשים, או לחילופין כשל בשמירה על שלמותם של ספריות הנתונים של ספקי שירותי הריאות (או שניהם).

(13) כשל טכני של המארח, של מתקן האחסון או של תשתית הרשת

איומים אלה כוללים כשלים בחומרה, בפעילות הרשתות או כשלים במתקני אחסון הנתונים. כשלים אלה מהווים בדרך כלל כשל באחת מבקרות ניהול התפעול המפורטות בסעיף 10 של תקן ISO/IEC 27002:2005. למרות שהוא בשום אופן אינו ייחודי למגזר שירותי הבריאות, אובדן הזמינות של מערכות מעין אלה עלול להביא להשלכות מסכנות חיים בעבור מטופלים.

(14) כשל בתמיכה סביבתית (לרבות כשלי מתח חשמלי והפרעות לשירות הנגרמות עקב אסונות טבע או מעשה ידי אדם)

מערכות מידע בריאות יכולות להתגלות כקריטיות בעת אסונות טבע ואירועים אחרים המסכנים את חייהם של אנשים רבים. אותם האסונות עלולים לזרוע להרס במערכות התמיכה הסביבתיות הנחוצות להמשך הפעילות. הערכה נאותה של האיום והסיכון הכרוך במידע הבריאות יכלול הערכה באשר למידה בה אותן המערכות יהיו קריטיות בעתות של אסונות טבע, ועד כמה איתן יהיה התפקוד שלהן תחת תרחישי אסון מעין אלה.

(15) כשל תוכנת מערכת או תוכנת רשת

חולשותיהן של תוכנות מערכות ההפעלה או של תוכנות הרשתות, או תצורתן השגויה, הופכות את התקפות מניעת שירות לפשוטות הרבה יותר. כשל תוכנת מערכת הפעלה או תוכנת רשת מהווה כשל בבדיקת שלמותן של תוכנות, בבקרת בדיקת המערכות, או בבקרת אחזקת תוכנות.

(16) כשל תוכנת אפליקציה

כשלים בתוכנה של אפליקציה יכולים להיות מנוצלים להתקפת מניעת שירות, כמו גם על מנת לסכן את סודיותו של מידע מוגן. כשל בתוכנת אפליקציה מהווה כשל בבדיקת תוכנות, בבקרות החלפות תוכנה, או בבדיקת שלמות התוכנות.

(17) טעות מפעיל

טעויות מפעיל מהוות אחוז קטן אך משמעותי בגילוים שלא במתכוון של מידע סודי, וחלק ניכר מן המחיקות שלא במתכוון של מידע. טעות מפעיל מהווה כשל באחד, או יותר, מן הבאים:

(א) בקרות תפעוליות;

(ב) ביטחון כוח אדם (לרבות הדרכה יעילה);

(ג) התאוששות מאסון (לרבות גיבוי ושחזור נתונים)

(18) טעות אחזקה

טעויות אחזקה הם משגים המבוצעים על ידי אלה הנושאים באחריות לאחזקת מערכות חומרה ותוכנה.

טעויות אחזקה יכולות להיות מבוצעות על ידי צוותי עובדים בארגון, כמו גם על ידי עובדי צדדים שלישיים ששירותיהם נרכשים על מנת שהם יבצעו עבודות אחזקה. מאידך, טעויות מעין אלה עלולות לסכן את סודיותו של מידע מוגן. טעויות תצורה של תוכנה במהלך תהליך ההתקנה הן סיבה נפוצה לפגיעות המנוצלת בשלבים מאוחרים יותר על ידי פורצי מחשבים. טעויות אחזקה מהוות כשל בבקרות אחזקת חומרה, בבקרות אחזקות תוכנה, בבקרות שינויי תוכנה, או בשילוב כזה או אחר בין אלה.

(19) טעות משתמש

טעויות על ידי משתמש עלולות להוביל, לדוגמה, לכך שמידע סודי יישלח לנמען הלא נכון. טעויות משתמש יכולות להוות לעיתים כשל באחד מאלה:

(א) בקרות משתמש (לרבות ממשקי משתמש שנבנו תוך התחשבות במרכיב הביטחון)

(ב) ביטחון כוח אדם (לרבות הדרכה).

