תקציר הנוהל[1]

המידע והידע בשירותי בריאות כללית (להלן הכללית) הנם נכס המאפשר את פעילות הארגון, שמירה על רמה מקצועית, שירות לקוחות ייחודי ומוניטין.

חוקי המדינה מחייבים אותנו להגן על "מידע רגיש"* ולאבטח אותו.

מדיניות **הגנת המידע בכללית כפי שבאה לידי ביטוי בנוהל זה , מחייבת כל עובד בתחום אחריותו וכל מנהל כלפי העובדים הכפופים לו בכללית, להגן על המידע ולאבטח אותו.

פרוט הנושאים במסמך המדיניות : עקרונות יסוד, רגישות וסיווג המידע, הגדרת אחריות להגנת מידע, שילוב הגנת מידע בכללית, הגנת מידע בתהליכים, תקציב, הוצאת מידע מחוץ לארגון, הגנת מידע בתרבות הארגונית, מהימנות כ"א, שימוש לצרכים פרטיים, חיבור ב"גישה מרחוק", חובת דיווח, דואר אלקטרוני ואינטרנט.

מדיניות הגנת מידע – הנה מסמך פנימי ואין לעשות בו שימוש כלשהו מחוץ לכללית.

---

* "מידע רגיש " – כהגדרתו בחוק הגנת הפרטיות התשמ"א 1981

** ביולי 2009 הוחלט לשנות את השם "אבטחת מידע" ל"הגנת מידע". נוהל זה עודכן בהתאם לשינוי.

אושר ע"י :[2] גדי כהן סמנכ"ל, ראש חטיבת התשתיות והלוגיסטיקה	חתימה :
נכתב ע"י : הממונה על הגנת המידע בכללית, חטיבת התשתיות והלוגיסטיקה	

[1] תקציר הנוהל עודכן ב- 27/10/2009
[2] הגורם המאשר של הנוהל עודכן ב- 27/10/2009

תוכן העניינים

הנושא	עמוד
1. כללי	3
2. מסמכים ישימים	4
3. אחריות וסמכות	5
4. הגדרות ומונחים	7
5. עקרונות	11
6. סיווג מידע	15
7. וועדת אתיקה עליונה להגנת המידע	16
8. תהליכים	17
9. שילוב הגנת המידע בארגון	19

1. כללי

1.1. מבוא[3]

1.1.1. הגנת מידע בארגוני הבריאות במדינת ישראל נדרשת מכורח חוקי ודיני המדינה, ונועדה להגן בעיקר על פרטיות וזכויות האדם וכן של נותני השירותים הבריאותיים, הפיננסיים, הטכנולוגיים והעסקיים במסגרת הארגון. קיימת חשיבות רבה בהגנת מידע כדי לאפשר לגלגלי העשייה לפעול ללא פגיעה בתדמית ובשירות המוגש ללקוחות.

1.1.2. מסמך זה הינו גרסה 4 של המדיניות ומבטל את מסמך המדיניות שהופץ ביוני 2009 ובא במקומו.

1.2. מטרות הנוהל

מטרת מסמך זה הנה להגדיר, לפרט ולהבהיר לכל מנהל/ת ועובד/ת בכללית וחברות בנות, ולכל שותף עסקי את חשיבות אבטחת והגנת המידע בארגון, את מדיניות ההנהלה בנושא זה וכן את נוהלי קיומה על מנת שהמידע על כל היבטיו יהיה אמין, זמין וחסוי .

1.3. חלות[4]

כל עובדי הכללית וחברות הבת.

1.4. מילות מפתח[5]

* אבטחת/הגנת מידע	* סיווג מידע	* רשומה/מסמך
* הרשאה	*תהליך/פרויקט	* הצפנה

[3] סעיף 1.1.1 עודכן ב- 27/10/2009, סעיף 1.1.2 עודכן ב- 17/6/2008 וב- 27/10/2009
[4] עודכן ב- 27/10/2009
[5] עודכן ב- 17/6/2008 וב- 27/10/2009

2. מסמכים ישימים[6]

2.1. הוראות הדין (לרבות חוקים, תקנות ונהלים) אשר עניינם בהגנה על מידע והנוגעים בהגנת הפרטיות, ובכלל זה, אך מבלי לגרוע מכלליות האמור, חוק יסוד : כבוד האדם וחירותו, חוק הגנת הפרטיות, חוק זכויות החולה, חוק המחשבים, וכיוב'.

2.2. תקן מכון התקנים הישראלי להגנת המידע ISO - 27001.

2.3. חוק HIPAA - הגנת מידע בשירותי וארגוני הבריאות בארה"ב.

2.4. תקן משותף להערכת הגנת מידע - Common Criteria.

2.5. תקן PCI - אבטחת מידע בכרטיסי אשראי

[6] סעיף 2.1 עודכן ב 17/6/2008, סעיף 2.2 עודכן ב 17/6/2008 וב- 27/10/2009, סעיפים 2.3 ו- 2.4 עודכנו ב- 27/10/2009

3. אחריות וסמכות

3.1. אחריות כללית[7]

3.1.1. אחריות בסיסית – האחריות לקיום המדיניות והוראת עבודה הגנת המידע מוטלת על כל עובד בתחום אחריותו. עובד המועסק בפיתוח מערכת מידע יפתח את המערכת "פיתוח מאובטח" המותאם לשפת הפיתוח.

