مجله پیاورد سلامت
دوره ۱۶، شماره ۶، بهمن ۱۴۰۱، ۵۴۸-۵۳۸
مقاله پژوهشی

تعیین اهمیت الزامات امنیت اطلاعات در شبکه پزشکی از راه دور از دیدگاه مدیران و کارکنان واحد فناوری اطلاعات دانشگاه علوم پزشکی و بیمارستان‌های آموزشی شهر بیرجند

فاطمه بهادر[۱]، اعظم صباحی[۲]، سمیه پایدار[۳]، فاطمه زنگوئی سنو[۴*]

دریافت مقاله: ۱۴۰۱/۵/۲۳
پذیرش مقاله: ۱۴۰۱/۱۰/۱۰

* نویسنده مسئول:
فاطمه زنگوئی سنو؛
دانشکده پیراپزشکی و بهداشت فردوس دانشگاه علوم پزشکی بیرجند

Email:
zangoei.f@bums.ac.ir

چکیده

زمینه و هدف: امروزه با پیشرفت تکنولوژی اطلاعات، استفاده از فناوری پزشکی از راه دور گسترش زیادی پیدا کرده است. اما از آن‌جاکه فناوری پزشکی از راه دور متکی بر انتقال داده‌هاست، توجه به مسایلی از جمله امنیت شبکه، محرمانگی و حفظ حریم خصوصی بیماران امری ضروری است. ازاین‌رو این مطالعه با هدف تعیین اهمیت الزامات امنیت اطلاعات در شبکه پزشکی از راه دور از دیدگاه مدیران و کارکنان واحد فناوری اطلاعات دانشگاه علوم پزشکی و بیمارستان‌های آموزشی شهر بیرجند انجام پذیرفت.

روش بررسی: این مطالعه به شیوه توصیفی مقطعی در سال ۱۴۰۰ انجام شد. جامعه‌ی پژوهش را مدیران و کارکنان واحد فناوری اطلاعات دانشگاه علوم پزشکی و بیمارستان‌های آموزشی شهر بیرجند(۴۰ نفر) تشکیل دادند که به‌صورت سرشماری مورد بررسی قرار گرفتند. ابزار مورد استفاده، پرسش‌نامه‌ی محقق‌ساخته بود که روایی توسط استادان و صاحب‌نظران تایید و پایایی آن با آلفای کرونباخ(۰/۸۳) محاسبه شد. داده‌ها پس از جمع آوری، در نرم‌افزار SPSS وارد و با استفاده از آمار توصیفی، تحلیل شدند.

یافته‌ها: یافته‌های پژوهش نشان داد که الزام امنیتی مربوط به انتقال اطلاعات از درجه اهمیت بالاتری نسبت به سایر الزامات برخوردار است. همچنین در زمینه‌ی منابع انسانی، ارایه مستندات دقیق و راهنمای آموزشی برای کاربران سیستم‌ها با میانگین(۴/۴۷)، در زمینه‌ی تجهیزات تشخیص پزشکی، مجهز بودن سیستم‌های شبکه پزشکی از راه دور به برق اضطراری با میانگین(۴/۷۲)، در زمینه‌ی ذخیره و دسترسی به اطلاعات مربوط، نصب آنتی‌ویروس‌ها و ضد بدافزارها بر روی تمامی سیستم‌ها با میانگین(۴/۷۵) و نیز در زمینه انتقال اطلاعات، رمزگذاری فایل‌ها و اطلاعات مهم و حساس با میانگین(۴/۶۹) مهم‌ترین نیاز امنیتی بودند.

