Journal of Military Medicine
2020, Volume 22, Issue 10
Pages: 1054-1064
10.30491/JMM.22.10.1054

Identifying Information Security Risk Components in Military Hospitals in Iran

Maryam Yaghoubi [1], Parsa Bayat [2 *], Akram Parandeh [3], Sayyed-Morteza Hosseini-Shokouh [1,4]

[1] Health Management Research Center, Baqiyatallah University of Medical Sciences, Tehran, Iran
[2] MSc Student in Financial Management, Ershad Damavand Institute of Higher Education, Tehran, Iran
[3] Medicine, Quran and Hadith Research Center, Faculty of Nursing, Baqiyatallah University of Medical Sciences, Tehran, Iran
[4] Faculty of Health, Baqiyatallah University of Medical Sciences, Tehran, Iran

Received: 31 March 2020 **Accepted**: 8 December 2020

Abstract

Background and Aim: Information systems are always at risk of information theft, information change, and interruptions in service delivery. Therefore, the present study was conducted to develop a model for identifying information security risk in military hospitals in Iran.

Methods: This study was a qualitative content analysis conducted in military hospitals in Iran in 2019. The sample consisted of 8 experts in the field of health information. Data were collected through semi-structured interviews. Data were analyzed using framework analysis and MAXQDA 12 software.

Results: Data analysis resulted in the extraction of 78 codes and 16 categories in 7 themes (management in information security, patient information security, information security in organizational resources, organize in information security, communication in information security, monitoring, and control, equipment security). Information security in organizational resources has the highest number of codes and the management in information security and communication in information security have the least number of codes.

Conclusion: Health care organization's security programs, especially in military hospitals faced with many challenges, the first step of which is to identify potential risks and threats. Then develop policies, guidelines, and programs to eliminate or reduce these threats.

Keywords: Information, Information security, Risk, Military hospital.

*Corresponding author: **Parsa Bayat**, Email: parsabyt@gmail.com

مجله طب نظامی
دوره ۲۲، شماره ۱۰، دی ۱۳۹۹
صفحات: ۱۰۶۴-۱۰۵۴
10.30491/JMM.22.10.1054

شناسایی مولفه‌های ریسک امنیت اطلاعات در بیمارستان‌های نظامی در ایران

مریم یعقوبی [۱]، پارسا بیات [۲*]، اکرم پرنده [۳]، سید مرتضی حسینی شکوه [۱،۴]

[۱] مرکز تحقیقات مدیریت سلامت، دانشگاه علوم پزشکی بقیه الله(عج)، تهران، ایران
[۲] دانشجوی کارشناسی ارشد مدیریت مالی، موسسه آموزش عالی ارشاد دماوند، تهران، ایران
[۳] مرکز تحقیقات طب، قرآن و حدیث، دانشکده پرستاری، دانشگاه علوم پزشکی بقیه الله (عج)، تهران، ایران
[۴] دانشکده بهداشت، دانشگاه علوم پزشکی بقیه الله (عج)، تهران، ایران

چکیده

زمینه و هدف: سیستم‌های اطلاعاتی همواره در خطر سرقت اطلاعات، تغییر اطلاعات و ایجاد وقفه در ارائه خدمات می‌باشند. پژوهش حاضر به‌منظور تدوین الگوی شناسایی ریسک امنیت اطلاعات در بیمارستان‌های نظامی ایران انجام شد.

روش‌ها: این مطالعه یک بررسی کیفی از نوع تحلیل محتوا در سال ۱۳۹۸ بود. جامعه پژوهش ۸ نفر از صاحب نظران در حوزه اطلاعات سلامت بودند. جمع‌آوری اطلاعات به روش مصاحبه نیمه‌ساختاریافته صورت گرفت. تحلیل داده‌ها با استفاده از روش تحلیل چارچوب و بکارگیری نرم‌افزار MAXQDA 12 انجام شد.

یافته‌ها: تحلیل داده‌ها منجر به استخراج ۷۸ کد و ۱۶ طبقه در ۷ مقوله (مدیریت در امنیت اطلاعات، امنیت اطلاعات بیمار، امنیت اطلاعات در منابع سازمانی، سازماندهی در امنیت اطلاعات، ارتباطات در امنیت اطلاعات، نظارت و کنترل، امنیت تجهیزات) شد. مقوله امنیت اطلاعات در منابع سازمانی دارای بیشترین تعداد کد و دو مقوله مدیریت در امنیت اطلاعات و ارتباطات در امنیت اطلاعات کمترین تعداد کد را به خود اختصاص دادند.

نتیجه‌گیری: برنامه امنیتی سازمان مراقبت بهداشتی به‌ویژه در بیمارستان‌های نظامی با چالش‌های بسیاری مواجه است که در گام اولِ مواجه با آن، شناسایی ریسک‌ها و تهدیدها است. سپس بایستی خط مشی، دستورالعمل و برنامه‌هایی برای رفع یا کاهش این تهدیدات تدوین گردد.

کلیدواژه‌ها: اطلاعات، امنیت اطلاعات، ریسک، بیمارستان نظامی.

*نویسنده مسئول: **پارسا بیات**. پست الکترونیک: parsabyt@gmail.com
دریافت مقاله: ۱۳۹۹/۰۱/۱۲ پذیرش مقاله: ۱۳۹۹/۰۹/۱۸

مقدمه

در سال‌های اخیر سازمان‌های مراقبت بهداشتی برای ارایه‌ی خدمات به مشتریان خود استفاده از پیشرفته‌ترین دستاوردهای علوم مختلف را آغاز کرده‌اند. سیستم های اطلاعات کامپیوتری یکی از این دستاوردها است که در سال‌های اخیر استفاده از این سیستم‌ها در سازمان‌های مراقبت سلامت افزایش یافته است (۱،۲). با پیشرفت فناوری اطلاعات و ارتباطات، حوزه درمان شاهد افزایش درخواست و بکارگیری سیستم‌های کامپیوتری و اطلاعات سلامت و روش‌های مجازی در بخش عمده‌ای از فعالیت‌های بیمارستان‌ها همچون ارائه، نظارت و اطلاع‌رسانی خدمات درمانی شده‌است (۳،۴). یکی از موارد پرکاربرد سیستم‌های اطلاعاتی و کامپیوتری در پرونده الکترونیک بیمار می‌باشد که می‌تواند فواید زیادی در حل معظلات پزشکی از جمله کاهش معضل تجویز غیرضروری دارو داشته باشد. همچنین توسعه استفاده از فناوری اطلاعات می‌تواند منجربه شفافیت اقتصادی و جلوگیری از پرداخت‌های غیرضروری بیماران گردد (۵). و این بدان معناست که مسئولیت حفظ امنیت و محرمانگی اطلاعات سلامت خصوصاً در سیستم‌های کامپیوتری روز به روز پیچیده‌تر و دشوارتر می‌گردد (۸-۶) و به تبع آن، آسیب‌پذیری فضای تبادل اطلاعات افزایش یافته است و روش‌های اعمال تهدیدهای مربوط به امنیت اطلاعات گسترده‌تر و پیچیده‌تر شده است (۶). مطالعات نشان می‌دهد که استقرار سیستم‌های اطلاعات مدیریت در سازمان‌های مراقبت سلامت دارای ریسک بالا و هزینه‌های پنهان هستند و این سیستم‌ها با ریسک بالا و هزینه زیاد بودجه قابل توجهی را به خود اختصاص می‌دهند (۹). علاوه بر هزینه‌بر بودن و ریسک بالای این سیستم‌ها، با افزایش دانش بیماران در خصوص اهمیت اطلاعات مربوط به پرونده پزشکی خود و انتظار آنها از بیمارستان برای حفظ امنیت آنها (۱۰). بیمارستان‌ها به دنبال بررسی علل ریسک و مخاطرات شغلی نیروی انسانی کاهش آنها در بکارگیری از سیستم‌های اطلاعات سلامت می‌باشند (۱۱،۱۲).