3.1.2. אחריות המנהל – כל מנהל בארגון אחראי על קיום מדיניות והוראת המידע הגנת המידע ע"י העובדים הכפופים לו, וכך גם לגבי המידע המצוי באחריותו. מנהל אליו כפופים מפתחי אפליקציה, מתכנני תשתית יוודאו כי אלו הוכשרו לנושאי הגנת מידע.

3.1.3. חובת הדיווח – עובד שגילה כי נגרמה פגיעה בהגנת מידע ידווח למנהלו הישיר ולקצין הביטחון במוסד. שני האחרונים יעבירו דיווח על התקלה לממונה הגנת מידע בכללית.

3.1.4. אחריות לסיווג מידע - האחריות על סיווג המידע בהתאם לרגישותו, חלה על כל מחבר או יוזם המידע, בין אם המידע הוא מידע כתוב, מידע קולי, מידע אלקטרוני, מידע אופטי או כל מידע אחר. סיווג המידע יצוין במקום בולט בכל מופע של עיון במידע.

3.2. אחריות לשילוב אבטחת המידע בארגון[8]

3.2.1. האחריות הכוללת לשילוב הגנת המידע בארגון וביצוע ביקורת על יישום הגנת המידע בארגון חלה על **סמנכ"ל וראש חטיבת תשתיות ולוגיסטיקה**. לשם כך יפעלו ארבעה גורמים :

א. **הממונה על הגנת המידע** - מנחה מקצועי לכלל הארגון. אחראי על פיתוח שיטות הטמעה והדרכה, התווית הוראות עבודה להגנת מידע, בקרה וביקורת על יישום הגנת המידע הכולל. דרישות הגנת מידע בתהליך חדש, שינוי גרסה. קשר בנושא עם גורמים חיצוניים תקשורת מקצועית. הפעלת מרכז לאיתור פגיעה בשלמות זמינות וסודיות המידע (SOC). ניהול משתמשים והרשאות.

ב. **ראש אגף מחשוב ומערכות מידע** - יישום מדיניות, הוראות עבודה ודרישות הגנת מידע במערכות מידע ומערכות משובצות מחשב, קביעת כלי הגנת מידע, הפעלת אמצעי הגנת מידע במערכות. ביקורת על הנושאי הגנת המידע שבאחריותו.

---

[7] סעיפים 3.1.1-3.1.3 עודכנו ב- 17/6/2008 וב- 27/10/2009. סעיף 3.1.4 עודכן ב- 17/6/2008
[8] סעיף 3.2 עודכן ב- 17/6/2008 וב- 27/10/2009

ג. **קצין ביטחון ארצי** - יישום דרישות אבטחה פיזית וקביעת כלי אבטחה פיזיים על המידע, טיפול בעבירות הגנת מידע. ביקורת על הנושאים שבאחריותו.

ד. **סמנכ"ל וראש חטיבת משאבי אנוש** – ביצוע הדרכת והכשרת עובדים, והטמעת הידע בתרבות הארגונית.

3.2.2. בכל מוסד/מחוז/בית חולים/חברת בת, ימונו שלושה **נאמני הגנת מידע** אחד במשרד קצין הביטחון, השני ביחידת מחשוב והשלישי אחראי פמ"א/הדרכה. אלו יסייעו למנהל, בהתאמה לתפקידי קב"ט ארצי, ראש אגף מחשוב וראש אגף פמ"א/הדרכה המפורטים לעיל.

3.2.3. המנהל האדמיניסטרטיבי בכל אתר פיזי שמעליו יש קצין ביטחון (מרפאה/מחלקה בבית חולים/חטיבה/חברת בת/הנהלת מחוז) בארגון ,יפעל לקיום מדיניות זאת בנושאים הללו :

א. ביצוע הגנת מידע במסמכים וניירת.

ב. ניהול סיסמאות עובדיו

ג. כיבוי מחשבים ואבטחת מסמכים בהם מידע "חסוי אישי".

ד. הדרכת עובדיו ב"כללי הגנת המידע לעובד" (נוהל 01-02-08)

3.3. <u>אחריות על שילוב הגנת מידע בתהליך</u>[9]

3.3.1. האחריות על שילוב הגנת מידע בתהליך ויישומה חל על יוזם התהליך או על הרפרנט (אם הוגדר).

3.3.2. כל מנהל אחראי על שילוב הגנת המידע לגבי מידע שבאחריותו.

3.4. <u>אחריות רישום מאגרי מידע</u> [10]

רישום מאגרי מידע כמתחייב מחוקי המדינה הוא באחריות המנהל האחראי על המערכת הכוללת את מאגר המידע. ביצוע הרישום ינוהל ע"י **ממונה הגנת המידע בכללית**.

3.5. <u>סמכות</u>[11]

בסמכות ועדת אתיקה עליונה להגנת מידע לטפל בכל סוג מידע רפואי ממנו ניתן לזהות אדם פלוני ו/או "מידע רגיש" כהגדרתו בחוק הגנת הפרטיות התשמ"א-1981, פרק ב', סעיף 7. החלטות הועדה יפורסמו בחוזר מרוכז כהוראות עבודה מחייבות.

---

[9] סעיף 3.3 עודכן ב- 17/6/2008 וב- 27/10/2009
[10] עודכן ב- 17/6/2008 וב- 27/10/2009
[11] עודכן ב- 17/6/2008 וב- 27/10/2009

4. הגדרות ומונחים

4.1. מידע - כל מידע שנכתב או הודפס, מידע אלקטרוני, מידע קולי, מידע שניתן לצפות בו, מידע משונע, מידע מאוחסן.