نتیجه‌گیری: همان‌طورکه نتایج پژوهش نشان داد، الزامات امنیتی مربوط به انتقال اطلاعات از درجه‌ی اهمیت بالاتری نسبت به سایر الزامات برخوردار است؛ در ابتدا می‌توان با ایجاد سیاست‌های امنیتی، به‌روز رسانی و نظارت بر اجرای آن‌ها و همچنین آموزش به کارکنان تاحدود زیادی امنیت اطلاعات را تضمین کرد. اما جهت انتقال اطلاعات حساس پزشکی می‌توان از روش‌های رمزگذاری و تایید صلاحیت، پروتکل امن انتقال اطلاعات، شبکه‌های خصوصی و مجازی و سایر تکنولوژی‌های جدید در این زمینه استفاده کرد؛ البته در خصوص ایجاد زیرساخت‌های فنی مناسب جهت پیاده‌سازی سیاست‌های امنیتی در انتقال اطلاعات بایستی تمهیدات لازم صورت پذیرد.

واژه‌های کلیدی: پزشکی از راه دور، امنیت اطلاعات، فناوری اطلاعات، امنیت پزشکی از راه دور، امنیت اطلاعات پزشکی، امنیت مراقبت از راه دور

۱ دانشجوی دکتری مدیریت اطلاعات سلامت، دانشکده پیراپزشکی، دانشگاه علوم پزشکی تهران، تهران، ایران

۲ استادیار گروه فناوری اطلاعات سلامت، دانشکده پیراپزشکی و بهداشت فردوس، دانشگاه علوم پزشکی بیرجند، بیرجند، ایران

۳ استادیار گروه فناوری اطلاعات سلامت، دانشکده پیراپزشکی، دانشگاه علوم پزشکی کرمانشاه، کرمانشاه، ایران

۴ کارشناس فناوری اطلاعات سلامت، دانشکده پیراپزشکی و بهداشت فردوس، دانشگاه علوم پزشکی بیرجند، بیرجند، ایران

[DOR: 20.1001.1.17358132.1401.16.6.8.5]

مقدمه

امروزه که پیشرفت‌های فناوری اطلاعات، زندگی و محیط‌های کاری را با تغییرات عدیده‌ای مواجه کرده است، صنایع مختلف برای رقابت با سازمان‌های دیگر از فناوری اطلاعات استفاده می‌کنند. نظام سلامت نیز برای ارتقای سطح سلامت و بهبود نتایج بالینی و مالی خود نیازمند استفاده از آخرین دستاوردهای فناوری اطلاعات است(۱). یکی از فناوری‌های کاربردی در حوزه‌ی سلامت، فناوری پزشکی از راه دور یا تله‌مدیسین است. سازمان جهانی بهداشت تله‌مدیسین (Telemedicine) را«عمل مراقبت‌های پزشکی با استفاده از تعامل صدا و تصویر و داده‌های انتقالی شامل مراقبت‌های پزشکی و تشخیص، مشاوره‌ی درمان و همچنین آموزش و انتقال اطلاعات پزشکی» تعریف می‌کند(۲). پزشکی از راه دور یک حوزه‌ی بین‌رشته‌ای متشکل از پزشکی، فناوری اطلاعات و فناوری ارتباطات از راه دور است و هدف اولیه آن حمایت از بیمارانی است که به‌علت فاصله جغرافیایی، قادر به دسترسی سریع و به‌موقع به خدمات بهداشتی درمانی نیستند(۳). همان‌طورکه مشخص است به‌کارگیری هر تکنولوژی در هر زمینه‌ای با مزایا و چالش‌هایی همراه است که شناسایی و تعیین این چالش‌ها سبب پیشگیری و رفع مشکلات احتمالی در مسیر فعالیت‌ها می‌شود.