مدیران و کارکنان بیمارستان، در حفظ اطلاعات محرمانه بیمار نقش بسزایی داشته و بسته به نوع و سطح خدماتی که ارایه می‌دهند به اطلاعات محرمانه بیمار دسترسی دارند و وظیفه قانونی و اخلاقی جهت حفظ محرمانگی مدارک و اطلاعات پزشکی بیماران دارند به گونه‌ای که این وظیفه حتی پس از مرگ بیماران نیز ساقط نمی‌شود بیمارستان‌ها باید دارای ضوابط روشنی پیرامون نحوه دسترسی به اطلاعات پرونده پزشکی بیمار و حفظ امنیت در اطلاعات باشند تا بر اساس معیارهای آن کادر بهداشتی درمانی مرکز، وظیفه حفظ محرمانگی اطلاعات افراد را به خوبی دانسته را آن مراعات نمایند (۱۳). البته وجود ضوابط به تنهایی ضمانت حفظ امنیت نیست و ایجاد امنیت در اطلاعات یک موضوع چند بعدی بوده که مواردی مانند آموزش سیاستگذاری، عوامل مدیریتی فنی و فیزیکی و فرهنگ امنیت اطلاعات را در برمی‌گیرد (۱۴،۱۵). اگر به اطلاعات موجود در پرونده‌های پزشکی توجه کنیم، درمی‌یابیم که علاوه بر اطلاعات تشخیصی و آزمایشگاهی، اطلاعات مربوط به سوابق خانوادگی، تست‌های ژنتیک، سوابق و درمان بیماری‌های مربوطه، سابقه مصرف دارو و مواد مخدر، تست‌های مربوط به بیماری‌های آمیزشی و اطلاعاتی در مورد شخصیت و سلامت روحی، روانی نیز در پرونده بیماران وجود دارد (۱۱،۱۶). این موضوع در بیمارستان‌های نظامی به دلیل وجود تهدیدات نظامی از اهمیت بیشتری برخوردار است افرادی که در بیمارستان‌های نظامی بستری می‌شوند افراد کلیدی بوده و گاهی در امور سیاسی و اقتصادی کشور نقش دارند در واقع هدف اصلی امنیت اطلاعات در بیمارستان‌های نظامی به حداقل رساندن تهدیدهای مربوط به امنیت Security-related threats و آسیب‌پذیری سازمانی Vulnerabilities organizational است (۱۷).

از طرفی تحقیقات در کشور ما نشان می‌دهد که نبود زیرساخت‌های فنی و اجرایی امنیتی مناسب و عدم انجام اقدام مؤثر درخصوص ایمن‌سازی فضای تبادل اطلاعات در بعضی مؤسسات موجب گردیده است که وضعیت امنیت تبادل اطلاعات کشور در سطح مطلوب قرار نگیرد (۱۸). همچنین بخش‌های بیمارستانی نیز از استانداردهای مربوط به امنیت و محرمانگی فاصله و انحراف دارد و کشور ما فاقد الزامات امنیتی پرونده‌ی الکترونیک سلامت می‌باشد (۶) از طرفی مطالعات انجام شده در ایران نشان می‌دهد که مطالعه جامعی در بیمارستان‌های نظامی صورت نگرفته است از این رو این مطالعه با هدف شناسایی ریسک امنیت اطلاعات در بیمارستان‌های نظامی در ایران صورت گرفته است.

روش‌ها

این مطالعه یک مطالعه کیفی است که با استفاده از روش تحلیل محتوای قراردادی با رویکرد استقرا انجام شده است. مطالعه در سال ۱۳۹۸ در سطح ملی انجام شده است. جامعه مورد مطالعه افراد مطلع و صاحب‌نظر در حوزه فناوری اطلاعات سلامت، مدیران ارشد دانشگاه‌های علوم پزشکی و بیمارستان‌های نظامی که سابقه بیش از ۵ سال را در حوزه فناوری اطلاعات سلامت داشتند، بوده‌اند که استراتژی اصلی نمونه‌گیری در این پژوهش، نمونه‌گیری هدفمند و در راستای نمونه‌گیری هدفمند، ما همچنین نمونه‌گیری گلوله برفی را به کار بردیم. که در نهایت ۸ نفر انتخاب شدند (جدول-۱). مصاحبه‌ها تا جایی ادامه پیدا کرده است که داده‌ها به سطح اشباع برسند. اطلاعات مورد نیاز از طریق مصاحبه‌های عمیق نیمه‌ساختاریافته (in depth interviews Semi-structured) جمع‌آوری شد. روال کار به این صورت بود که ابتدا مصاحبه‌شوندگان شناسایی شده، سپس با هماهنگی با مصاحبه‌شونده و کسب رضایت وی برای شرکت در مصاحبه وقت مصاحبه تعیین شد. در زمان تعیین شده به فرد مصاحبه شونده

مراجعه شد و از طریق مصاحبه نیمه‌ساختاریافته، و براساس راهنمای مصاحبه (سوالات اولیه Interview guide) که مشتمل بر مفهوم اطلاعات، امنیت اطلاعات، امنیت اطلاعات در بیمارستان‌های نظامی و همچنین تعریف ریسک و مولفه‌های آن می‌باشد اطلاعات مورد نیاز جمع‌آوری شد. برای ثبت مصاحبه‌ها از دستگاه ضبط صدا استفاده گردید و همزمان با آن نیز یادداشت‌برداری و ثبت نکات مهم و کلیدی توسط پرسشگر صورت گرفت. مدت زمان مصاحبه بین ۴۵ تا۸۰ دقیقه متغیر بود. تحلیل داده‌ها با استفاده از روش تحلیل محتوا و بکارگیری نرم‌افزار MAXQDA 12 انجام شد. تجزیه و تحلیل داده‌های حاصل از هر مصاحبه، راهنمایی برای مصاحبه بعدی بوده است. بدین ترتیب نمونه‌گیری تا اشباع داده‌ها، زمانی که دیگر کد جدیدی استخراج نشد، ادامه یافت و و در نهایت طی نشستی با حضور تیم تحقیق نهایی گشت. تمامی مصاحبه‌ها به‌عنوان واحد تحلیل کدگذاری شده؛ کلمات، جملات و یا پاراگراف‌هایی از متون مصاحبه به عنوان واحدهای معنایی لحاظ خواهد شد؛ آن‌گاه واحدهای معنایی به‌هم مرتبط از نظر محتوای اصلی، در کنار یکدیگر قرار گرفته و با برچسبی به‌عنوان کد نامگذاری شده‌اند؛ بازنگری کل متن بعد از کدگذاری، مقایسه کدها از لحاظ تشابه و تفاوت، دسته‌بندی آنها تحت زیرطبقات و طبقات صورت گرفته است. طبقات و زیرطبقات در طی یک جلسه ۳ ساعته با اعضای اصلی تیم تحقیق مورد بررسی و تصحیح قرار گرفتند. ابزار گردآوری داده ها پرسشنامه ای به صورت باز پاسخ بوده است. جهت ارزیابی کیفی مطالعه از معیارهای اعتبار (Credibility)، قابلیت تأیید (Confirmability)، قابلیت اعتماد (Dependability) و انتقال‌پذیری (Transferability) برای ارزیابی روایی، دقت و پایایی داده‌های کیفی استفاده گردید (۱۹). در مطالعه حاضر از ۴ تکنیک جهت بررسی اعتبار (Credibility) داده‌ها بهره گرفته شد. درگیری طولانی مدت محقق با موضوع تحقیق و داده‌ها (غرق شدن در داده‌ها، با مطالعه مکرر نوشته‌ها) به‌منظور کسب درکی عمیق تر از داده‌ها، سپس استخراج واحدهای معنایی و دسته‌بندی آن‌ها صورت پذیرفت و در این مرحله بازبینی توسط همکار به عمل آمد، به‌طوری‌که در مرحله رمزگذاری و کدبندی از دو محقق دیگر خواسته شد در این مرحله مشارکت داشته باشند و در انتها، نظرات اصلاحی آنها لحاظ گردید. کنترل توسط خود مشارکت‌کنندگان نیز یکی دیگر از تکنیک‌های بکارگرفته شده است که بخشی از متن مصاحبه همراه با کدهای اولیه به رویت مشارکت‌کنندگان رسید و میزان تجانس ایده‌های استخراج شده محقق از داده‌ها با نظر مشارکت‌کنندگان مقایسه گردید. مثلث‌سازی، دیگر تکنیکی است که در این مطالعه به منظور ارزیابی ارزش داده‌ها از آن بهره گرفته شده است. تکنیک حاضر به دو صورت مثلث‌سازی منابع داده‌ها (استفاده از منابع مختلف متون و مصاحبه برای یافتن داده‌ها) و مثلث‌سازی محقق (بهره‌مندی از دو محقق دیگر به منظور تجزیه، تحلیل و تفسیر داده‌ها و همچنین تشکیل میزگرد کارشناسی جهت بهره‌جویی از نظرات مفید اساتید راهنما) جهت بالا بردن اعتبار درونی داده‌ها بکار گرفته شده است. در انتخاب مشارکت‌کنندگان (جدول-۱) معیار انتقال‌پذیری با استفاده از تکنیک نمونه‌گیری با حداکثر تنوع (samplingvariation maximum) استفاده شده است. قابلیت تأیید نیز از طریق کنترل ناظران خارجی (check external) سنجیده شده است، به این معنی که بخش‌هایی از متن مصاحبه، کدهای مربوط و طبقات پدیدار شده، توسط دو ناظر آشنا به تحقیق کیفی و مدیریت نوآوری مورد بررسی و تایید قرار گرفته است. همچنین معیار قابلیت اعتماد، از طریق نسخه‌نویسی در اسرع وقت و همچنین ثبت دقیق مراحل و روند تحقیق صورت پذیرفته است تا امکان پیگیری و استفاده از این مطالعه برای دیگران فراهم گردد.