4.2. סוג המידע[12] – מידע מודפס ברשומות ומסמכים, מידע במערכות אלקטרוניות, מידע מילולי, מידע חזותי, מידע משונע, מידע מאוחסן.

4.2.1. מידע כתוב – מידע כתוב או מודפס על גבי מצע שאינו מצע אלקטרוני.

4.2.2. רשומות ומסמכים - כל אמצעי עליו ניתן להציג מידע.

4.2.3. מידע אלקטרוני – מידע המופק במערכות משובצות מחשב ומוצג באמצעים אלקטרוניים/תקשורת אלקטרונית.

4.2.4. מידע קולי – מידע המועבר באמצעות קולו של אדם או מכונה אלקטרונית המייצרת קול.

4.2.5. מידע חומרי – מידע שנמצא בתוך מבנה והמבנה משמש מקום לשימוש בו או אחסונו או ציוד מכל סוג שעשוי לחשוף מידע.

4.3. הגנת מידע[13] – מימוש דרישות הגנה על מידע כך שיהיה :

אמין - מידע שלא נעשה בו שינוי מרגע שמחברו סיים כתיבתו או הפקתו.

זמין – המידע נגיש לבעלי תפקידים מתאימים ע"פ צרכי הארגון.

חסוי – מידע שתוכנו לא ייחשף לבלתי מוסמכים.

4.4. סיווג המידע[14] – קביעת רמת הגנת המידע הנדרשת עבור המידע.

4.5. שילוב הגנת מידע[15] – שילוב נהלים ופתרונות טכנולוגיים שמטרתם אבטחת מידע.

4.6. מנהל בארגון – כל עובד אליו כפופים עובדים.

---

[12] סעיף 4.2 עודכן ב- 17/6/2008
[13] סעיף 4.3 עודכן ב- 17/6/2008 וב- 27/10/2009
[14] עודכן ב- 17/6/2008
[15] עודכן ב- 17/6/2008 וב- 27/10/2009

4.7. נאמני הגנת מידע[16] – קצין ביטחון, מנהל יח' מחשוב וממונה פמ"א/הדרכה הם נאמני הגנת מידע בכל מוסד / מחוז / בית חולים / חברת בת.

4.8. המנהל האדמיניסטרטיבי[17] – אחראי על הגנת המידע בתוך אותו מתקן או יחידה ארגונית קטנה מעליה יש קצין ביטחון.

4.9. תהליך[18] - סוג של פעולה ראשונית או פרויקט בתחום : מחשוב, משאבי אנוש, תכנון וארגון, לוגיסטיקה, בינוי תשתיות (ציוד/מכשור רפואי) ובו עשוי להימצא מידע. כך גם לגבי עדכון גרסה, שיפוץ מבנים.

4.10. הרשאה – אישור עקרוני לצפות בסוג מסוים של מידע.

4.11. סוג הרשאה – מקצוע או תפקיד שלנושא אותו אושר לצפות בסוג מידע אחד או יותר בהתאם לדרישות התפקיד ורגישות המידע.

4.12. צמתי מידע – מרכז של מידע רב (רשת וחדרי מחשב, מח' רשומות, מערכות בעלות סגמנטים רבים, ארכיון וכיו"ב).

4.13. ספק חיצוני - כל אדם העובד בכללית או עבור הכללית ואינו עובד הארגון המחויב בתנאי העבודה בארגון (יחסי עובד מעביד).

4.14. מידע רגיש[19] – על פי חוק הגנת הפרטיות התשמ"א 1981

4.14.1. נתונים על אישיותו של אדם, צנעת אישותו, מצב בריאותו, מצבו הכלכלי, דעותיו ואמונתו ;

4.14.2. מידע ששר המשפטים קבע בצו, באישור ועדת החוקה חוק ומשפט של הכנסת, שהוא מידע רגיש.

4.15. "חסוי אישי"[20] – כל פרט מידע או תהליך ממנו ניתן לזהות אדם פלוני ו/או מידע רגיש כהגדרתו בחוק הגנת הפרטיות התשמ"א – 1981.

---

[16] עודכן ב- 27/10/2009
[17] עודכן ב- 27/10/2009
[18] עודכן ב- 17/6/2008
[19] עודכן ב- 17/6/2008

4.16. "תקלה/פגיעה בהגנת מידע"[21] – מצב בו נפגע חיסיון המידע, שלמות המידע, זמינות המידע, וכתוצאה מכך המידע הגיע לבלתי מוסמכים או נפגעה זמינותו ופגעה בשירות לקוחות או חיי אדם.

4.17. "פיתוח מאובטח"[22] – פיתוח אפליקציית מחשב בה שולבו דרישות הגנת המידע ייחודית לשפת הפיתוח.

4.18. "הלבנה"/התאמה[23] – מצב בו עוברת תוכנה/חומרה/מידע בדיקת הגנת מידע בכללית ושולב בה כלי הגנה כדי לקיים את מדיניות הגנת המידע בכללית.

4.19. "שינוי גרסה משמעותי"[24] – גרסה המשנה שינוי מהותי בתהליכי העבודה במערכת או מתממשקת עם מערכות שלא היה ממשק עד כה, או שונו בה חוקי הזדהות והרשאות משתמשים, מנהלי מערכת ותומכים.

