הרצליה
מדיקל
סנטר

נוהל, הצהרה והנחיות אבטחת מידע לרופא

1.בללי

1.1 עובדי בית החולים עלולים להיחשף במהלך ביצוע תפקידם למידע חסוי ומידע חסוי ביותר. מידע זה כולל: כל מידע עסקי, מידע פיננסי מידע על לקוחות, מידע אישי על עובדי בית החולים וכל מידע אחר שיוגדר כחסוי.

1.2 כל מידע חסוי וחסוי ביותר אליו תחשפו במהלך עבודתכם בבית החולים, מחויב להיות מוגן על פי נהלי ה*תיאור הארגון ועל פי "חוק הגנת הפרטיות".

1.3 מודגש בזאת כי סודיותו של מידע חסוי וחסוי ביותר אליו תחשפו במהלך עבודתכם בבית החולים חייבת להישמר.

2.עקרון האחריות האישית

2.1 כל עובד בית החולים אחראי באופן אישי לאבטחת המידע אליו הוא נחשף במהלך עבודתו. על העובד לנקוט בכל האמצעים העומדים לרשותו על מנת להגן על מידע זה.

3.שמירת סודיות

3.1 כל עובדי בית החולים מחויבים לשמור על סודיות המידע והנתונים אליהם הם נחשפים במהלך עבודתם.

3.2 חל איסור לשתף גורם שאינו מורשה במידע חסוי וחסוי ביותר הקשור לעבודה בבית החולים (כולל שיתוף עמיתים לעבודה אשר המידע אינו רלוונטי לעבודתם).

3.3 תוקפו של ההסכם באשר למידע עסקי – 7 שנים מתום ההעסקה.

3.4 תוקפו של ההסכם באשר למידע אישי – ללא תפוגה.

4.מסירת מידע חסוי

4.1 בכלל חל איסור להוציא ו/או למסור מידע חסוי מחוץ לבית החולים.

4.2 במידה ונדרשת העברת מידע חסוי הדבר יעשה בהתאם לנוהל א.8.2 'סיווג, מיפוי וטיפול במידע ונכסי מידע' בלבד.

5.הוצאת מידע מבית החולים

5.2 חל איסור חמור להוציא מידע חסוי וחסוי ביותר מבית החולים למעט במקרים הנדרשים ושאושרו ע"י המנהל הישיר וצרכי העבודה מחייבים זאת.

5.3 אין להוציא מצעי מידע המכילים מידע חסוי וחסוי ביותר אל מחוץ לכותלי בית החולים, אלא באישור מיוחד של המנהל הישיר ובתיאום עם ממונה אבטחת מידע, כמו כן אין להעביר מידע לגורמים חיצוניים אלא באישור הממונה אבטחת מידע והמנהל הישיר.

5.4 בכל מקרה של הוצאת מידע ינקטו כל האמצעים הנדרשים לאבטח את המידע מחוץ למשרד.

6.התקנת תוכנות

6.1 חל איסור מוחלט להתקין במחשבי בית החולים תוכנות. כל תוכנה תותקן על המחשב ע"י צוות המחשוב בלבד ולאחר שאושרה בהיבטי מחשוב ואבטחת מידע. לא יאושרו תוכנות העלולות לפגוע בתפקוד המחשב, תפקוד רשת בית החולים או לחשוף מידע חסוי או חסוי ביותר של בית החולים.

6.2 בכל מקרה של צורך בתוכנה חדשה, יש לפנות לצוות המחשוב על ידי פתיחת קריאת שירות במערכת ולבצע את הרכישה וההתקנה באמצעותה.

מחוייבים אישית לבריאות שלך

נוהל, הצהרה והנחיות אבטחת מידע לרופא

7.שם משתמש וסיסמא

7.1 שם המשתמש הוא אישי ונועד לשימושו של המשתמש בלבד ולצורך ביצוע עבודתו.
הסיסמא מהווה מפתח גישה למידע רגיש ביותר ולמערכות, ולפיכך עליה להיות אישית וסודית.

7.2 חל איסור למסור את שם המשתמש והסיסמא שלך לאדם אחר או להשתמש בשם משתמש וסיסמא של עובד אחר במהלך עבודתך.