ملاحظات اخلاقی: بعد از هماهنگی با واحد پژوهش و اخذ مجوزهای لازم پژوهش شروع شد. تجزیه و تحلیل داده‌ها توسط پژوهشگر به‌صورت محرمانه انجام شد. در طول مطالعه اصول اخلاقی در پژوهش مانند حفظ بی‌نامی، رازداری و اختیار شرکت‌کنندگان برای ترک مطالعه رعایت شده است. قبل از جمع‌آوری اطلاعات، کمیته اخلاق و تحقیقات دانشگاه علوم پزشکی بقیه الله (عج) این مطالعه را با با کد ۱۸۲,۱۳۹۶ IR.BMSU.REC.1398.075مورد تایید قرار داد.

نتایج

ویژگی‌های ۸ مشارکت‌کننده در بخش مطالعه کیفی در جدول-۱ ارائه شده است. مقوله، طبقات و کدهای موثر بر امنیت اطلاعات در بیمارستان‌های نظامی در جدول-۲ آمده است. مدیریت در امنیت اطلاعات: مقوله مدیریت در امنیت اطلاعات شامل ۲ طبقه (مهارت مدیران در بهره‌گیری از داده‌ها، وظایف مدیریت) می‌باشد طبقه مهارت مدیران در بهره‌گیری از داده‌ها شامل ۵ زیر طبقه یا کد و طبقه وظایف مدیریت شامل ۵ زیرطبقه یا کد میباشد.

تعدادی از گویه‌های مربوط به این مقوله عبارت است از

" توانایی‌های افراد برای تبدیل و تحلیل این داده‌ها و تبدیل به خرد توانمندی‌های خاصی است "

"اطلاعات می تواند ساده باشد و می‌تواند پردازش شده باشد و بستگی به مخاطب دارد که بتواند از آن در تصمیم‌گیری استفاده کند."

جدول-۱. ویژگی‌های مشارکت‌کنندگان مطالعه کیفی

مشارکت‌کننده شماره ۱	۴۴ ساله، مدرک دکتری تخصصی رتبه دانشیار، ۱۵ سال سابقه هیات علمی، مسئول بخش فناوری اطلاعات پزشکی.
مشارکت‌کننده شماره ۲	۳۴ ساله، مدرک کارشناسی ارشد، ۶ سال سابقه کار، کارشناس ارشد مهندسی فناوری اطلاعات یک بیمارستان نظامی.
مشارکت‌کننده شماره ۳	۶۲ ساله، مدرک دکتری تخصصی بیش از ۳۰ سال سابقه کار در دانشگاه نظامی، معاونت یکی از سازمان‌های بیمه‌ای
مشارکت‌کننده شماره ۴	۶۵ ساله، مدرک دکتری تخصصی بیش از ۳۰ سال سابقه کار در شرکت های فناوری اطلاعات.
مشارکت‌کننده شماره ۵	۵۲ ساله، مدرک دکتری تخصصی، ۲۸ سال سابقه تدریس در در دانشگاه علوم پزشکی اصفهان. و فعالیت در زمینه اطلاعات سلامت
مشارکت‌کننده شماره ۶	۳۸ ساله، مدرک دکتری تخصصی، ۱۷ سال سابقه تدریس و فعالیت در حوزه فناوری اطلاعات در دانشگاه علوم پزشکی تهران.
مشارکت‌کننده شماره ۷	۴۷ ساله، مدرک کارشناسی ارشد نرم‌افزار، ۲۰ سال سابقه کار در زمینه شبکه های کامپیوتری.
مشارکت‌کننده شماره ۸	۵۸ ساله، مدرک کارشناسی ارشد، ۲۵ سال سابقه کار، فعالیت درزمینه ی سیستم های اطلاعات مدیریت.