4.20. ארוע הגנת מידע משמעותי[25] – מצב בו נפגעה זמינות, אמינות, לחסיון המידע, במעל 50 תחנות עבודה לפחות, 5 מכשירים רפואיים יחד וכל אלו נמשכו מעל 60 דקות רצופות. כך גם במקרה של פגיעה בשלמות המידע, הדבקה בוירוסים לסוגיהם, גנבת מידע.

4.21. הזדהות חזקה חד חד ערכית[26] – תהליך הזדהות הדורש סיסמה חזקה משאר המשתמשים ושלא ניתן יהיה להתכחש לקיומה.

4.22. וירוס מחשב[27] – תוכנת מחשב שחודרת למחשב ללא ידיעת המשתמש, וגורמת על פי רוב לשיבושים ולתקלות שונות בהפעלת המחשב. התוכנה עוברת ממחשב למחשב ומריצה פקודות מחשב זדוניות עד כדי השתלטות מלאה על המחשב ללא ידיעת המשתמש. דוגמאות לשמות של וירוס : וירוס רגיל, וירוס תולעת, וירוס סוס טרויאני.

---

[20] עודכן ב- 17/6/2008
[21] עודכן ב- 17/6/2008 וב- 27/10/2009
[22] עודכן ב- 17/6/2008 וב- 27/10/2009
[23] עודכן ב- 27/10/2009 וב- 27/10/2009
[24] עודכן ב- 27/10/2009
[25] עודכן ב- 27/10/2009
[26] עודכן ב- 27/10/2009
[27] עודכן ב- 27/10/2009

4.23. הצפנה [28] - תהליך מתמטי מחשובי הגורם לשינוי המידע מגלוי ומובן לבלתי מובן לאלו שאינם מורשים לצפות במידע. תהליך ההצפנה מבוצע באמצעות תוכנה יעודית אותה מפעילים גורמי המחשוב בארגון. מידע "חסוי אישי", שנחוץ להוציאו ממערכת המידע בכללית ולהעבירו להתקן חיצוני , יוצפן ע"ג ההתקן הנייד (דיסק און קי מוצפן,הצפנה במחשב נייד).

[28] עודכן ב- 27/10/2009

5. עקרונות יסוד

5.1. מידע ותהליכים המעבדים את המידע יאובטחו על פי מדיניות זו בכל עת ובכל מקום בו הם נמצאים ו/או אמורים להימצא בשליטה ובבעלות הכללית וחברות בנות[29].

5.2. קיום מדיניות זאת הוא תנאי יסודי להמשך העסקתו של כל עובד והפרתו תטופל משמעתית וע"פ החוק.

5.3. מדיניות זו כפופה ומבוססת על הוראות הדין (לרבות חוקים, תקנות ונהלים) אשר עניינם בהגנה על מידע ובכלל זה, אך מבלי לגרוע מכלליות האמור, חוק הגנת הפרטיות, חוק המחשבים, חוק זכויות החולה, תקנות משרד הבריאות, חוק יסוד כבוד האדם וחירותו וכיוב'.[30]

5.4. מידע ומערכות המעבדות את המידע הנמצאים בתחומי הארגון או שנמסרו לספק חיצוני לשם שרות הארגון הם רכוש הארגון וכפופים למדיניות זו.

5.5. שימוש במערכות המידע של הכללית מותנה בהזדהות אישית חד משמעית של המשתמש. גישה מחוץ לארגון למערכות הארגון מותנה בהזדהות חד חד ערכית, הזדהות חזקה של המשתמש והתחנה ממנה הוא מתקשר[31].

5.6. לכל מערכת מידע, חוצת ארגון או מקומית, ימונה רפרנט בהתאמה. הרפרנט אחראי על שילוב דרישות ובקרה של הגנת המידע לפי המדיניות לכל משך מחזור החיים של המערכת[32].

5.7. גישה למידע תהיה מותנית בהרשאות מתאימות הנגזרות מהתפקיד לסקור/ לצפות/ לנהל/ לערוך/ לעבד את המידע.

---

[29] עודכן ב- 17/6/2008 וב- 27/10/2009
[30] עודכן ב- 17/6/2008
[31] עודכן ב- 27/10/2009
[32] עודכן ב- 17/6/2008 וב- 27/10/2009

5.8. הרשאות יוענקו לתפקידים ע"פ הנחיצות בגישה למידע לשם מילוי התפקיד והמידור המתחייב מרגישות המידע. הרשאה תוענק על ידי רפרנט המערכת באישור יוצרי המידע ו/או ועדת האתיקה עליונה להגנת מידע בהנהלה הראשית[33].

5.9. גישה למידע תנוטר ותבוקר באופן פרטני בכדי להבטיח מתן דין וחשבון אישי.

5.10. מידע ישמר **זמין**, **אמין**, **חסוי** ע"פ הנדרש לקיום מטרות ויעדי הכללית.

5.11. כל רשומה, מסמך, מערכת או תהליך המכילים, מעבדים, מעבירים מידע יסווגו ויאובטחו בהתאם לדרישות הסיווג.

5.12. לכל אדם בכללית ומחוץ לכללית מכל שיוך סקטוריאלי, לרבות חברות חיצוניות להם עובדים בכללית, תפתח רשומה במערכת כ"א, זו תשמש בסיס לפתיחת חשבון משתמש ברשת הכללית, ניהול זהויות ושיוך לתפקידים. רשומת המשתמש ותפקידיו יעודכנו כך שישקפו בכל עת מצבו ומעמדו של העובד בארגון[34].