7.3 חל איסור על שמירת הסיסמא במקום בו היא עלולה להיחשף.

7.4 בכל מקרה של חשיפת הסיסמא או חשד לחשיפתה, יש להחליף את הסיסמא מידית ולדווח לממונה אבטחת מידע על המקרה.

8.עזיבת עמדת העבודה

8.1 משתמש העוזב את עמדתו ינעל את מחשבו (CTRL+Alt+Delete).

8.2 בתום יום העבודה יבוצע תהליך סיום עבודה מסודר הכולל יציאה מכל המערכות וכיבוי של תחנת העבודה.

8.3 יש להקפיד על קיום מדיניות "שולחן נקי", הכוללת ניקוי שולחן העבודה מכל ניירת או מדיה בסיווג "חסוי" או "חסוי ביותר".

8.4 יש להקפיד לאחסן כל נייר או מדיה המכילים מידע "חסוי" או "חסוי ביותר" במיקום מאובטח (ארון נעול, מגירה נעולה או כספת) בתום יום העבודה או בעת עזיבת העמדה.

8.5 יש לוודא כי לגורמים שאינם מוסמכים (עמיתים לעבודה, אורחים, ספקים, קהל), לא תהיה גישה לחומרים בסיווג חסוי או חסוי ביותר.

8.6 יש לגרוס כל נייר משרדי שאין בו עוד צורך ובפרט מידע חסוי ביותר ומידע חסוי.

8.7 ניירת שאינה מכילה מידע חסוי או מידע בכלל תיגרס גם כן ע"מ למנוע טעויות.

9.שימוש באינטרנט

9.1 חל איסור להעביר מידע שהינו חסוי וחסוי ביותר באמצעות היישומים השונים שברשת האינטרנט, אלא עפ"י הנחיות הממונה אבטחת מידע בבית החולים.

9.2 אין לבצע הורדת קבצים מרשת האינטרנט. אישור חריג להורדת קבצים, יינתן רק לפי צורך הכרחי וחיוני, ובאישור מנהלת תשתיות.

9.3 יש להימנע ממסירת פרטים אישיים וחל איסור למסור את כתובת האימייל של מקום העבודה בעת רישום לאתרי אינטרנט, למעט רישום לאתרים הקשורים לעבודה.

10.שימוש נאות בציוד המשרד

10.1 חל איסור לבצע בציוד המחשוב של בית החולים כל פעילות החורגת ממסגרת התפקיד.

10.2 חל איסור לבצע שימוש פרטי בציוד המחשוב של בית החולים.

10.3 חל איסור לחבר או להכנים מדיה מגנטית פרטית או של גורם חיצוני למחשבי המשרד (דיסק און קי, HD , DVD , CD חיצוני וכו').

10.4 חל איסור לחבר טלפונים סלולריים למחשבי בית החולים.

10.5 חל איסור להפסיק את פעולת המערכות לאבטחת מידע כגון אנטי וירוס.

10.6 על כל מחשב נייד עליו שמור מידע של בית החולים, תותקן תוכנת הגנת והצפנת מידע המאושרים ע"י מנהל תשתיות והמשתמש יקבל תדריך בנוגע לסיכונים הייחודיים למחשבים ניידים

10.7 חל איסור לשנות את הגדרות המחשב.

מחוייבים אישית לבריאות שלך

נוהל, הצהרה והנחיות אבטחת מידע לרופא

11.שימושים אסורים בתקשורת אלקטרונית

11.1 השימוש במשאבי המידע של בית החולים, כולל תקשורת אלקטרונית, מיועדים לצרכי עבודה בלבד.

11.2 חל איסור על הצגה מוטעית, טשטוש, הסתרה או החלפה של זהות משתמש או מערכת תקשורת אלקטרונית.

11.3 שם המשתמש, כתובת הדואר האלקטרוני והמידע הכלול במסרים אלקטרוניים או הודעות חייבים לשקף את המחבר בפועל של המסרים או ההודעות.

11.4 חל איסור על קריאה, חטיפה או חשיפה של תקשורת אלקטרונית של עובד אחר ללא רשות מאותו עובד.