جدول-۲. مقوله، طبقات و کدهای موثر بر امنیت اطلاعات در بیمارستان‌های نظامی

مقوله ها	طبقات	کد یا زیر طبقات (فراوانی)	تعدادکل کد (فراوانی)
۱-مدیریت در امنیت اطلاعات	۱-مهارت مدیران در بهره‌گیری از داده‌ها	داشتن توانایی تبدیل داده به خرد (۱) ادراک مدیران از داده‌ها و اطلاعات نظامی (۱) مهارت بهره‌گیری از داده‌ها (۱) قدرت پردازش اطلاعات و استفاده در تصمیم‌گیری در بین مدیران (۱) خرد یا بصیرت در بین مدیران در مورد داده‌ها و اطلاعات نظامی (۱)	۵(۵)
	۲-وظایف مدیریت	-آگاهی مدیران در مورد مباحث امنیت اطلاعات (۱) حمایت مدیریت از برنامه های امنیت اطلاعات (۳) ایجاد اعتماد بین مدیر و کارکنان (۱) تدوین برنامه جامع امنیتی (۱) تعهد مدیران نسبت به اطلاعات بیمارستان (۱)	۵(۷)
۲-امنیت اطلاعات بیمار	۳-حقوق بیمار	حفظ حریم شخصی بیمار و احترام گذاشتن به خواست او (۲) قانون محرمانگی اطلاعات بیماران (۴) وجود فردی به نام وکالت اطلاعات سلامت (۱) حق مالکیت داده برای بیمار یا وکیل قانونی او (۱)	۴(۸)
	۴-حفاظت از اطلاعات بیمار	تدوین قوانین رازداری و صیانت بین کادر درمانی و بیمار (۱) ثبت پرونده های سلامت افراد نظامی با نام ها و کدملی های مستعار (۲) وکیل نظامی برای سران کشور و افراد نظامی رده بالا (۱) حفاظت از اطلاعات ژنتیک سران نظامی (۱) پزشکی شخصی شده (۱)	۵(۶)
۳-امنیت اطلاعات در منابع سازمانی	۵-آموزش و اگاهی در مورد امنیت اطلاعات	سنجش آگاهی و ادراک کاربران از امنیت اطلاعات (۱) آموزش مستمر (۱) آگاهی کارکنان از کارهای مجاز و غیرمجاز امنیتی و تبعات آن (۱) وجود برنامه آموزشی مدون در مورد خط مشی و مقررات امنیت اطلاعات(۱) آموزش درست و دقیق در مورد امنیت اطلاعات (۲) طراحی دوره‌های امنیت اطلاعات متناسب با نیاز کاربران (۱)	۶(۷)
	۶-منابع (مالی،زیر ساخت)	ریسک تکنولوژیکی (۱) زیرساخت مناسب انتقال اطلاعات (۲) اختصاص بودجه مشخص و کافی به امنیت از اطلاعات (۲)	۳(۵)
	۷-امنیت نیروی انسانی	محدود کردن دسترسی به تجهیزات کامپیوتری (۱) تصدیق موجودیت یا تأیید هویت کاربران (۱) افراد دارای صلاحیت و متعهد (۱) توجه به گفته‌های شفاهی در مورد مسایل امنیتی بیمارستان (۱) رفتار عامدانه نیروی انسانی (۱) انتخاب افراد مجاز برای دسترسی به اطلاعات نظامی (۳) سطح بندی و دسترسی محدود و منطقی به داده‌ها و برنامه‌ها (۱) به کارگیری افراد با تحصیلات و تخصص در زمینه امنیت اطلاعات (۲) رعایت اصول امنیت اطلاعات حتی بعد از ساعت کاری (۱)	۹(۱۴)

۴- سازماندهی در امنیت اطلاعات	۸-ساختار امنیت اطلاعات	سیستم گزارش‌دهی در مورد وقایع امنیتی (۲) عدم امنیت در فضای تبادل اطلاعات (۱) فرایندی برای خاتمه دسترسی به اطلاعات الکترونیکی حفاظت شده (۱) وجود ساختار و تیم امنیت اطلاعات (۲)	۴(۶)
	۹-سیاست و رویه ها	تدوین خط مشی و مقررات امنیت اطلاعات و به‌روزرسانی آن (۳) شرح وظایف مسئول امنیت اطلاعات (۱) ضوابط برای انهدام اطلاعات (۱) ابلاغ سیاست های مجازات و سایر سیاست‌های امنیتی به کارکنان (۱) سیاست روشن و درستی در زمینه مجازات افراد خاطی: خط مشی مجازات (۱)	۵(۷)
۵- ارتباطات در امنیت اطلاعات	۱۰-شبکه الکترونیک	امنیت رمز الکترونیکی (۱) کنترل و مدیریت رمز عبور کاربران (۲) اعتبار کاربر برای ارتباطات و تماس‌های خارج از سازمان (۱) امنیت در خدمات الکترونیکی و آنلاین (۱) امنیت سیستم‌های اداری الکترونیک (۳)	۵(۸)
	۱۱- سازمانهای بیرونی	تدوین خط مشی و مقررات چگونگی ارتباط با سازمان‌های بیرونی (۱) وجود امنیت در فرآیند تبادل اطلاعات با سازمان‌های بیرونی (۲) توجه به نوع و میزان اطلاعات در تبادل اطلاعات با سازمان‌های بیرونی (۱)	۳(۴)
۶-نظارت و کنترل	۱۲-امنیت در کسب و کار	نظارت بر متن قراردادها و کسب و کار با سازمان‌های بیرونی (۱) ممیزی در مورد شرکت‌های بیرونی طرف قراردادهای کاری (۱) نظارت در توسعه نرم‌افزارهای برونسپاری شده (۱)	۳(۳)
	۱۳-ممیزی سیستمهای اطلاعاتی	ممیزی محتوی، فرایند و شیوه های تبادل داده (۱) یکپارچه بودن اطلاعات (۲) ریسک اطلاعاتی (۱) جلوگیری از افشای اطلاعات به افراد غیرمجاز (۴) رمزگذاری و رمزگشایی اطلاعات (۱)	۵(۹)
	۱۴-نظارت بر دسترسی اطلاعات	شناسایی اطلاعات موردنظر و شناسایی کاربر اطلاعات (۱) ثبت و ضبط به موقع داده (۲) دسترسی محدود و منطقی به داده‌ها و برنامه ها (۱) رعایت ضوابط و اخلاق پژوهش در محیط‌های نظامی (۱) ریسک‌هایDuplication (۱) دیکشنری واحد بین سیستم های اطلاعاتی (۱) توجه به دسترسی در تمامی مراحل مدیریت داده(۱)	۷(۸)
۷-امنیت تجهیزات	۱۵-امنیت نرم‌افزاری	برنامه‌نویسی توسط افراد در داخل بیمارستانهای نظامی (۱) توجه به رخنه‌های امنیتی (۲) ایجاد نسخه پشتیبان (۱) جلوگیری از هک و نفوذ به اطلاعات نظامی (۴) استفاده و به روز رسانی نرم‌افزارهای امنیتی (۲) شرکتهای نرم‌افزاری حائز صلاحیت به لحاظ امنیت(۱)	۶(۱۱)
	۱۶-امنیت فیزیکی	نرم‌افزارهای بدون کسب مجوز (۱) حفاظت از سخت‌افزار در برابر آسیب‌های فیزیکی (۴) امنیت سیستم برق (۱)	۳(۶)
جمع کل			۷۸(۱۱۴)

"مدیران الزاماً باید بصیرت داشته باشند و یک مدیر بیمارستان اگر پزشک باشد زمانی به بصیرت می‌رسد که مدیریت مالی را بفهمد، مدیریت منابع انسانی را بفهمد، انگیزش را بفهمد، سازماندهی را بفهمد و سیستم‌های ارائه خدمت را بفهمد به بصیرت رسیده است."

"اگر مدیر ادراک استفاده از آمار بیمارستانی را نداشته باشد برای مدیر نقش داده را ایفا می‌کند و اگر بتواند از آن‌ها استفاده کند و در تصمیم‌گیری او نقش داشته باشد حکم اطلاعات را پیدا می‌کند".

"عدم آگاهی مدیران از اهمیت داده‌ها و مواردی که از آنها قابل استخراج است می‌تواند امنیت اطلاعات رو به خطر بندازه"

"برنامه های امنیت اطلاعات عبارتنداز سیاست‌ها، رویه‌ها، استانداردها و رهنمودهای مکتوب که توسط مراجع مسئول مورد تأیید و حمایت قرار گرفته است."

-امنیت اطلاعات بیمار

مقوله امنیت اطلاعات بیمار شامل ۲ طبقه (حقوق بیمار، حفاظت از اطلاعات بیمار) می‌باشد این مقوله دارای ۹ کد می‌باشد که طبقه حقوق بیمار شامل ۴ زیرطبقه یا کد و طبقه حفاظت از اطلاعات بیمار شامل ۵ زیرطبقه یا کد می‌باشد. در بین کدها، قانون محرمانگی اطلاعات بیماران دارای بیشترین فراوانی می‌باشد.

تعدادی از گویه‌های مربوط به این مقوله عبارت است از:

"حریم شخصی به قوانین و مقررات بین آدم‌ها برمی‌گردد که مکلف هستند از آن تبعیت کنند که باید در قانون و آموزش و تربیت افراد دیده شود نه در تکنولوژی. که شامل عدم افشای اطلاعات بیماران می‌شود که هیچ ارتباطی با نرم‌افزار ندارد. حریم شخصی به امنیت اطلاعات مقدم است."

