

ספטמבר 2014

התחייבות לשמירת סודיות והגנת מידע לעובד בשירותי בריאות כללית

מידע העשוי לזהות לקוח ו/או מצב בריאותו ו/או מצבו הכלכלי הנם בגדר "מידע רגיש" כהגדרתו בחוק הגנת הפרטיות וככזה מחייב זהירות מיוחדת מאת הגורמים אשר להם נגישות למידע זה. כן, מוגדר ככזה, כל מידע עסקי ו/או אחר אשר הגיע לידי העובד במהלך ו/או עקב עבודתו בכללית ואשר אינו בגדר מידע שהוא נחלת הרבים. הפרת חובת סודיות הקבועה בחוק ו/או הפרת חובת סודיות עובד-מעביד עלולה לגרור אחריות אישית ואף פלילית.

לאור מהות מידע זה חלה עליך חובה מיוחדת ומחמירה לשמירת סודיות.

לנוחיותך ומבלי לגרוע מכלליות החובה המוטלת עליך לשמירת סודיות, להלן מפורטים כללי הגנת מידע ב"שירותי בריאות כללית";

בשל רגישות המידע ב"שירותי בריאות כללית" ומתוך כבודו של הלקוח שלנו, הוגדרה ב"כללית" מדיניות הגנת מידע לכל סוג של מידע ולכל מערכת המעבדת מידע. לרבות "נוהל מסירת מידע רגיש" לכל הגורמים בתוך ומחוץ לארגון.

א. הגדרות:

1. שירותים מקוונים / מיוחדים – הינם, כל מסר אלקטרוני לרבות:

- דואר אלקטרוני
- הודעות SMS
- שירותי וידאו באמצעות האינטרנט
- הודעות באמצעות מערכת מסרים באינטרנט ואתרים חברתיים לסוגיהם
- הודעות במשיבון טלפוני
- הודעות טלפוניות אוטומטיות
- הודעות באמצעות פקס
- שיחות וידאו
- אינטרנט

2. מידע "חסוי אישי"

- כל סוג מידע ממנו ניתן לזהות אדם פלוני. ו/או מידע רגיש על פי הגדרתו בחוק הגנת הפרטיות התשמא 1981 כאמור.

3. מדיניות "שולחן נקי"

- מצב בו מבוצעת פעולה שתמנע גישת זרים למידע רגיש/חסוי אישי, בעת שאת/ה עוזב/ת את סביבת עבודתך. באופן הבא:
 - ביצוע פעולת Lock במחשב עליו עבדת.
 - נעילת כל המסמכים בהם מידע רגיש/ חסוי אישי.
 - השלכת פסולת נייר מכל סוג לפח/ שק גריסה. ולא לאשפה הציבורית.
 - נעילת דלתות וחלונות.
 - הפעלת מערכת הזעקה.

- #### **4. פורטל ארגוני – מערכת מידע ארגונית ממנה ניתן להגיע לכל מערכות הארגון ומירב סוגי המידע והנהלים הארגוניים.**

ב. כללי הגנת המידע לעובד

1. מידע בקשר ללקוח יימסר ללקוח עצמו רק לאחר זיהוי ואימות ודאי של פרטיו. (נוהל 08-01-02 בפורטל הארגוני).
2. מידע של לקוח יכול להימסר לאחר, רק אם חתם הלקוח על טופס יפוי כח/ויתור סודיות רפואית ובו פרוט סוג הויתור ו/או לגורמים מוסמכים לקבל מידע על פי חוקים והוראות דין שונות. (נוהל 08-01-02 בפורטל הארגוני).
3. אין להעביר מידע רגיש/מידע עסקי המצוי בידך לאחר, לרבות לצוות במקום עבודתך אלא אם הוא נמסר למטרה לשמה נמסר המידע לך ו/או נחוץ למילוי תפקידך ו/או נחוץ להמשך טיפול בלקוח.
4. העברת מידע של לקוח לגורמים רפואיים באמצעות הטלפון/פקס יתבצע רק לאחר שבוצע אימות ודאי כי מדובר בצוות רפואי וכי בוצע וידוא בדבר בטיחות העברת המידע ליעדו ואכן נמצא כי מטרת העברת המידע הנה המשך טיפול בלקוח ו/או למטרה אחרת המותרת על פי דין ובכפוף להוראות נוהל מסירת מידע רגיש (נוהל 08-01-02 בפורטל הארגוני). חובת ההוכחה חלה על מוסר המידע.