11.5 חל איסור על העברת דואר אלקטרוני באופן אוטומטי (עקוב אחרי) לדואר אלקטרוני מחוץ לבית החולים.

11.6 חל איסור מפורש על שימוש בתקשורת האלקטרונית לכל אחת מהמטרות הבאות:

11.6.1. עיסוק בפלילים.

11.6.2. פעילות בלתי מורשית להשגת כסף או הפעלת עסק פרטי.

11.6.3. גישה לאחת ממערכות המחשב של בית החולים או כל ארגון או גוף אחרים, ללא אישור מתאים.

11.6.4. הפצת מכתבי שרשרת, דואר זבל אלקטרוני או התכתבות דומה.

11.6.5. העברת מסרים מטרידים.

11.6.6. הפצה, צפייה, הורדה, אחסנה או העברה הלאה של תכנים נושאי אופי מיני או מידע אחר העשוי להוות עלבון, כולל חילול הקודש, בדיחות גסות, חומר שיש בו משום השפלה, ביזוי, אפליה או הטרדה של קבוצה כלשהי (דהיינו, כל חומר הנוגד את הערכים וההנחיות של בית החולים).

11.6.7. הורדה או אחסון של חומר (כולל תוכנה) המוגן בזכויות יוצרים ללא רישיון חוקי.

11.6.8. הפצת מסמכים פנימיים של בית החולים או סוגי תקשורת אחרים מחוץ לבית החולים ללא אישור מתאים.

11.6.9. העברת מידע המוגן על פי חוק הגנת הפרטיות.

11.6.10. הפצה ביודעין של מידע לא מדויק.

11.6.11. עיסוק בפוליטיקה.

11.6.12. מידע חסוי המוגן על פי חוקי מדינת ישראל.

12.שימוש במדפסות ובמכשירי פקס

12.1 העובד אחראי לאסוף את החומר מהמדפסת מיד לאחר שליחתו להדפסה, על מנת לוודא כי החומר המודפס לא יילקח על ידי גורם לא מורשה.

12.2 במקרה של מכשיר פקס מרכזי, הנמצא בשטח ציבורי, יש להשגיח שהחומר הנכנס או היוצא לא יילקח על ידי אדם אחר.

13.אבטחה פיזית

13.1 יש להקפיד כי גורמים שאינם מורשים או אינם מוכרים לא יכנסו אל שטחי אתרי בית החולים.

13.2 יש לנעול את דלת המשרד בסוף יום עבודה.

13.3 בכל מקרה בו מזהה העובד גורמים שאינם מוכרים לו או מתנהלים בצורה חשודה באזורי העבודה השונים, יש לוודא את זהות הגורם וללוות לנקודה אליה צריך להגיע. בכל חשד לפעילות לא חוקית, יש לדווח מידית למנהל הישיר ולממונה ביטחון.

מחוייבים אישית לבריאות שלך

נוהל, הצהרה והנחיות אבטחת מידע לרופא

14.דיווח על אירועי אבטחת מידע

14.1 עובד המזהה אירוע / בעיית אבטחת מידע ידווח עליו באופן מידי לממונה אבטחת מידע בבית החולים.

14.2 סוגי אירועים עליהם יש לדווח:

14.1.1. עבירות אבטחת מידע הנעשות ע"י העובד/ת עצמו/ה ו/או עובדים אחרים.

14.1.2. חשד לפריצות אבטחת מידע במערכות השונות ובמחשב האישי.

14.1.3. חשד בלשהו כי המידע האגור במערכות נפגע (נמחק/ שונה /נחשף).

14.1.4. חשד של עובד/ת כי נעשה שימוש לא מורשה בזיהוי המשתמש שלו.

הרצליה מדיקל סנטר רח' רמת ים 7, הרצליה, 4685107 **Herzliya Medical Center** 7 Ramat Yam St., Herzliya, Israel | טלפון. 9599* Tel.+972.9.9592555 Web. www.hmc.co.il
מרכז המומחים של הרצליה מדיקל סנטר רח' החושלים 8, הרצליה, 4672408 **HMC Experts** 8 Hahoshlim St., Herzliya, Israel | Email. information@hmc.co.il www.hmcisrael.com