"در کشور قانون محرمانگی اطلاعات بیماران وجود دارد که بسیار ناقص است و از آن مهم‌تر که رعایت نمی‌شود".

"در دنیا حتی یک شغل جدید هم ایجاد شده است با عنوان وکالت اطلاعات سلامت افراد که همین وظیفه را دارند. که هنوز قانون HIPAA در ایران تصویب نشده."

"به طور سهوی و گاهی عمدی امکان افشای اطلاعات وجود دارد. قوانین رازداری و صیانت هم باید مورد توجه قرار گیرد که در ایران سند و قوانینی در خصوص رازداری که مقدم بر امنیت اطلاعات است، وجود ندارد".

"چون که نمی‌توانیم امنیت سخت‌افزار و نرم‌افزار را به طور صددرصد تضمین نماییم باید به روش‌های دیگری روی بیاوریم که روس‌ها ابداع کرده‌اند، مثل این که پرونده‌های سلامت این افراد با نام‌ها و کدملی‌های مستعار ثبت شوند."

-امنیت اطلاعات در منابع سازمانی

مقوله امنیت اطلاعات در منابع سازمانی شامل ۳ طبقه (آموزش و آگاهی در مورد امنیت اطلاعات، منابع (مالی-زیرساخت) و امنیت نیروی انسانی می‌باشد. این مقوله دارای ۱۸ کد می‌باشد که طبقه امنیت نیروی انسانی دارای بیشترین کدها و شامل ۹ کد و طبقه منابع (مالی-زیرساخت و ...) دارای کمترین تعداد کد و شامل ۳ کد می‌باشد. در بین کدها، انتخاب افراد مجاز برای دسترسی به اطلاعات نظامی دارای بیشترین فراوانی می‌باشد.

تعدادی از گویه‌های مربوط به این مقوله عبارت است از:

"یکی از جنبه‌ها و راه‌های مهم برای حفاظت و مدیریت امنیت اطلاعات، ارتقاء آگاهی و ادراک کاربران از امنیت اطلاعات است. دراین صورت، افراد آگاهی‌های لازم و مربوط به نقش و مسئولیت خویش در حفظ امنیت اطلاعات در کار مربوط به خود را کسب می‌کنند."

"در واقع خود نیروی انسانی یک عامل ریسک هست همان طور که بعضی از موارد رو گفتم آموزش خیلی مهمه آیا افراد سازمان کارهای مجاز و غیرمجاز امنیتی را می‌شناسند و از تبعات آنها آگاهند؟"

"سطح دسترسی به افراد بدهیم و از همه مهم‌تر بعضی داده‌ها باید توسط افراد خاص محافظت شوند و در عین حال قابل کشف برای افراد مجاز باشند مثل فرمول کوکاکولا که صدوپنجاه سال است که در هر لحظه فقط دو نفر این فرمول را می‌دانند و هیچ کس هم آن‌ها را نمی‌شناسد که یک روش خوب امنیت اطلاعات است."

"وقتی حرف دسترسی به میون میاد یک معنی مثبت میده ولی دسترسی باید برای هرکی محدود باشه که این به ویژه تو فضای نظامی این مسله خیلی مهمه. دسترسی اگر باز باشد در سیستم اختلال ایجاد میکنه از طرفی اگر جلوی دسترسی افراد مجاز به اطلاعات مرتبط با آنها را گرفته باشیم، در واقع کاری نامطلوب انجام داده‌ایم."

"موضوع تصدیق موجودیت" که به تأیید هویت کاربران قبل از دسترسی و همچنین جلوگیری از دسترسی همه کاربران غیرمجاز و به کارگیری مکانیسم های تأیید اشاره دارد. خیلی مهم"

-سازماندهی در امنیت اطلاعات

مقوله سازماندهی در امنیت اطلاعات شامل ۲ طبقه (ساختار امنیت اطلاعات، سیاست و رویه‌ها) می‌باشد این مقوله دارای ۹ کد می‌باشد که طبقه سیاست و رویه ها دارای بیشترین کدها و شامل ۵ کد می‌باشد. در بین کدها، تدوین خط مشی و مقررات امنیت اطلاعات و به روز رسانی آن دارای بیشترین فراوانی می‌باشد.

تعدادی از گویه‌های مربوط به این مقوله عبارت است از:

"همچنین اطلاعات سایر منابع مثل ثبت یافته‌های تشخیصی و درمانی در سیستم اطلاعات بیمارستان، ثبت اطلاعات بیماران، و ارائه دهندگان خدمات ورعایت الزاماتی درخصوص امنیت داده‌ها در برابر دسترسی غیرمجاز و یا برنامه نگهداشت نرم‌افزارها و سخت‌افزارهای بیمارستان وجود دارد و اجرا می‌شود."

"افراد نباید در سازمان احساس ترس کنند و در مورد وقایع امنیتی اطلاعات مثل خطاهای کامپیوتری گزارش‌دهی داشته باشند گزینش افراد هم مهم است."

یک موردی که به نظرم میرسه که نبودش ریسک هستش داشتن ساختار امنیت اطلاعات هست مثل چه کمیته‌هایی باید تشکیل بشه چه ساختار سازمانی برای اداره روش‌های امنیت اطلاعات لازم هست؟

"این خط مشی‌ها بایستی به روز رسانی شود و با فضای بیمارستان‌های نظامی سازگار شود"

"یک موردی که به نظرم میرسه که نبودش ریسک هستش داشتن ساختار امنیت اطلاعات هست مثل چه کمیته‌هایی باید تشکیل بشه چه ساختار سازمانی برای اداره روش‌های امنیت اطلاعات لازم هست؟"

-ارتباطات در امنیت اطلاعات

مقوله ارتباطات در امنیت اطلاعات شامل ۲ طبقه (شبکه الکترونیک، سازمان‌های بیرونی) می‌باشد این مقوله دارای ۸ کد می‌باشد که طبقه شبکه الکترونیک دارای بیشترین کدها و شامل ۵ کد می‌باشد. در بین کدها، امنیت سیستم‌های اداری الکترونیک دارای بیشترین فراوانی می‌باشد.

تعدادی از گویه‌های مربوط به این مقوله عبارت است از:

"در مورد مکاتبه ایمیلی با خارج از سازمان افرادی که از این نظر آموزش دیده‌اند، انتخاب شوند."

"منظور از امنیت فنی، روش‌های فنی جهت تضمین امنیت اطلاعات سلامت می‌باشد مانند دسترسی کاربران غیرمجاز به اطلاعات الکترونیکی از طریق اینترنت"

"سیاست‌های سازمان برای برخورد با افراد بیرونی و پیمانکاران در ارتباطات با اطلاعات سازمان چیست؟

" باید همه اینا تو بیمارستان لحاظ بشه در بیمارستان نظامی افراد بیرونی که با اطلاعات ما رو میگیرن باید با دقت انتخاب بشن ارتباطات نادرست ریسک بزرگی برای امنیت اطلاعات هست."

-نظارت و کنترل

مقوله نظارت و کنترل شامل ۳ طبقه (نظارت بر دسترسی اطلاعات، امنیت در کسب‌وکار و ممیزی در سیستم های اطلاعاتی می‌باشد این مقوله دارای ۱۵ کد می‌باشد که طبقه نظارت بر دسترسی اطلاعات دارای بیشترین کدها و هر کدام شامل ۷ کد می‌باشند. در بین کدها، جلوگیری از افشای اطلاعات به افراد غیرمجاز دارای بیشترین فراوانی می‌باشد.