5. שירותים מקוונים

- **פקס**
 - לפני שאתה מעביר מידע בפקס למבוטח בכללית, חובתך לוודא שהמבוטח הסכים מראש ובכתב לקבל את הפקס .
 - חובתך לזהות את המבקש " זיהוי וודאי "
 - לגורמי הממשל ומוסדות ציבור לא יועבר מידע "חסוי אישי " בפקס.
 - בכל מקרה, ולכל גורם לא יועבר בפקס מידע חסוי אישי מעולם הפסיכיאטריה, מידע חסוי אישי מעולם התפתחות הילד, מידע חסוי אישי מעולם גנטיקה, מידע חסוי אישי המעיד על קיום הריון/הפסקת הריון, מידע חסוי אישי מעולם מחלות זיהומיות מסוג : HIV , הפטיטיס, מחלות מין.
- **דואר אלקטרוני – מסירת מידע בדואר אלקטרוני יישלח רק לאלו הרשאים לקבלו על פי דין ובתנאים הללו :**
 - מידע מכל סוג יכול להשלח רק ברשת הדואר האלקטרוני הארגוני, כשהכתובת מסתיימת ב @clalit.org.il .
 - מידע חסוי אישי יכול להשלח ללקוח רק אם הסכים לכך הלקוח מראש ובכתב בעת הצטרפותו לשירותי כללית אונליין או התחייב לכך בכתב בטופס ייעודי המצוי כנספח בנוהל מסירת מידע רגיש, נוהל 08-01-02.
 - אין לשלוח מידע חסוי אישי לרשויות המדינה ומוסדות ציבור אלא רק באמצעות מערכת כספות או שהמסר נחתם בחתימה ותעודה אלקטרונית.
 - מערכת הדואר האלקטרוני הארגוני נועדה לצרכי עבודה ומידע אישי . אין להשתמש בה להעברת מסרים בלתי הולמים, פרסומים, קמפיין מכל סוג, מכתבי שרשרת.
 - חל איסור להעביר מידע פרטי באמצעות פורומים המשווייכים למערכת הדואר האלקטרוני הארגוני.
 - אל תפתח/י הודעת דואר אלקטרוני אם אינך מכיר/ה את השולח. אם השולח מוכר אך נושא ההודעה אינו סביר או הגיוני בעבור השולח, התקשר/י טלפונית לוודא אמיתות ההודעה.
 - בהודעת דואר אלקטרוני שהגיע אליך מחוץ לכללית חל איסור ללחוץ על קישורים מתוך ההודעה או שמופעים בהודעה.
- **הודעות /תזכורות SMS**
 - הודעות ותזכורות SMS יישלחו ללקוח רק אם הסכים לכך הלקוח מראש ובכתב. או באישור הממונה על הגנת המידע בכללית.
- **שיחות ווידאו**
 - חל איסור לבצע מתוך מתקני הכללית שיחות ווידאו מכל סוג לרבות ממכשירי סמארטפון.
 - מותר לבצע שיחות ווידאו ברשת הווידאו הפנימית של הכללית רק עם מנויים שהם עובדי הכללית.
- **אינטרנט**
 - הגלישה באינטרנט מיועדת לצורכי עבודה והעשרה מקצועית בלבד.

הממונה על הגנת המידע

6. חל איסור חד משמעי לצלם פעולות רפואיות, או לצלם במתקני הכללית צילום ממנו ניתן לזהות פנים או פרטי אדם פלוני. אלא אם נתן אותו אדם הסכמתו מראש ובכתב.
7. אין להעלות/להעביר לאתרי אינטרנט מידע ממנו ניתן לזהות פרטי אדם פלוני. אלא אם נתן האדם הסכמתו מראש ובכתב.
8. אין להעלות לאתרי אינטרנט מידע משירותי בריאות כללית אלא באישורי דוברת שירותי בריאות כללית מראש.