(20) מחסור בכוח אדם

האיום של מחסור בכוח אדם כולל את אפשרות היעדרותו של כוח אדם מפתח מן הארגון, ואת הקושי הקיים למלא את מקומו. הפגיעות לאיום זה תלויה בהיקף בו מחסור מעין זה בכוח אדם פוגע בתהליכים העסקיים. במגזר שירותי הבריאות, מגיפה המגבירה באופן ניכר את הדרישה לגישה בזמן למידע בריאות עלולה גם לגרום למחסור בכוח אדם המסכן את זמינותן של אותן מערכות המידע. כשל מסוג זה מהווה כשל בניהול ההמשכיות העסקית (ראה סעיף 14 של ISO/IEC 27002:2005).

(21) גניבה על ידי גורמי פנים

לגורמי פנים יש בדרך כלל גישה נרחבת יותר למידע סודי מאשר לגורמי החוץ, ולכן גורמים אלה מצויים בעמדה עדיפה, המאפשרת להם, לכאורה, לגנוב מידע על מנת למכור, או לגלות אותו, לאחרים. למרות שמדובר באיום נדיר יחסית, איום גניבת המידע על ידי גורמי פנים גובר ביחס ישר למידת פרסומו או חשיבותו של המטופל (כגון ידוען, או ראש מדינה), והוא קטן ביחס ישר לחומרת הענישה הפוטנציאלית הכרוכה בצעד של גניבה מעין זו (כגון אובדן רישיונו של רופא). הגניבה על ידי גורמי פנים מהווה כשל של בקרה אחת מרבות אפשריות, לרבות של בקרות על תפוקות בדפוס, על מסמכים או מדיה, כשל ביטחון פיסי, או כשל בהגנה הפיסית מפני גניבת הציוד.

(22) גניבה על ידי גורמי חוץ (לרבות גניבת ציוד או נתונים)

גניבת נתונים וציוד על ידי גורמי חוץ מהווה בעיה חמורה בבתי חולים מסוימים. הגניבה יכולה לגרום להפרות של סודיות, בין אם המידע הסודי שמור בשרת או במחשב נייד הנגנבים, או מכיוון שהמידע עצמו מהווה מטרה לגניבה. גניבה על ידי גורמי חוץ עלולה להוות כשל בבקרה אחת מרבות, לרבות בבקרות מחשוב נייד, ההעברה הבטוחה של מדיה, טיפול בתקריות, בדיקות ציות או כשל בהגנה הפיסית מפני גניבה.

(23) נזק מכוון על ידי גורמי פנים

נזק הנגרם במתכוון על ידי גורמי פנים כולל מקרים של וונדליזם, ומקרים אחרים בהם נגרם נזק פיסי למערכות טכנולוגיות מידע או לסביבות התמיכה שלהן על ידי אנשים שקיבלו הרשאת גישה. משתמשי מערכות מידע הבריאות הם בדרך כלל אנשי מקצוע מסורים, ונזק הנגרם במתכוון הוא נדיר. נזק מכוון על ידי גורמי פנים מהווה כשל בביטחון משאבי האנוש (ראה סעיף 8 של תקן ISO/IEC 27002:2005).

(24) נזק מכוון על ידי גורמי חוץ

איום הנזק המכוון על ידי גורמי חוץ כולל מעשי וונדליזם, ומקרים אחרים בהם נגרם נזק פיסי למערכות טכנולוגיות מידע או לסביבות התמיכה שלהן על ידי אנשים שלא קיבלו הרשאת גישה למערכות אלה. בעוד שבמרבית המגזרים התעשייתיים צעדים מעין אלה מהווים כשל ביישום נאות של בקרות ביטחון פיסיות, הגישה של מטופלים, חבריהם וקרובי משפחותיהם לאזורים התפעוליים בבתי חולים, קליניקות וארגוני בריאות אחרים עלולים להפוך איומים אלה למסובכים הרבה יותר למניעה מאשר במרבית הסביבות התפעוליות האחרות. יש צורך לבחור וליישם בקפידה את בקרות הביטחון המפורטות בסעיף 9 של תקן

ISO/IEC 27002:2005 על מנת להקטין באופן מרבי את האיומים דלעיל.