تعدادی از گویه‌های مربوط به این مقوله عبارت است از:

"عدم رعایت ضوابط و اخلاق پژوهش در پژوهش‌هایی که محیط پژوهش آنها بیمارستان‌های نظامی است."

"ممیزی در مورد شرکت‌های بیرونی که به‌صورت برون‌سپاری شده خدماتی را از آنها دریافت می‌کنیم بسیار حائز اهمیت است"

"یکپارچه بودن یعنی جلوگیری از تغییر داده‌ها به‌طور غیرمجاز و تشخیص تغییر در صورت دستکاری غیرمجاز اطلاعات. یکپارچگی وقتی نقض می‌شود که اطلاعات نه فقط در حین انتقال بلکه در حال استفاده یا ذخیره شدن و یا نابود شدن نیز به‌صورت غیرمجاز تغییر داده شود".

"امنیت اطلاعات به معنای کنترل دسترسی و حفظ اطلاعات از افشای تصادفی یا غیرعمدی اطلاعات برای افراد غیرمجاز و جایگزینی یا دستکاری اطلاعات می‌باشد".

"پس این طور که من متوجه شدم باید کاربر و اطلاعات مورد نظر رو بشناسیم در واقع شناسایی اطلاعات موردنظر و بعدش هم شناسایی کاربر اطلاعات مورد نیاز است".

"ریسک‌های بعدی ریسک‌های Duplication است که همان ریسک عدم ورود یکسان یا ثبت بیش از یکبار در سیستم است که یک داده نباید از مجراهای گوناگون و توسط اشخاص مختلف وارد شود و هر داده توسط یک فرد وارد شده و برای همه قابل مشاهده باشد و فقط خود او قابلیت ویرایش داشته باشد. هر بار ثبت مجدد یک داده سی درصد امکان خطا داشته و در موارد بعدی این درصدها در هم ضرب می‌شوند."

-امنیت تجهیزات

مقوله امنیت تجهیزات شامل ۲ طبقه (امنیت تجهیزات، امنیت فیزیکی) می‌باشد این مقوله دارای ۹ کد می‌باشد که طبقه امنیت نرم‌افزاری دارای بیشترین کدها و شامل ۶ کد می‌باشد. در بین کدها، حفاظت از سخت‌افزار در برابر آسیب‌های فیزیکی دارای بیشترین فراوانی می‌باشد.

تعدادی از گویه‌های مربوط به این مقوله عبارت است از:

"رخنه‌ها (Breaches) می‌تواند بدون ضرر به نظر بیاید، مانند Screen Saverهای دریافت شده از اینترنت"

"استفاده و به روز رسانی از نرم‌افزارهای امنیتی، برای نظارت و کنترل دسترسی به اطلاعات و سیستم‌های کامپیوتری"

"عدم همکاری با شرکت‌های نرم‌افزاری بدون صلاحیت به دلیل حفظ امنیت داده‌ها در بیمارستان‌های نظامی"

"برنامه‌نویسی توسط افراد در داخل بیمارستان‌های نظامی و استفاده نکردن از افراد بیرونی"

"یک مورد دیگه‌ای که در امنیت اطلاعات تهدید و ریسک هست ناامن بودن خود تجهیزات فیزیکی است مثل ناامن بودن اطلاعات سیستم از نرم‌افزارهای مخرب و ویروس‌ها"

"ریسک‌های شنود شدن را داریم که باید همان امنیت سیستم‌های بانکی را برای سیستم‌های سلامت هم قایل شویم که امکان هک شدن در حوزه‌ی بانکی بسیار پایین است.

بحث

همان‌طورکه در بخش نتایج گفته شد، تعداد کل مقوله‌های موثر بر امنیت اطلاعات ۷، تعداد طبقات مربوط به آن ۱۶ طبقه و تعداد کل کدها ۷۸ است. مقوله امنیت اطلاعات در منابع سازمانی با بیشترین تعداد کد به سه طبقه (آموزش و آگاهی در مورد امنیت اطلاعات، منابع، امنیت نیروی انسانی) تقسیم شده است. در اهمیت حفظ امنیت و محرمانگی اطلاعات سلامت، طراحی و اجرای برنامه‌های آموزشی جهت آشنایی پرسنل با موضوعات مربوط به امنیت اطلاعات یکی از موارد اصلی و مهم است و آموزش اثربخش یکی از مکانیسم‌های قدرتمند برای کاهش خطرات امنیتی است (۲۰،۲۱).

از سوی دیگر با افزایش آگاهی کارمندان یک سازمان از امنیت اطلاعات، رعایت اصول امنیتی به تدریج نهادینه می‌شود و این امر به تغییر فرهنگ و ارزش‌های امنیتی کمک می‌کند (۲۲،۲۳). منابع (مالی، زیرساخت و...) از دیگر طبقات این مقوله (امنیت اطلاعات در منابع سازمانی) می‌باشد از جمله این منابع به زیرساخت مناسب انتقال اطلاعات و اختصاص بودجه مشخص و کافی به امنیت از اطلاعات می‌توان اشاره کرد. از جمله پژوهش‌هایی که در زمینه امنیت اطلاعات در سیستم‌های اطلاعات سلامت انجام گرفته می‌توان به پژوهش Juanita و همکاران اشاره کرد. یافته‌های این پژوهش حاکی از آن بود که عوامل مختلفی مثل کاربرد نامناسب اطلاعات و زیرساخت‌های امنیتی منسوخ شده، می‌توانند امنیت و محرمانگی اطلاعات در سیستم‌های کامپیوتری را در معرض خطر قرار دهند (۲۴).

طبقه دیگر در این مقوله، مربوط به منابع انسانی است در این طبقه به کدهایی مانند آموزش و تحصیلات نیروی انسانی و سطح دسترسی او مانند محدود کردن دسترسی به تجهیزات کامپیوتری، انتخاب افراد مجاز برای دسترسی به اطلاعات نظامی سطح‌بندی و دسترسی محدود و منطقی به داده‌ها و برنامه‌ها می‌توان اشاره کرد، یکی از جنبه‌ها و راه‌های مهم برای حفاظت و مدیریت امنیت اطلاعات، ارتقا آگاهی کاربران از امنیت اطلاعات است. برنامه آگاه‌سازی امنیتی کلیدی‌ترین عنصر در اجرای موفق یک سیاست

امنیتی در کل سازمان است. هدف اصلی این برنامه تعریف نقش تک تک کارکنان در محافظت از منابع اطلاعاتی حیاتی سازمان است (۲۵). بسیاری از پژوهش‌ها نشان می‌دهند بیش از ۸۰ درصد مشکلات امنیتی در سازمان‌ها ناشی از خطاهای سهوی و عمدی کارکنان بوده است اما خطاهای سهوی اکثراً به دلیل عدم آگاهی به وجود می‌آید (۲۶). دسترسی محدود و منطقی به داده‌ها و برنامه‌ها از طریق کامپیوتر و وسایل ارتباطی، سطح مهمی از امنیت است. کاربران باید تنها اجازه دسترسی به اطلاعاتی را داشته باشند که مجاز به استفاده از آنها هستند. مطالعه Kruger و همکاران به این نتیجه دست یافت که استانداردهای لازم در خصوص کنترل دسترسی به سیستم‌های اطلاعاتی رعایت نشده است (۲۷). در بین مقوله‌های به‌دست آمده مقوله امنیت ارتباطات که شامل دو طبقه شبکه الکترونیک و سازمان‌های بیرونی می‌باشد به بررسی مواردی مانند امنیت رمز الکترونیکی، کنترل و مدیریت رمز عبور کاربران، اعتبار کاربر برای ارتباطات و تماس‌های خارج از سازمان، امنیت در خدمات الکترونیکی و آنلاین، امنیت سیستم‌های اداری الکترونیک می‌پردازد. گرچه سرویس‌های ایمیل مورد حمایت سازمان‌ها قرار گرفته‌اند اما وسیله‌ای محرمانه برای ارتباطات نیستند. استفاده از این سرویس‌ها ممکن است به صورت نادرست باشند و کاربران آنها ممکن است مورد تهاجم کاربرانی خارج از سازمان قرار گیرند. با این حال تلاش‌های فراوانی برای کاهش سوءاستفاده از سرویس‌های ایمیل صورت گرفته است (۲۸). در مطالعه که در کانادا صورت گرفت، پژوهشگران قادر به شکستن پسورد ۹۳ درصد فایل‌ها شدند همچنین، مشخص شد که فایل‌های محتوای اطلاعات سلامت شخصی بیماران به وسیله ایمیل و درایوها به اشتراک گذاشته می‌شود (۲۹).

