

לכבוד,
אמיר שי
מנהל תחום תשתיות וטכנולוגיות תקשוב
והממונה על הגנת הסייבר
משרד הבריאות

**הנדון: חוזר המנהל הכללי מיום 15 לפברואר 2015 מס' 3/15
"הגנה על מידע במערכות ממוחשבות במערכת הבריאות"**

בנוגע לחוזר שבנדון שפורסם על ידכם, ולאור חוסר בהירות שעדיין קיים גם לאחר יום העיון שהתקיים בנושא אנו מבקשים לברר מיהם הספקים שהוא אמור לחול עליהם ומהו היקף התחולה.

עפ"י החוזר "ספק" בהקשר לחוזר זה, ספק חיצוני המחזיק בידיו מידע רפואי או מידע על – תשתיות מערכת הבריאות (פרטי רופאים וכיו"ב) בסטנדרטים להגנת מידע ממוחשב.
נבקשכם להבהיר:

1. מה הכוונה בספק המחזיק מידע "בסטנדרטים להגנת מידע ממוחשב"? הגדרה זו אינה ברורה ולא ניתן להבין ממנה על אילו ספקים חל החוזר.

תשובת משרד הבריאות:

החוזר מטיל אחריות על המוסד הרפואי לבדוק זאת (לא על הספק): "באחריות מנהל המוסד רפואי לוודא עמידתו של כל ספק חיצוני המחזיק בידיו מידע רפואי או מידע על תשתיות מערכת הבריאות (פרטי רופאים וכיו"ב), בסטנדרטים להגנת מידע ממוחשב, המוסדות כפופים לנוהלי א"מ המפרטים את הסטנדרטים הנ"ל. (הנחיות של רמו"ט, משרד הבריאות, התקשוב הממשלתי...).

2. להבנתנו, באחזקת "מידע רפואי" הכוונה הינה אך ורק למידע רפואי מזוהה אודות מטופלים (רשומות רפואיות מזוהות). או, ככל שכוונתכם לכלול גם מידע רפואי כלשהו מסוג אחר, נבקשכם לפרט באופן ברור מהו אותו המידע עליו הנכם מתבקשים להגן על מנת שניתן יהיה לבחון ולהבין על אילו ספקים חל החוזר.

תשובת משרד הבריאות:

שוב, הגדרות סיווג וחיסיון המידע הן באחריות המוסד הרפואי. למוסד יש כלים (גם משפטיים) לבדוק זאת בין אם מדובר במידע פרטני מזוהה ובין אם מדובר במידע רגיש / קריטי מסיבות אחרות.

3. למה הכוונה ב"מידע על תשתיות הבריאות (פרטי רופאים וכיו"ב)" בשים את הדגש שההבהרה נדרשת לספקי ציוד רפואי - מהו מידע על תשתיות בריאות?
כמו כן נבקשכם לחדד שאין הכוונה למידע על תשתיות בריאות שנמצא בנחלת הכלל ואין הכוונה לפרטי רופאים שהמידע לגביהם גם כן מצוי בנחלת הכלל.

תשובת משרד הבריאות:

ראו תשובה קודמת. כמו כן, אכן מידע הנמצא בנחלת הכלל אינו נדרש להגנת חיסיון.

4. בסעיף 8.3 לחוזר נאמר: "עד ליום 31.12.2015 יש לתת עדיפות לספקים העומדים בתקן בינלאומי לאבטחת- מידע ISO 27001 – אן בתקן לאבטחת מידע במוסדות בריאות ISO 27799

.. החל מה 1.1.2016 יש לבצע התקשרויות רק עם ספקים העומדים בתקנים הנ"ל " על מנת להימנע מאי הבנות, נבקשכם להבהיר שהכוונה הינה שגם לאחר ה – 1.1.2016 על הספק לעמוד אך ורק באחד התקנים הנ"ל ולא בשניהם יחד.

תשובת משרד הבריאות :

הכוונה לעמידה באחד מהתקנים הנ"ל.

5. למיטב ידיעתנו עמידה בתקני ה – ISO הנ"ל אינה נדרשת במדינות אחרות כתנאי להתקשרות עם מוסדות בריאות ומשכך הספקים הבינלאומיים פועלים לפני סטנדרטים אחרים בהתאם לדרישות הנהוגות במדינות בהן הם פועלים. להבנתנו מדובר בדרישות מחמירות. בשים לב לאופן פעילות התאגידים הבינלאומיים, נבקשכם להבהיר שעמידת הספק המקומי הפועל בהתאם לנוהלי התאגיד הבינלאומי שאליו הוא משתייך, בתנאים הקבועים לאבטחת מידע ממוחשב במדינות המוכרות מהווה חלופה לעמידה בתקני ה – ISO הנזכרים בחוזר.

תשובת משרד הבריאות :

משרד הבריאות במדינת ישראל אכן מתקדם יותר בנושא אבטחת המידע והגנת הסייבר במערכות רפואיות מהרבה מדינות. להבנתנו לא מדובר בדרישות מחמירות יותר אלא בדרישות המשקפות נכון יותר את מציאות האיומים בתחום זה. אנו רואים כי יותר ויותר ארגונים ומדינות מאמצים תקנים אילו (או מקבילים) אצלם – HIPPA כדוגמא בארה"ב.

חלופה לתקן ISO תיבחן פרטנית לכל מקרה ותאושר בהתאם לבחינה.

נודה לבדיקתכם ותשובתכם בהקדם.

בברכה,

חנה לאידרשניידר
מנהלת תחום בימיה ופרמצבטיקה