از مزایای تله‌مدیسین می‌توان به بهبود مراقبت از بیمار، کاهش هزینه‌های ارایه خدمات سلامت، مدیریت بحران در بخش سلامت، کنترل بیماری‌های مزمن و بهره‌مندی یکسان و عادلانه از خدمات بهداشتی و غیره اشاره کرد(٤و۲). پزشکی از راه دور مدل نوینی از ارتباط بین پزشک و بیمار است(٤) که مشاوره تلفنی بین پزشک و بیمار، مشاوره پزشکی بین صاحبان حِرَف پزشکی، ویزیت‌های اینترنتی، نظارت بر عمل جراحی و حتی خود عمل جراحی نمونه‌هایی از خدمات پزشکی از راه دور هستند که اطلاعات پزشکی بیمار و پرونده پزشکی وی در این نوع خدمات مبادله می‌شوند. ازاین‌رو حفظ امنیت اطلاعات مبادله‌شده از اهمیت بسزایی برخوردار است(۳). شناسایی چالش‌های موجود در این حوزه از قبیل حریم شخصی و محرمانگی و امنیت ضروری است(٤)؛ چراکه حفظ و نگهداری فیزیکی سیستم‌ها و اطمینان از حریم شخصی و امنیت اطلاعات بیماران که جزو حساس‌ترین و محرمانه‌ترین اطلاعات می‌باشد از اهمیت بسزایی برخوردار است(٦و٥). افزایش تبادل اطلاعات بین بیماران و ارایه‌دهندگان خدمات بهداشتی، اطلاعات و سیستم‌های اطلاعاتی را در معرض خطراتی از جمله افشای اطلاعات سلامت اشخاص، جعل عناوین خاص پزشکی، انتقال ویروس‌ها به شبکه‌های اینترنتی، استماع غیرمجاز ارتباطات و در نهایت افشای اطلاعات قرار می‌دهد(۷و٦).

بررسی‌های انجام‌شده در آمریکا حاکی از آن است که ۷۵ درصد افراد از افشای غیرمجاز و به اشتراک گذاشتن اطلاعات بر روی شبکه‌ها و وب‌سایت‌ها نگرانند(۸). در ایالات‌متحدآمریکا نیز امنیت فناوری پزشکی از راه دور موضوعی بسیار مهم برای سیاستگذاران در این زمینه است که پیاده‌سازی استانداردهای امنیتی به‌منظور اطمینان از ارایه ایمن و محرمانه خدمات پزشکی از راه دور یکی از این سیاست‌هاست(۹). مطالعات جدید نشان می‌دهد که تهدیدات امنیتی سیستم‌های اطلاعات مراقبت سلامت در سال‌های اخیر پیشرفت چشم‌گیری داشته است(۱۰). بنابراین ضروری است که مراکز بهداشتی درمانی، اقدام به ایجاد راهکارهای امنیتی برای حفظ حقوق اطلاعاتی بیماران نمایند؛ ازآن‌جاکه مدیران فناوری اطلاعات که بیشترین ارتباط را با داده‌های متنوع در نظام سلامت دارند و به‌عنوان برنامه‌ریزان و تصمیم‌گیران اصلی و مشاوران سیستم‌های بهداشتی محسوب می‌شوند(۱۱)، در این راستا در درجه اول باید حوزه‌ها و زیرمجموعه‌های مرتبط با امنیت اطلاعات شناسایی گردد؛ تا با بررسی الزامات امنیتی در حوزه‌های مرتبط بتوان راهکارهای موثر و عملی را جهت ارتقای سطح امنیت اطلاعات در فناوری پزشکی از راه دور ارایه نمود. مطالعات متعددی در زمینه‌ی امنیت اطلاعات در حوزه‌های مختلف انجام گرفته است. مشابه پژوهش حاضر، مطالعه‌ی حسینیان نیز به بررسی الزامات امنیت از جنبه‌های ذخیره‌سازی و دسترسی به اطلاعات، منابع انسانی، انتقال اطلاعات و تجهیزات تشخیص پزشکی می‌پردازد(۱۲). اما از آن‌جاکه در مراکز درمانی مختلف تجهیزات و زیرساخت‌های پزشکی از راه دور، متنوع و مختلف است و هر مرکز درمانی سیاست و اولویت‌های امنیتی خاص خود را دارد، انجام این تحقیق در سایر مراکز می‌تواند مهم‌ترین جنبه‌های امنیتی را مشخص کرده و پیشنهادهایی جهت حل مشکلات در این زمینه ارایه نماید. ازاین‌رو هدف این مطالعه، تعیین میزان اهمیت هریک از جنبه‌های امنیت اطلاعات در به‌کارگیری فناوری پزشکی از راه‌دور از دیدگاه مدیران و کارکنان واحد فناوری اطلاعات دانشگاه علوم پزشکی و بیمارستان‌های آموزشی شهر بیرجند می‌باشد.