در خصوص امنیت رمز و بررسی دسترسی، روش شناسایی بیومتریک به یکی از صورت‌های ثبت صدا، اثر انگشت، اسکن شبکیه، اسکن کل بدن و غیره پیشنهاد می‌شود. اعتبار کاربر به‌طور کلی موضوعی است که در شبکه‌های الکترونیکی در بیمارستان‌ها چه در ارتباطات داخلی چه در ارتباط با سازمان‌های بیرونی مورد توجه بایستی قرار بگیرد عنوان تصدیق موجودیت "به تأیید هویت کاربران قبل از دسترسی و همچنین جلوگیری از دسترسی همه کاربران غیرمجاز و به‌کارگیری مکانیسم‌های تأیید اشاره دارد (۳۰). در مورد امنیت از طرف سازمان‌های بیرونی از آنجایی که سیستم‌های اطلاعات بیمارستانی از شرکت‌های نرم‌افزاری متفاوتی خریداری می‌شوند، ضروری است تا وجود امنیت درفرآیند تبادل اطلاعات با سازمان‌های بیرونی به دقت مورد بررسی قرار گیرد و از شرکت‌های طرف قرارداد خواسته شود تا خط مشی و مقررات تدوین شده توسط بیمارستان نظامی درخصوص چگونگی ارتباط با سازمان‌های بیرونی را رعایت کنند. نتایج مطالعه دیگری نشان می‌دهد که امنیت فیزیکی امنیت اطلاعات در سازمان‌های مراقبتی نقش بسزایی در ارتقای سطح امنیتی اطلاعات دارد (۳۱). از دید ژوبرت فرآیند توسعه الکترونیکی ذاتاً پیچیده است و عوامل بسیاری شانس موفقیت آن را بیشتر می‌کند و یکی از این مسائل بلوغ فنی است. برای بهتر یا بدتر شدن وضعیت یک پروژه تنها بر مسائل فرهنگی و اجتماعی و مالی تمرکز نشود و باید مسائل فنی بیش از پیش مورد توجه قرار گیرد.«این مطلب نیز مؤید نتایج به‌دست آمده از پژوهش حاضر می‌باشد (۳۲).

امروزه سازمان‌های مراقبت سلامت به دلایل متعددی از جمله حفظ محرمانگی اطلاعات از سیستم‌های اطلاعاتی استفاده می‌کنند (۳۳). که استفاده موفقیت‌آمیز از سیستم‌های اطلاعات بالینی، مستلزم روش‌های موثر و ایمن برای تبادل محتوای پرونده‌های الکترونیکی است (۳۴). مقوله دیگر مربوط به امنیت اطلاعات بیمار است که مواردی چون وکیل نظامی برای سران کشور و افراد نظامی رده بالا، حق مالکیت داده برای بیمار یا وکیل قانونی او، حفاظت از اطلاعات ژنتیک سران نظامی، حفظ حریم شخصی بیمار و احترام گذاشتن به خواست او را شامل می‌شود. صفدری در این رابطه می‌نویسد بیمار باید مطابق با قوانین تدوین شده مجاز به اصلاح یا تغییر اطلاعات هویتی پرونده‌اش باشد و داده‌های غیر صحیح یا ناقص را تصحیح کند؛ و هر بیمار بزرگسال یا نماینده قانونی بیمار مجاز باشند که مطابق با قوانین تدوین شده تمام اطلاعات ذخیره شده در پرونده را جستجو و کپی کند (۳۵). در مقوله نظارت و امنیت اطلاعات، طبقات ممیزی در سیستم‌های اطلاعاتی، امنیت در کسب و کار و نظارت بر دسترسی اطلاعات شناسایی شده است که مواردی چون توجه به دسترسی در تمامی مراحل مدیریت داده، نظارت بر متن قراردادها و کسب‌وکار با سازمان‌های بیرونی، رمزگذاری و رمزگشایی اطلاعات وجلوگیری از افشای اطلاعات به افراد غیرمجاز را مد نظر دارد Geum و همکارانش یک روش امنیتی با استفاده از تئوری فازی برای مدیریت ریسک امنیت اطلاعات ارائه دادند و کنترل و نظارت مستمر مدیریت امنیت اطلاعات را جهت پیشگیری از خسارات ناشی از حملات و خرابی سیستم‌های اطلاعاتی در یک سازمان، ضروری برشمردند (۳۶).

محدودیت دسترسی به منابع علمی مرتبط با زمینه موضوع تحقیق و سخت بودن هماهنگی قرار ملاقات با بعضی از اساتید

نتیجه‌گیری

برنامه امنیتی سازمان مراقبت بهداشتی به‌ویژه در بیمارستان‌های نظامی با چالش‌های بسیاری مواجه است که در گام اول بایستی ریسک‌ها و تهدیدات بالقوه شناسایی گردد سپس خط مشی، دستورالعمل و برنامه‌هایی برای رفع یا کاهش این تهدیدات برای رسیدن به اهدافی از قبیل محرمانگی، صحت و دقت و موجود بودن در بیمارستان تدوین شود، اما نباید فراموش گردد که در یک مرکز بهداشتی– درمانی حفظ امنیت علاوه بر اطلاعات پرونده الکترونیک شامل مواردی از قبیل شبکه‌ها، سخت‌افزار، نرم‌افزار و برنامه‌های کاربردی و نیروی انسانی نیز می‌باشد، از این رو مراکز

بهداشتی–درمانی برای داشتن برنامه امنیتی مؤثر به تمام این موارد بایستی توجه کنند.

نکات بالینی کاربردی برای جوامع نظامی

- با توجه به نقش کلیدی نیروی انسانی درمانی در حفظ امنیت اطلاعات توصیه می‌شود در قابلیت دسترسی برای سطوح مختلف کاری محدودیت ایجاد شود و تمامی اطلاعات حساس و آسیب‌پذیر رمزنگاری شوند. از طرفی پسوردها باید به‌طور امن نگه‌داری شوند و حساب کاربران باید مخفی باشند. توجه به برنامه‌ریزی جهت تدوین و اجرای جدیدترین سیاست‌ها و دستورالعمل‌های امنیتی منطبق با نیازمندی‌های امنیت اطلاعات در بیمارستان‌ها و پیشرفت‌های فناوری ضروری است.

تشکر و قدردانی: مطالعه حاضر منتج از طرح تحقیقاتی دانشگاه علوم پزشکی بقیه الله (عج) به شماره ۹۷۰۰۰۴۹۶ با کد اخلاق IR.BMSU.REC.1398.075 بوده که به این وسیله از زحمات متخصصان فن آوری اطلاعات سلامت که در مصاحبه شرکت کردند تقدیر و تشکر می‌گردد.

نقش نویسندگان: ارائه ایده و طرح اولیه توسط یعقوبی، انجام مصاحبه‌ها توسط بیات، کدبندی و استخراج مقوله‌ها، طبقات و کدها توسط همه نویسندگان، ورود در نرم‌افزار توسط بیات و تحلیل و تفسیر نهایی توسط یعقوبی. همه نویسندگان در نگارش اولیه مقاله یا بازنگری آن سهیم بودند و همه با تایید نهایی مقاله حاضر، مسئولیت دقت و صحت مطالب مندرج در آن را می‌پذیرند.