(25) טרור

האיום במעשי טרור כולל צעדים של קבוצות קיצוניות המעוניינות להזיק לעבודתם של ארגוני שירותי הבריאות, או להפסיקה, או להזיק לספקי שירותי בריאות, או לחילופין לגרום להשחתת מערכות שירותי הבריאות. למרות העובדה כי טרם אירעו התקפות בהיקף כה ניכר, מומלץ כי מתכננים אכן יתייחסו לאיום הטרור, במיוחד בבואם לתכנן מערכות מידע בריאות גדולות, מאחר שהתקפה על מערכת בסדר גודל כזה תוכל להגביר את יעילותן של התקפות הביו-טרור, ושל התקפות טרור מסוגים אחרים, הגורמות למשבר בתחום שירותי הבריאות.

נספח ב'
(לידיעה)

משימות מערך ניהול ביטחון המידע ומסמכים נלווים

ב.1 משימות הדרושות להקמת מערך ניהול ביטחון המידע והמסמכים הקשורים (שלב התכנון)

		משימות	מסמכים קשורים (דוגמאות)	
תכנן (קביעת מערך ניהול ביטחון המידע)	**שלב 1**	הגדרת טווח התוכנית	מסמך המגדיר את הטווח הישים	
	שלב 2	תכנון מדיניות התוכנית		
עשה (יישום והפעלת מערך הניהול)	**שלב 3**	תכנון גישה שיטתית להערכת סיכונים	מדיניות ביטחון המידע	תרשים מבנה ניהול מערך ביטחון המידע
	שלב 4	זיהוי סיכונים (זיהוי גורמי הסיכון ואת נכסי המידע)		
בדוק (פיקוח וסקירה של מערך ניהול ביטחון המידע)	**שלב 5**	ביצוע הערכת סיכונים (הערכת סיכונים)	נהלים לזיהוי נכסי מידע	גיליון לזיהוי נכסי מידע (מלאי נכסים)
	שלב 6	תכנון טיפול בסיכונים (בחירת בטיפול המתאים בסיכון)	רשימת סיכונים	נהלי הערכת סיכונים
	שלב 7	בחירת יעדי ובקרות ההנהלה	דו"ח הערכת סיכונים	נהלי טיפול בסיכונים
פעל (שמירה על מערך ניהול ביטחון המידע ושיפורו)	**שלב 8**	הכנת תצהיר ישימות	דו"ח טיפול בסיכונים	תוכנית טיפול בסיכונים
	שלב 9	אישור הסיכונים הנותרים ואישור ביצוע למערך ניהול ביטחון המידע	קריטריונים החלים על צעדי ביטחון מידע	תצהיר ישימות

תרשים ב' 1 - משימות להקמת מערך ניהול ביטחון המידע והמסמכים הקשורים

ב' 2 - משימות הדרושות ליישומו והפעלתו של מערך ניהול ביטחון המידע (שלב העשייה)

		משימות	מסמכים קשורים (דוגמאות)		
תכנן (קביעת מערך ניהול ביטחון המידע)	**שלב 1**	ביצוע טיפול בסיכונים	תוכנית לטיפול בסיכונים		
	שלב 2	הקצאת משאבים עסקיים על ידי הדרג הניהולי			
עשה (יישום והפעלת מערך הניהול)	**שלב 3**	שימוש בבקרות (תכנון הנהלים הנדרשים) הלכה למעשה)	תכנון הפעלת מערכת ביטחון מידע	תכנון ההמשכיות העסקית	תכנון ההסברה וההדרכה בנושא ביטחון מידע
	שלב 4	ביצוע החינוך וההדרכה			
בדוק (פיקוח וסקירה של מערך ניהול ביטחון המידע)	**שלב 5**	ניהול התפעול	נהלים הדרושים להסברה והדרכה בנושא ביטחון מידע	נהלים לניהול מסמכי מערך ניהול ביטחון המידע	נהלים אחרים
	שלב 6	ניהול המשאבים העסקיים	דו"ח על ההסברה וההדרכה בנושא ביטחון המידע		
	שלב 7	צעדים להתמודדות עם תקריות ביטחון	דו"ח על תפעול ביטחון המידע		
פעל (שמירה על מערך ניהול ביטחון המידע ושיפורו)			תוכנית לצעדים בהם יש לנקוט במקרה של תקריות ביטחון	דו"ח על צעדים בהם יש לנקוט במקרה של תקרית ביטחון	