روش بررسی

پژوهش حاضر از نوع مطالعات توصیفی و کاربردی بود که به‌صورت مقطعی در سال ۱٤۰۰ در دانشگاه علوم پزشکی و بیمارستان‌های آموزشی بیرجند انجام شد. شهر بیرجند دارای سه بیمارستان آموزشی(ولیعصر، امام

[DOR: 20.1001.1.17358132.1401.16.6.8.5]

رضا و رازی) می‌باشد و جامعه‌ی پژوهش را مدیران و کارکنان واحد فناوری اطلاعات دانشگاه علوم پزشکی و بیمارستان‌های آموزشی شهر بیرجند(٤٠ نفر) تشکیل دادند. نظر به محدودبودن تعداد افراد جامعه پژوهش، نمونه‌گیری انجام نشد و با استفاده از روش سرشماری از کلیه افراد برای شرکت در پژوهش به‌طور حضوری دعوت شد. ابزار گردآوری داده‌ها پرسش‌نامه‌ی محقق‌ساخته بود که با الگوبرداری از پرسش‌نامه‌ی حسینیان و همکاران(١٢) طراحی شد، به‌طوری‌که یک بُعد به پرسش‌نامه‌ی مذکور اضافه گردید و مجدداً روایی آن توسط چهار نفر از استادان و صاحب‌نظران حوزه‌ی فناوری اطلاعات سلامت بررسی و تایید شد. پایایی آن با استفاده از آلفای کرونباخ(α=٠/٨٣) تعیین گردید. این پرسش‌نامه، شامل پنج قسمت بود. قسمت اول سوالات مربوط به مشخصات دموگرافیک افراد شرکت‌کننده در پژوهش(٥ سوال) بود و قسمت‌های دوم تا پنجم سوالات تعیین درجه اهمیت الزامات امنیت اطلاعات در فناوری پزشکی از راه دور در زمینه‌ی انتقال اطلاعات(٧ سوال)، منابع انسانی(٨ سوال)، تجهیزات تشخیص پزشکی(١٣ سوال) و ذخیره و دسترسی به اطلاعات(١٤ سوال) را در بر گرفت. این پرسش‌نامه بر اساس مقیاس پنج‌گزینه‌ای لیکرت (likert) طراحی شد؛ امتیاز هریک از گزینه‌ها به شرح زیر بود: بسیارمهم(امتیاز=٥)، مهم(امتیاز=٤)، نظری ندارم(امتیاز=٣)، کم‌اهمیت(امتیاز=٢) و بی‌اهمیت(امتیاز=١). به‌منظور تحلیل داده‌ها از نرم‌افزار SPSS استفاده شد و نتایج با استفاده از آمار توصیفی(میانگین و انحراف‌معیار) در قالب جدول گزارش گردیدند. برای محاسبه‌ی درجه اهمیت هریک از الزامات امنیتی در کل و براساس امتیازبندی، ابتدا مجموع امتیازات برای هر پرسش‌نامه به‌طور جداگانه و بر مبنای امتیاز ١ تا ٥ محاسبه گردید و با توجه به سقف امتیازات که ٥ بود، اهمیت الزامات امنیتی از دیدگاه افراد شرکت‌کننده در پژوهش در نظر گرفته شد. سپس از هر بُعد، میانگین کل برای ردیف بسیارمهم و مهم محاسبه شد و در نهایت، با توجه به مقایسه میانگین کل ابعاد به‌دست آمده، الزامات امنیتی شبکه پزشکی از راه دور رتبه‌بندی شدند.

یافته‌ها

پژوهش حاضر، متشکل از ٤٠ نفر از صاحب‌نظران بود که ٣٢ نفر پرسش‌نامه را تکمیل نموده و عودت دادند.