5.13. מערכות מידע לרבות מערכות תקשורת יתוכננו תוך שילוב אפשרות לקבלת מידע מלא על כל הפעילות המתרחשת במערכת. כמו כן, תתוכנן ותשולב אפשרות לקבלת התרעות הגנת מידע, זיהוי כשלים, תהליכי תגובה מיטביים, זיהוי אנומליות. במערכות קיימות ישולב נושא זה בהדרגתיות[35].

5.14. במערכות המידע ישולבו פתרונות שרידות, גיבוי והתאוששות בהתאם לסיווג המידע ו/או החלטת ועדת אתיקה עליונה להגנת מידע. השמדת מידע תבוצע ע"פ הנהלים והתקנות[36].

5.15. בכל תהליך בארגון חוזה התקשרות עם ספקים ויועצים, מכרז, תוכנית בינוי, יציאה ל- R.F.P בין אם התהליך חדש או שינוי גרסה, בהם עשוי להיחשף מידע חסוי או חסוי אישי, או יש מידע שפרטיו עשויים לזהות אדם פלוני, ישולב פרק הגנת מידע. קיום הדרישות בפרק הגנת המידע הינו תנאי לאישור/הפעלת התהליך, מכרז, חוזה

---

[33] עודכן ב- 17/6/2008 וב- 27/10/2009
[34] עודכן ב- 17/6/2008
[35] עודכן ב- 17/6/2008 וב- 27/10/2009
[36] עודכן ב- 17/6/2008 וב- 27/10/2009

התקשרות, אישור בניה. אחריות שילוב פרק הגנת המידע חלה על מנהל הפרוייקט/רפרנט המערכת. כתיבת פרק הגנת המידע – באחריות ממונה אבטחת מידע. כפועל יוצא מדרישות הגנת המידע מטעם הממונה על הגנת המידע, ייכתב בנספח הטכני, פרק הגנת מידע – באחריות ראש אגף מחשוב/מנהל מחשוב במוסד[37] .

5.16. מדיניות זו תתורגם להוראות עבודה להגנת מידע הלכה למעשה שיהוו קווים מנחים לביצוע הגנת המידע בידי הגורמים המבצעים את הגנת המידע עפ"י מדיניות זאת. אלו יכינו נהלי ביצוע בהתאם[38].

5.17. לא ישולב למערכות המידע של הארגון או בבעלות הארגון כל סוג מידע, חומרה, תוכנה, מכשור רפואי שלא עבר "הלבנה" ובדיקה של הגנת מידע. במקרה של מידע או תוכנה או חומרה פרטית-ראה סעיף 8.4 בהמשך[39].

5.18. מידע, בין אם מסמכים או רכיבי זיכרון, יושמד רק בדרך של גריסת פתיתים באופן שלא ניתן לשחזר את המידע או לעשות שימוש ברכיבי הזיכרון[40].

5.19. תקציב הגנת המידע הינו מתקציב הפרוייקט /תחזוקת המערכת[41].

5.20. האינטרנט מהווה סכנה לשלמות, זמינות, סודיות המידע הארגוני. לא יועבר מידע "חסוי" "חסוי אישי" על גבי תשתיות רשת האינטרנט למעט הצגת נתוני אדם לפי הרשאת אותו אדם בלבד, במערכת כללית On Line. תחסם גישה לשירותי האינטרנט המהווים סכנה לשלמות, זמינות וסודיות המידע[42].

5.21. כל ארוע של פגיעה בהגנת המידע יתוחקר כדי לוודא מניעת הישנות מקרים בעתיד. דו"ח הארוע והתחקיר יועבר ליו"ר ועדת אתיקה עליונה להגנת מידע, לידיעת סמנכ"ל וראש חטיבת תשתיות ולוגיסטיקה והממונה על הגנת המידע[43].

---

[37] עודכן ב- 17/6/2008 וב- 27/10/2009
[38] עודכן ב- 17/6/2008 וב- 27/10/2009
[39] עודכן ב- 17/6/2008 וב- 27/10/2009
[40] עודכן ב- 17/6/2008
[41] עודכן ב- 17/6/2008 וב- 27/10/2009
[42] עודכן ב- 17/6/2008
[43] עודכן ב- 17/6/2008 וב- 27/10/2009

5.22. סיכוני הגנת מידע – יבוצע תהליך רציף של סקר סיכונים, הערכת סיכונים. ניהול הסיכונים יבוצע באמצעות מערכת ניהול סיכוני הגנת מידע באחריות הממונה על הגנת המידע בכללית[44].

5.23. פתרונות מחשוב, ישומים חדשים ושינוי גרסה משמעותי המפותחים על ידי או בעבור הכללית יתוכננו ויפותחו באופן שניתן לקיים עץ היררכיה של מנהלי מערכת (ADMIN). תתוכנן שכבת מנהל ראשי (super user) אשר יהיה בעל הרשאות מקסימליות ובעל יכולת לקבוע הרשאות למנהלי מערכת תחתיו. הזדהות והרשאות של משתמשים בעלי הרשאות פריבלגיות, מנהלי מערכת ואנשי IT ותמיכה תהיה הזדהות חזקה וחד חד ערכית משאר משתמשי הארגון.[45]

5.24. בתחילת שנת עבודה תקבע על ידי הממונה על הגנת המידע וראש אגף מחשוב, המלצה לתוכנית עבודה לשנה הנכחית. התוכנית תקבע בהתחשב באישור התקציבי של המועצה המנהלת לנושא המחשוב. תוכנית העבודה תובא לאישור ועדת אתיקה עליונה להגנת מידע.