תרשים ב' 2 - משימות ליישומו והפעלתו של מערך ניהול ביטחון המידע והמסמכים הקשורים

ב' 3 - משימות הדרושות לפיקוח על מערך ניהול ביטחון המידע ולסקירתו (שלב הבדיקה)

		משימות	מסמכים קשורים (דוגמאות)		
תכנן (קביעת מערך ניהול ביטחון המידע)	**שלב 1**	פיקוח וניטור נהלים ובקרות	נהלים דרושים לביקורת פנים	תוכנית ביקורת פנים	רשימת תיוג לביקורת פנים
	שלב 2	סקירה תקופתית קבועה של מערך ניהול ביטחון המידע			
עשה (יישום והפעלת מערך הניהול)	**שלב 3**	סקירת הנהלה	דו"ח על הסברה והדרכה בנושא ביטחון מידע	דו"ח על תפעול ביטחון מידע	
בדוק (פיקוח וסקירה של מערך ניהול ביטחון המידע)			דו"ח על צעדים בהם יש לנקוט במקרה של תקרית ביטחון	דו"ח על ביקורת פנים	
			נהלים להקמת וועדת תפעול	פרוטוקול ישיבת וועדת תפעול	
פעל (שמירה על מערך ניהול ביטחון המידע ושיפורו)					

תרשים ב' 3 – משימות לפיקוח על מערך ניהול ביטחון המידע ולסקירתו והמסמכים הקשורים

ב' 4 - משימות הדרושות לשימור ושיפור מערך ניהול ביטחון המידע וסקירתו (שלב הפעולה)

		משימות	מסמכים קשורים (דוגמאות)	
תכנן (קביעת מערך ניהול ביטחון המידע)				
עשה (יישום והפעלת מערך הניהול)				
בדוק (פיקוח וסקירה של מערך ניהול ביטחון המידע)				
פעל (שמירה על מערך ניהול ביטחון המידע ושיפורו)	**שלב 1**	ביצוע צעדי שיפור (פעילות תיקון ומניעה)	תוכנית לטיפול בסיכונים	נהלי תיקון ומניעה
	שלב 2	דיווח על הצעדים שננקטו		

תרשים ב' 4 – משימות לשימור ושיפור מערך ניהול ביטחון המידע והמסמכים הקשורים

נספח ג'

(לידיעה)

יתרונות פוטנציאליים ותכונות הנדרשות מכלי תמיכה

ג. 1 יתרונות פוטנציאליים של כלי תמיכה

למרות העובדה כי כלי מאגרי מידע כלל אינם בגדר חובה, הראיות בשטח הוכיחו שוב ושוב כי הם מעניקים יתרונות משמעותיים.

קיימת קשת רחבה של כלים זמינים, בטווח רחב של מחירים – מן הכלי הפשוט והזול ועד ליקר, והיקר עוד יותר. בבואם לשקול את אימוצם של כלים, על ארגוני הבריאות לוודא האם נצבר ניסיון מוצלח בשימוש בהם בקרב גורמים אחרים, תוך שיקול זהיר גם של עלויות ההדרכה והאחזקה הכרוכות בהם, למרות שאלה אינן צפויות להיות משמעותיות יתר על המידה.

ארגוני שירותי בריאות לאומיים ישאפו, ככל הנראה, להשיג מידה מרבית של ציות בעלויות הנמוכות ביותר האפשריות. ברור כי אין צורך כי מאות בתי חולים יערכו את אותו התהליך של הערכת סיכונים. כדי להתמודד עם בעיה זו, פיתח, לצורך הדוגמה, שירות הבריאות הלאומי הבריטי ערכת כלים, בה נכללו מודלים גנריים של סיכונים טיפוסיים בעבור סביבת שירותי בריאות. השימוש המקומי בכלי מתמקד לאחר מכן ביצירתו של פיתרון העולה בקנה אחד עם הנסיבות המקומיות, בעוד שהוא עדיין שומר על ציות עם מודל שעוצב על ידי גורם מכוון מרכזי. גישה דומה אפשר לפתח כלפי שלבי התהליך הנכללים בתקן ISO/IEC 27002.