9. " שולחן נקי "

- א. בעוזבך את סביבת המחשב עליו עבדת, חובתך לבצע פעולה של ניתוק (Lock) כך שעבודה מחודשת בו תחייב הקשת סיסמאת כניסה.
 - ב. בעוזבך את סביבת עבודתך חלה עליך חובה לנעול את כל המסמכים בהם מצוי מידע רגיש/ חסוי אישי, כך שלזרים לא תהא גישה למידע.
 - ג. מסמכים שאין בהם שימוש יושלכו לפח /שק גריסה (שק אדום) ולא יושלכו לאשפה הציבורית
 - ד. בעוזבך את סביבת עבודתך עליך לנעול את החדר בו פעלת ולנעול חלונות.
10. בעת שאת/ה משוחח/ת עם לקוח בנושאים רפואיים שמור/י על פרטיות מלאה מהסובבים אותך.
 11. כניסה למערכת מחשב מותרת רק באמצעות **סיסמא אישית הידועה רק לך**. אין למסרה לאחר. בעת קבלת סיסמא בפעם הראשונה עליך להחליפה כך שתהא ידועה רק לך. עליה להיות קשה לזיהוי. אם סיסמתך נתגלתה לאחר, יש להחליפה. אין סיבה או צורך להעביר את סיסמתך לאחר. גם לא לאנשי המחשב.
 12. יובהר כי עשיית שימוש בסיסמא אישית שלך על ידי מאן דהוא עלולה לחייב אותך אישית באחריות לביצוע פעולותיו של אותו מאן דהוא באמצעות סיסמתך.
 13. אין לשלב למערכות הממוחשבות חומרה או תוכנה פרטית, אין לבצע שינוי כלשהו בהגדרות המחשב. אין לשלב אמצעי שידור אלחוטיים. לרבות שימוש בסמארטפון ודומיו, כנתב אלחוטי למערכות המידע של הכללית.
 14. אם לצורך עבודתך נחוץ להוציא מחוץ ל"כללית" מסמכים או מחשב או מידע צרוב על אמצעי אחסון נייד, יש לנקוט באמצעי ביטחון לשמירת המידע על פי הנחיית הגנת המידע ב"כללית" וכפי שיעודכנו מעת לעת. מידע בקשר ללקוח ו/ או מידע רגיש יוצפן. אם המידע אינו מוצפן עליו להיות תחת השגחה של מחזיק המידע כל העת.
 15. על גבי מכשירי טלפון חכמים (סמארטפון) ומכשירי טאבלט ומחשב נייד לא יישמר מידע משירותי בריאות כללית.
 16. אין לחבר מכשירי סמארטפון ודומיו בכבל תקשורת או כבל סינכרון או כבל טעינה למערכות הכללית.
 17. חל איסור חד משמעי להשאיר מחשב או מידע רגיש/ חסוי אישי ברכב ללא השגחה.
 18. כל סוג תוכנה או חומרה השייך ל"כללית" יסומן וירשם טרם הוצאתו מכתלי ה"כללית".
 19. העברת מידע מכל סוג לגורם חיצוני מחוץ ל"כללית" מחייב עמידה בהנחיות הגנת המידע מטעם הממונה על הגנת המידע ב"כללית".
 20. חיבור מערכת ממוחשבת לגורמים מחוץ ל"כללית" דורש אישור מהממונה עליך, ממנהל המוסד/ מחוז, ראש אגף המחשוב וממונה הגנת המידע ב"כללית". כולם יחד ומראש.
 21. בכל תהליך חדש שיש בו מידע ממנו ניתן לזהות אדם פלוני, חובה לוודא שיש לכך אישור מטעם הממונה על הגנת המידע בכללית.