تضاد منافع: نویسندگان تصریح می کنند که هیچ‌گونه تضاد منافعی در مطالعه حاضر وجود ندارد.

منابع

1. Cavalli E, Mattasoglio A, Pinciroli F, Spaggiari P. Information security concepts and practices: the case of a provincial multi-specialty hospital. International Journal of Medical Informatics. 2004;73(3):297-303. doi:10.1016/j.ijmedinf.2003.12.008
2. Mehraeen E, Ayatollahi H, Ahmadi M. Health information security in hospitals: The application of security safeguards. Acta informatica medica. 2016;24(1):47. doi:10.5455/aim.2016.24.47-50
3. Claude BJ, Hansson H, Ben R. Integrated computer-based management information systems: The complexity and diffusion in Rwandan higher education institutions. International Journal of Education and Development using ICT. 2019;15(1). doi:10.1007/978-94-017-9553-1_531-1
4. Hickle RS, Allen CK, Derouen JP. Computer assisted patient navigation and information systems and methods. Google Patents; 2019.
5. Meskarpour-Amiri M, Dopeykar N, Mehdizadeh P, Ayoubian A, Motaghed Z. A study on the factors affecting the prescription of injection medicines in Iran: a policy making approach. Global Journal of Health Science. 2015;7(3):291. doi:10.5539/gjhs.v7n3p291
6. Faroukhzad M, Farokhzad N, Dehghani M. The role of electronic records on the delivery of health information. Univ Learn J. 2011;2:28-36.
7. Susanto H, bin Muhaya F, editors. Multimedia information security architecture framework. 2010 5th International Conference on Future Information Technology; 2010: IEEE. doi:10.1109/FUTURETECH.2010.5482696
8. Fernando J. Factors that have contributed to a lack of integration in health information system security. The Journal on Information Technology in Healthcare. 2004;2(5):313-28.
9. Heeks R. Health information systems: Failure, success and improvisation. International journal of medical informatics. 2006;75(2):125-37. doi:10.1016/j.ijmedinf.2005.07.024
10. Ismail W, Alwi NHM, Ismail R, Bahari M, Zakaria O. Readiness of Information Security Management Systems (ISMS) Policy on Hospital Staff Using e-Patuh System. Journal of Telecommunication, Electronic and Computer Engineering (JTEC). 2018;10(1-11):47-52.
11. Fenz S, Ekelhart A, Neubauer T. Information security risk management: In which security solutions is it worth investing? Communications of the Association for Information Systems. 2011; 28 (1): 22. doi:10.17705/1CAIS.02822
12. Ghahremani E, Parandeh A, Vafadar Z, Ebadi A. Survey of the occupational hazards and related factors in health care workers in military hospitals during 2016-2017. Journal of Military Medicine. 2018; 20(1):56-64.
13. Foroughi F, editor. Information asset valuation method for information technology security risk assessment. Proceedings of the World Congress on Engineering; 2008.
14. Kwon J, Johnson ME. Security practices and regulatory compliance in the healthcare industry. Journal of the American Medical Informatics Association. 2013;20(1):44-51. doi:10.1136/amiajnl-2012-000906
15. Ray A, Newell S. Exploring information security risks in healthcare systems. Health Information Systems: Concepts, Methodologies, Tools, and

Applications: IGI Global; 2010. p. 1713-9. doi:10.4018/978-1-60566-988-5.ch110
16. Henderson JC, Venkatraman H. Strategic alignment: Leveraging information technology for transforming organizations. IBM systems journal. 1999;38(2.3):472-84. doi:10.1147/SJ.1999.5387096
17. Zaboli R, Shokri M, Javadi MS, Teymourzadeh E, Ameryoun A. Factors Affecting Quality of Emergency Service in Iran's Military Hospitals: A Qualitative Study. Electronic physician. 2016;8(9): 2990. doi:10.19082/2990
18. Sharifian R, Nematollahi M, Monem H, Ebrahimi F. Evaluating the security safeguards in hospital information system according to the health insurance portability and accountability act of university hospitals in Shiraz University of Medical Sciences. 2013.
19. Danayi Fard H. Methodology of quantitative research in management. Tehran: Safar. 2004.
20. Teo TS, Liu J. Consumer trust in e-commerce in the United States, Singapore and China. Omega. 2007;35(1):22-38. doi:10.1016/j.omega.2005.02.001
21. Tabibi S, Farhangi A, Nasiripour A, Kazemzadeh R, Ebrahimi P. Association between harrison cultural typology and acceptance of hospital information system. Health Inf Manage. 2013;10(3):380-90.
22. Aloul FA. The need for effective information security awareness. Journal of Advances in Information Technology. 2012;3(3):176-83. doi:10.4304/jait.3.3.176-183
23. Van Niekerk J, Von Solms R. Information security culture: A management perspective. Computers & security. 2010;29(4):476-86. doi:10.1016/j.cose.2009.10.005
24. Fernando JI, Dawson LL. The health information system security threat lifecycle: An informatics theory. International Journal of Medical Informatics. 2009;78(12):815-26. doi:10.1016/j.ijmedinf.2009.08.006
25. Rezgui Y, Marks A. Information security awareness in higher education: An exploratory study. Computers & Security. 2008;27(7-8):241-53. doi:10.1016/j.cose.2008.07.008
26. Kritzinger E, Smith E. Information security management: An information security retrieval and awareness model for industry. Computers & Security. 2008;27(5-6):224-31. doi:10.1016/j.cose.2008.05.006
27. Kruger H, Steyn T, Drevin L, Medlin BD. How secure are passwords that will be used by future health care workers? Redefining an agenda for Information Security. 2008:2-3.
28. Saran M, Zavarsky P, editors. A Study of the Methods for Improving Internet Usage Policy Compliance. 2009 International Conference on Computational Science and Engineering; 2009: IEEE. doi:10.1109/CSE.2009.10
29. Fernández-Alemán JL, Sánchez-Henarejos A, Toval A, Sánchez-García AB, Hernández-Hernández I, Fernandez-Luque L. Analysis of health professional security behaviors in a real clinical setting: An empirical study. International journal of medical informatics. 2015;84(6):454-67. doi:10.1016/j.ijmedinf.2015.01.010
30. Datta G, Ambassador H, Entwistle M. HL7 Is Foundational To Achieving Meaningful Use. Learning OpenCV. 2012.
31. Narayana Samy G, Ahmad R, Ismail Z. Security threats categories in healthcare information systems. Health informatics journal. 2010;16(3):201-9. doi:10.1177/1460458210377468
32. Joubert P, editor. Minimum critical technical success factors for e-development projects: A maturity model. Proceedings of the 9th International Conference on Social Implications of Computers in Developing Countries, São Paulo, Brazil; 2007.
33. Daniel F. A portable approach to exception handling in workflow management systems. Politecnico di Milano-Dipartimento di Elettronica e Informazione, Tech Rep. 2006.
34. Zandesh Z. EHR architecture and standards infrastructure. Amirkabir University of Technology, School of Biomedical Engineering. Hospital Information Systems. Health Inf Manage. 2014;10 (6):788.
35. Safdari R, Sieyed Farsjalah S. Strategies to protect the rights of patients in EHR systems. J Med Purification. 2009;74:48-56.
36. Geum Y, Cho Y, Park Y. A systematic approach for diagnosing service failure: Service-specific FMEA and grey relational analysis approach. Mathematical and Computer Modelling. 2011;54(11-12):3126-42 doi:10.1016/j.mcm.2011.07.042