היתרונות הפוטנציאליים הטמונים בכלי התמיכה הם כדלקמן:

(א) הכנסה ואחזקה פשוטה יותר של נתונים;
(ב) דוחות ותפוקות אחרות בפורמטים שנקבעו מראש;
(ג) בקרת גרסה מפושטת;
(ד) שימוש חוזר מיטבי של נתונים בתוך התהליך;
(ה) עקביות בגישה;
(ו) יכולת שימוש חוזר בנתונים ובתוצאות במהלכים עוקבים;
(ז) יכולת השוואת תוצאות;
(ח) שלמות הגישה;
(ט) אמון של צדדים שלישיים, במיוחד של מבקרים (אנשי ביקורת);
(י) נראות ההשלכות של החלטות;
(יא) תמיכה בקבלת החלטות ובתהליכים ניהוליים אחרים;
(יב) יכולת לבצע חיפושים ושאילתות;
(יג) צמצום משמעותי בהוצאות משאבי האנוש;
(יד) העברה פשוטה יחסית של חומר לממשיכים בתפקיד;

ג. 2 תכונות הנדרשות מכלי תמיכה

התכונות הנדרשות מכלי תמיכה אלה הן:

(א) יצרן בעל מוניטין;
(ב) זמינות התמיכה וההדרכה;
(ג) אחזקת תוכן במקביל לשינויים המבוצעים בתקן;
(ד) אינטגרציה יעילה עם כלי יעילות משרדיים אחרים;
(ה) אינטגרציה יעילה עם מערכת ההפעלה;
(ו) ממשק יעיל ואינטואיטיבי, בדרך כלל גרפי או מבוסס אינטרנט;
(ז) (באופן אידיאלי) היכולת להתאים הן את התוכן והן את התפוקה;
(ח) (באופן אידיאלי) קיום תהליך תמיכה למשתמשים מרובים.

ג. 3 תמיכת כלים בעבור תהליך ISO/IEC 27002

על תמיכת הכלים בעבור תהליך ISO/IEC 27002 יהיה לכלול:

(א) קביעת טווחים והפקת תצהיר הטווח;
(ב) ניתוח פערים ודיווח על ניתוח הפערים;
(ג) הגדרת נכסים ודיווח על מלאי הנכסים;
(ד) הפקת תוכנית שיפור בטוחה, דיווח ורישום יישום הסטאטוס;
(ה) רישום ודיווח תצהיר הישימות;
(ו) הגדרה ודיווח של משאב הביטחון;

מן הראוי לציין כי כל התהליכים דלעיל פועלים הדדית, וכי הם חייבים להיות מסוגלים לפעול ביחד.

ג. 4 כלי תמיכה לתהליך ניתוח הסיכונים

משימת ניתוח וניהול הסיכונים היכולה לקבל תמיכה של הכלים כוללת את כל תהליכי המינימום המוגדרים בסעיף ג. 3 לעיל. עם זאת, הכלים המתקדמים יותר מוסיפים מאפיין אחד, או יותר, מבין הבאים:

(א) תמיכה לספרית מודל הסיכון;
(ב) ספריות נכסים;
(ג) כלי הערכת נכסים;
(ד) תמיכה בעריכת מודלים של תלות;
(ה) קיבוץ נכסים שונים לצורך השגת יעילות בהערכה;
(ו) מיפוי איום/נכס/השלכה לצורך השגת יתר שלמות בעבודת ההערכה;
(ז) הערכת רמות איומים מרובות והערכת פגיעות לצורך עמידה בצרכים שונים;
(ח) ספריות אמצעי נגד;
(ט) פונקצית העדפה;
(י) הערכות עלות וזמנים של השיפורים;
(יא) תמיכה בתיעוד נושא הביטחון;
(יב) פונקציות תמיכה בקבלת החלטות;
(יג) תמיכה בעבודת הביקורת;
(יד) דיווח על טיפול בסיכונים;
(טו) פונקצית "מה אם?"
(יז) דוחות גראפיים.

גם במקרה זה, מן הראוי לציין כי רבים מן התהליכים דלעיל פועלים הדדית וחייבים להיות מסוגלים לפעול יחד.