5.25. מידע אמיתי יימצא רק בשרתי ייצור(production) ובבסיסי נתונים המשרתים את הייצור. בשרתי פיתוח ,בדיקות,הדרכה יעשה שימוש במידע לא אמיתי.

5.26. [46]כל שינוי מהאמור במדיניות הגנת המידע או שינוי ביישום/הגדרות הגנת מידע דורש אישור מראש מטעם הממונה על הגנת המידע. הממונה על הגנת המידע יודיע על כל שינוי כאמור לסמנכ"ל וראש חטיבת תשתיות ולוגיסטיקה.

---

[44] עודכן ב- 17/6/2008 וב- 27/10/2009
[45] עודכן ב- 17/6/2008 וב- 27/10/2009
[46] עודכן ב- 27/10/2009

6. סיווג מידע[47]

6.1. רגישות וסיווג מידע - המידע בארגון מורכב ממידע רפואי אישי של לקוח, מידע רפואי כללי שאינו מזהה לקוח, מידע עסקי, מידע פיננסי, מידע אישי המתייחס לעובד, ומידע אחר. כל יחידת מידע תקוטלג לאחת משלוש רמות סיווג הבאות :

6.1.1. **חסוי אישי** - כל מידע שעשוי לחשוף פרטיו הרפואיים, נתוני כ"א ושכר של אדם פלוני (כמוגדר בחוק הגנת הפרטיות התשמ"א 1981). מידע זה יוגן על פי החוק ובכל האמצעים הסבירים כדי שלא ייחשף לבלתי מורשים[48].

6.1.2. **חסוי** - כל מידע בו נתונים פיננסיים, מידע רפואי כללי, מחקרים רפואיים, מידע עסקי, מידע סטטיסטי וכל מידע שאין הכללית חייבת לחשוף על פי האמור בחוק חופש המידע. ומידע אחר שחשיפתו לבלתי מורשים או פגיעה באמינותו או בזמינותו עלולים להביא נזק חמור לניהול התקין של הכללית, לתדמיתה, או לספק יתרון למתחרה ו/או כל מידע שפגיעה בזמינותו או באמינותו עלולה לגרום לנזק בגוף האדם.

6.1.3. **בלתי מסווג**[49] - מידע שאינו בגדר מידע חסוי אישי ו/או מידע חסוי ארגונית ואשר בחשיפתו לא ייגרם נזק, מכל סוג, לכללית.

6.2. סיווג המידע יצוין במקום בולט לעין – כך שעין אדם תוכל לראותו בנקל בטרם תחל לעיין במידע. (דפי נייר, דפי מידע על גבי צג מחשב, ציוד וכיו"ב). הסיווג יצוין בראש כל דף במסמך, בכל מסך בו צופים במידע, ע"ג ציוד או מתקן שהוא המידע[50].

---

[47] עודכן ב- 17/6/2008
[48] עודכן ב- 17/6/2008
[49] עודכן ב- 17/6/2008
[50] עודכן ב- 17/6/2008

7. ועדת אתיקה עליונה להגנת מידע[51]

7.1. ועדת אתיקה עליונה להגנת מידע נועדה לקבוע קריטריונים של טיפול אחיד ומאובטח במידע הרפואי הרגיש של שרותי בריאות כללית וחברות הבת. הועדה תבסס החלטותיה על מדיניות זו, חוק הגנת הפרטיות התשמ"א-1981 וחוקים הנוגעים לטיפול במידע הרפואי ושמירת סודיות רפואית. כל זאת בהתחשב בצורכי הארגון והדגשים בתוכנית העבודה השנתית[52].

7.2. בסמכות הועדה לטפל בכל סוג מידע רפואי ממנו ניתן לזהות אדם פלוני ו.או "מידע רגיש" כהגדרתו בחוק הגנת הפרטיות התשמ"א-1981, פרק ב', סעיף 7. החלטות הועדה יפורסמו בחוזר מרוכז כהוראות עבודה מחייבות[53].

7.3. הועדה מורכבת מלפחות 12 חברים מכל מגזרי הארגון. יכול יו"ר הועדה לזמן מומחים או יועצים בהתאם לעניין. הרכב הועדה :[54]

7.3.1. **יו"ר הועדה** – ראש אגף תכנון ומדיניות בריאות.

7.3.2. **מזכיר הועדה** - ממונה הגנת מידע בכללית.

7.3.3. **חברי הועדה** – סמנכ"ל וראש חטיבת התשתיות והלוגיסטיקה, ראש אגף מחשוב ומערכות מידע, קצין ביטחון ארצי, נציג חט' בתי חולים, נציג חט' קהילה, נציג חט' לוגיסטיקה, נציג חט' כספים, נציג חטיבת שיווק,נציג אחות ראשית,נציג רופא ראשי,נציג חטיבת משאבי אנוש,נציג בתי חולים, נציג המחוזות, נציג מכל חברת בת,נציג היועץ המשפטי.ממונה הגנת המידע.

7.4. אחריות על כינוס הועדה היא על **מזכיר הועדה**. רשאי המזכיר לכנס את הועדה בנוכחות חלקית של יו"ר הועדה או ממלא מקומו ועוד 6 חברי הועדה. רשאי המזכיר לקבל החלטות בשם הועדה בנושאים שיוגדרו מראש ע"י הועדה.

7.5. **יו"ר ועדת האתיקה** יציג למנכ"ל הכללית דו"ח הערכת מצב אבטחת המידע בארגון אחת לשנה.