22. בכל הסכם / חוזה, לרבות התקשרות עם ספק או חתימה על חוזה התקשרות עם ספק בו עלול להיות מועבר מידע או שבו עלולה להיות לספק נגישות למידע, חובתך לשלב נספח שמירת סודות והגנת מידע מטעם הממונה על הגנת המידע בכללית.
23. מחשבי הכללית ומערכות המידע הינם רכוש הכללית. נקבעו בהם הגדרות אבטחת מידע. חל עליך איסור חד משמעי לבצע שינוי בהגדרות אבטחת המידע או לחבר אליהם ציוד מחשבי ואלחוטי שאינו של הכללית.
24. טכנאים/ אנשי אחזקה/ ספקים חיצוניים העובדים ע"ג ציוד או במתקן שיש בו מידע "חסי אישי" ו/או "חסי" מחייב ליווי צמוד של האחראי על הציוד או איש צוות במתקן בו נמצא הציוד.
25. חל איסור לעשות שימוש במידע שהגיע אליך בעבודה למטרות שאינן עבודתך ותפקידך הישיר. גם אם אלו נתבקשו על ידי עמית לעבודה שאינו ראוי לראות או לדעת את המידע
26. במקרה של גישה מרחוק למשאבי המידע ב"כללית" ידוע לך כי עליך לוודא שאיש מלבדך אינו צופה/ מעיין במידע שאושר לגישה עבורך.
27. אם גורם כלשהו, שאינו עובד בשירותי בריאות כללית, רוצה לחבר /לשלב למערכות המידע של הכללית מחשב, תוכנה, חומרה, ציוד ומכשור רפואי. חובתך לבקש לכך אישור מראש מטעם הממונה על הגנת המידע בכללית.
28. עם סיום עבודתך ב"כללית" ו/או עבור ה"כללית" חלה עליך חובה להעביר לרשות הגורם המוסמך ב"כללית" כל סוג של מידע ו/ או מדיה מגנטית עליו נאגר מידע ו/או כיו"ב אמצעים לאגור מידע רגיש כאמור.
29. באם חוקים ונהלים אינם מאפשרים העברת מידע ללקוח, תודיע/י ללקוח כי הנך מוגבל/ת על פי החוק.
30. במקרה של אובדן או גנבה של מסמך או מחשב או אמצעי זיכרון ניד או כל פגיעה בהגנת מידע יש לדווח מיד לממונה עליך ולקצין הביטחון.
31. אני מאשר שהובא לידיעתי כי הכללית מפעילה מערכת בקרת משתמש ומערכות המידע של שירותי בריאות כללית מנוטרות כל העת. כמו כן ידוע לי שתיבת הדואר האלקטרוני המשוייכת אלי הינה תיבה מוגנת ואין אישור לאיש לראות את המידע בה ללא אישורי המפורש אלא אם ארע אירוע שמבחינה חוקית מאפשר לארגון גישה למידע.
32. בעבודתי בכללית או על גבי מערכות המידע של הכללית, ידוע לי והנני מסכים כי חל עלי איסור להכנס/לגשת למידע של אדם פלוני אלא עם הפעולה היא לצורך מילוי תפקידי. ידוע לי כי בהפר איסור זה הרי שמדובר בעבירה משמעתית אשר בנסיבות מסוימות עלולה להחשב גם כעבירה פלילית, על כל המשתמש מכך.
33. הנני מתחייב לפעול לכך, שכל פעולה שונה מהאמור בהוראות מסמך זה מחייבת קבלת אישור מראש מטעם הממונה על הגנת המידע ב"כללית".

הנני לאשר כי קראתי והבנתי את הכללים המנויים לעיל והנני מתחייב לנהוג על פיהם ועל פי כל הנחיה לאמצעי אבטחה כפי שתועבר לי על ידי גורם מוסמך בכללית מעת לעת. כן הנני מצהיר כי ידוע לי כי הפרת כללי אבטחת מידע על פי הקבוע בחוק עלולה לגרור עמה אחריות אישית ופלילית. כן ידוע לי כי חלה עלי חובת שמירת סודיות המידע ללא הגבלת זמן.

שם ומשפחה _____ ת"ז _____ תאריך _____ חתימה _____

** שם ספק _____ שם הפרויקט בכללית _____

** מיועד עבור עובד שאינו עובד של שירותי בריאות כללית אלא עובד מטעם ספק חיצוני / יועץ חיצוני