---

[51] עודכן ב- 27/10/2009
[52] עודכן ב- 17/6/2008 וב- 27/10/2009
[53] עודכן ב- 27/10/2009
[54] עודכן ב- 17/6/2008 וב- 27/10/2009

8. תהליכים[55]

8.1. כל תהליך, בין אם הוא חדש או שינוי גרסה משמעותי, בארגון או מחוץ לארגון, האמור לשרת את הארגון, וכתוצאה ממנו עשוי להיות מופק או מעובד מידע, יסווג על ידי יוזם התהליך או ע"י הרפרנט (אם הוגדר) אלא אם ועדת אתיקה עליונה קבעה אחרת[56].

8.2. סיווג המידע יכתיב את דרישות הגנת המידע בהתאם לדרישות החוסן (הוראות עבודה להגנת המידע ראה נוהל 02-02-08) ואישור הממונה על הגנת המידע בכללית. דרישות אלו ישולבו בפרק הגנת מידע במסמך האיפיון[57].

8.3. בשלב ייזום מערכת מידע מסוג "חסוי" "חסוי אישי" על יוזם המערכת להקים ועדת אתיקה להרשאות[58].

8.4. תקציב הגנת מידע - תקציב הגנת מידע בתהליך/פרויקט/שינוי גרסה משמעותי/פרויקט רכש/פרויקט בינוי הוא כחלק מתחשיב עלות הפרויקט/תהליך. עלויות תגובה לאירועי הגנת מידע יועמסו על תקציב הפרויקט/תהליך. עלויות הגנת מידע אחרות יתוקצבו במסגרת דרישת תקציב שנתית[59].

8.5. החלת מדיניות הגנה רחבה, דורשת התייחסות מקיפה למספר ממדים בארגון, המכילים מידע ושותפים בהגנתו. ממדים אלה הנם :[60]

8.5.1. אבטחה פיזית על המידע

8.5.2. הגנת מידע במערכות המידע

8.5.3. הגנת מידע במערכות משובצות מחשב/מכשור וציוד רפואי

8.5.4. הגנת מידע בתקשורת

8.5.5. שרידות מידע ומערכות גיבוי

8.5.6. הגנת מידע בתרבות הארגונית

8.5.7. השמדת המידע

---

[55] עודכן ב- 17/6/2008
[56] עודכן ב- 17/6/2008
[57] עודכן ב- 17/6/2008 וב- 27/10/2009
[58] עודכן ב- 17/6/2008
[59] עודכן ב- 27/10/2009
[60] עודכן ב- 17/6/2008 וב- 27/10/2009

8.6. הגנת המידע בתהליכים השונים תתבצע בשבעה שלבים :[61]

שלב	***שלוב הגנת מידע***	***גורם האחראי על הביצוע***
שלב ייזום התהליך	הבנת התהליך, סוג המידע, דרישות סף להגנת המידע וסיווג המידע	היוזם +ממונה הגנת מידע
שלב הגדרת דרישות	קביעת דרישות הגנת מידע ע"פ דרישות החוסן בהתאם לסיווג המידע שנקבע לתהליך והוראות עבודה הממונה על הגנת המידע בכללית. הגדרת התקציב.	האחראי על התהליך באישור הממונה על הגנת המידע
שלב יישום הדרישות	שילוב מענה לדרישות בשלב הפיתוח ו/או הרכישה	גורם מפתח באמצעות ממונה הגנת מידע.
שלב בדיקות	בדיקת חוסן וישימות	גורם מפתח באמצעות ממונה הגנת המידע , צוות QA
שלב הפעלה/ ייצור	אישור היישום	ועדת היגוי להגנת מידע / הממונה על הגנת המידע בכללית
שלב בקרה שוטפת	בקרה על קיום נהלי הגנת המידע אישור הרשאת גישה של משתמש לתהליך	גורם מתפעל רפרנט המערכת.
שלב גריעה	השמדה מבוקרת של מידע ורכיבים אחרים	נאמן הגנת מידע/רפרנט המערכת

[61] עודכן ב- 17/6/2008 וב- 27/10/2009

9. שילוב הגנת מידע בארגון[62]

9.1 הוצאת מידע מחוץ למתקני הכללית[63]

9.1.1 הוצאת מידע המוגדר כחסוי אישי / חסוי / מחוץ למתקני הכללית או ביניהם, מחייב התייחסות מחמירה מהנהוגה בתוך מתקני הכללית. ההתייחסות תפורט בהוראת עבודה להגנת מידע ייחודית לנושא.

9.2 הגנת מידע בתרבות הארגונית[64]

9.2.1 עובד חדש או ספק חיצוני, בתהליך קליטתו או העסקתו, יקבל הדרכת הגנת מידע ויחתום על התחייבות לקיום כל דרישות מדיניות הגנת המידע בארגון ע"פ הנהלים.ההדרכה וההחתמה באחריות גורם משאבי אנוש שקולט את העובד.

9.2.2 עובדי הכללית יעברו הדרכת הגנת מידע אחת לשלש שנים.

9.2.3 הגנת אבטחת מידע תשולב בכל מסגרות ההכשרה במחלקת הדרכה או בכל מסגרות הכשרה מטעם החטיבות בהנהלה הראשית ובתי הספר לסיעוד, או גופים המעבירים הכשרה/לימודים לעובדי הכללית.

9.2.4 סעיף "דרישות הגנת מידע" ישולב בכל מסמך, דרישה או פיתוח הנכתב במסגרת או עבור פרויקט/תהליך.

9.2.5 בכל חוזה התקשרות עם ספק או מכרז ישולב פרק הגנת מידע,באחריות יוזם החוזה או ההתקשרות..

9.2.6 כל אדם העוסק בפיתוח מערכות מידע יוכשר בנושא הגנת המידע כדי שיפתח "פיתוח מאובטח". כל אדם העוסק בתקשורת ותכנון תשתיות יוכשר בנושא הגנת המידע לשם תכנון תשתיות ותקשורת מאובטח.

9.3 מהימנות כ"א

9.3.1 עובדים בצמתי המידע יאושרו לתפקיד רק לאחר אישור מהימנות מתאים מטעם קב"ט ארצי/ קצין ביטחון מחוזי/ מוסדי/ בית חולים/ חברת בת.

9.3.2 עובדי חברות יעוץ חיצוני/ ספקים חיצוניים להם גישה למידע של הכללית המסווג חסוי אישי/חסוי / עסקי יידרשו לאישור מהימנות מטעם קב"ט ארצי, או בא כוחו, טרם תחילת העסקתם.

---

[62] עודכן ב- 17/6/2008 וב- 27/10/2009
[63] עודכן ב- 17/6/2008 וב- 27/10/2009
[64] עודכן ב- 17/6/2008 וב- 27/10/2009

9.3.3. ספק חיצוני אשר לצורך ביצוע עבודתו מחויב להיחשף למידע של הכללית המוגדר כחסוי (אישי או עסקי) יידרש כתנאי להעסקתו, לעמוד בכל דרישות הגנת המידע כך שהמידע הארגוני לא ייחשף לבלתי מורשים[65].

9.4. צרכים פרטיים[66]

9.4.1. השימוש במשאבי המחשב של הארגון לצרכים פרטיים מכל סוג אסור. שילוב חומרה או תוכנה פרטית למערכות המידע אסור.

9.4.2. השימוש בדואר האלקטרוני הארגוני להעברת מסרים פרטיים מסוג: "מכתבי שרשרת", מסרים מטעם ארגונים, כתות, פרסומיים מסחריים שאינם לצרכי עבודה, מסרים שאינם הולמים ועשויים לפגוע בצנעת הפרט ,מסרים שיש בהם דבר הסתה- אסור!

9.4.3. עובד לא יעשה שימוש במידע שהגיע אליו מכורח תפקידו למטרות פרטיות ו/או שאינן לצורך מילוי תפקידו.

9.5. גישה מרחוק[67]

9.5.1. גישה מרחוק למערכות המידע של הכללית דורשת אישור מראש ממספר גורמים:

א. מנהל מוסד/ מחוז/ בית חולים/ ראש חטיבה/ חברת בת.

ב. ראש אגף מחשוב ומערכות מידע או מי מטעמו.

ג. ממונה הגנת מידע בכללית.

9.5.2. כל סוג גישה מרחוק, שמחוץ לארגון, למערכות המידע בארגון או בבעלות הארגון יעבור דרך "מחשב שער" הנמצא באזור מפורז (DMZ) ובתהליך "הזדהות חזק". בכל מקרה לא תתאפשר גישה ישירה לשרת ייצור או מסד נתונים.

9.5.3. ניהול המשתמשים באחריות ממונה על הגנת המידע בכללית.

9.6. דואר אלקטרוני, מערכות העברת מסרים, אינטרנט[68]

9.6.1. מידע "חסוי אישי" יכול להשלח לנמעני רשת הדואר הארגוני בתנאי שכתובת המייל מסתיימת ב- clalit.org.il@.

9.6.2. הודעת דואר אלקטרוני "חסוי אישי" תוצפן.

---

[65] עודכן ב- 27/10/2009
[66] עודכן ב- 17/6/2008 וב- 27/10/2009
[67] עודכן ב- 17/6/2008 וב- 27/10/2009
[68] עודכן ב- 17/6/2008

9.6.3. עובד אינו רשאי לבצע העברה/הפנייה אוטומטית של מסר אלקטרוני לכתובת דואר אלקטרוני, מחוץ לכללית

9.6.4. במערכת הדואר האלקטרוני המרכזית והמוסדית תחסם האפשרות לבצע הפנייה אוטומטית של דואר אלקטרוני מתוך הארגון לכתובת מחוץ לארגון.

9.6.5. מערכות העברת מסרים יכולות לפעול רק בתוך הרשת הארגונית ללא אפשרות להתחבר לגורם מחוץ לרשת הכללית ו/או האינטרנט.

9.6.6. כל אתר אינטרנט של הכללית וחברות בנות, כולל שינויי גרסה באתר, יעברו בדיקות חוסן למניעת פגיעה בזמינות, סודיות ושלמות המידע טרם "עלייתם לאוויר" ולפחות פעם בשנה.

9.7. <u>הלבנת תוכנות/חומרה/מידע</u>[69]

9.7.1. ייתכן מצב בו נדרש לשלב למערכות הארגון תוכנה/חומרה/מידע שלא נרכש/פותח/נוצר בכללית. במקרה זה חובה להעביר מראש את החומרה/תוכנה/מידע ליחידת המחשוב במוסד/מחוז/הנהלה לשם בדיקת הגנת מידע והתאמה לסטנדרט הגנת המידע בכללית לפי מדיניות זאת. כל זאת טרם שילובם במערכות הכללית. כך גם לגבי הורדת קבצים מהאינטרנט ושילובם במערכות הכללית.

[69] עודכן ב- 27/10/2009