جدول ١: اطلاعات دموگرافیک شرکت‌کنندگان

متغیر		فراوانی	درصد
جنسیت	زن	١٠	٪٣١/٣
	مرد	٢٢	٪٦٨/٧
نوع استخدام	رسمی	١٦	٪٥٠
	پیمانی	٤	٪١٢/٥
	قراردادی	٦	٪١٨/٨
	سایر	٦	٪١٨/٨
میزان تحصیلات	فوق‌دیپلم	٥	٪١٥/٦
	لیسانس	٢٤	٪٧٥
	فوق‌لیسانس	٣	٪٩/٤
سابقه‌کاری	١-٥	١٢	٪٣٧/٥
	٦-١٠	١٢	٪٣٧/٥
	١١-١٥	٤	٪١٢/٥
	١٦-٢٠	٤	٪١٢/٥
	٢٠-٢٥	١	٪٣/١
	٢٦-٣٠	٩	٪٢٨/١
سن	٣١-٣٥	١٠	٪٣١/٢
	٣٦-٤٠	٩	٪٢٨/١
	٤١-٤٥	٣	٪٩/٣

همان‌طورکه در جدول ۱ آمده است، نتایج پژوهش نشان داد که توزیع آماری جامعه پژوهش، عبارت از ۳۱/۳ درصد(۱۰ نفر) زن و ۶۸/۷ درصد(۲۲ نفر) مرد بودند. میانگین سنی شرکت‌کنندگان ۳۴/۰۳ سال و حداقل و حداکثر سن آن‌ها ۲۵ و ۴۵ سال بود. همچنین میانگین سابقه‌کاری آن‌ها ۸/۴۱ سال بود. نوع استخدام ۵۰ درصد شرکت‌کنندگان رسمی و ۷۵ درصد آن‌ها دارای مدرک لیسانس بودند. محل خدمت ۷۵ درصد(۲۴ نفر) بیمارستان‌های آموزشی شهر بیرجند و ۲۵ درصد(۸ نفر) دانشگاه علوم پزشکی بیرجند بود.

جدول ۲: درجه اهمیت الزامات امنیت اطلاعات در شبکه پزشکی از راه دور در زمینه‌ی انتقال اطلاعات

الزامات امنیت اطلاعات در شبکه پزشکی از راه دور در زمینه‌ی انتقال اطلاعات	بسیارمهم	مهم	نظری ندارم	کم‌اهمیت	بی‌اهمیت	میانگین±انحراف‌معیار
	تعداد(٪)	تعداد(٪)	تعداد(٪)	تعداد(٪)	تعداد(٪)	
پیاده‌سازی پروتکل‌های شبکه‌ای برای اطمینان از ارسال اطلاعات	۲۳(۷۱/۹)	۸(۲۵)	۰	۲(۳/۱)	۰	۴/۶۶±۰/۶۵
ایجاد پروتکل ارتباطی برای به اشتراک‌گذاشتن اطلاعات بین موسسات بهداشتی محلی و ملی	۱۷(۵۳/۱)	۱۱(۳۴/۴)	۴(۱۱)	۰	۰	۴/۴۱±۰/۷۱
رمزگذاری فایل‌ها و اطلاعات مهم و حساس	۲۲(۳۱/۳)	۱۰(۶۸/۷)	۰	۰	۰	۴/۶۹±۰/۴۷
بررسی مکانیسم رمزگذاری توسط تیم فنی ارزیاب امنیت	۲۲(۶۸/۷)	۷(۲۱/۹)	۱(۳/۱)	۲(۶/۳)	۰	۴/۵۳±۰/۸۴
استفاده از ترکیب اعداد، حروف بزرگ و کوچک جهت رمزگذاری سیستم‌های شبکه پزشکی از راه دور	۱۶(۵۰)	۱۲(۳۷/۵)	۲(۶/۳)	۱(۳/۱)	۱(۳/۱)	۴/۲۸±۰/۹۶
اجرای مکانیسم‌هایی جهت یکپارچگی اطلاعات برنامه‌های کاربردی	۱۶(۵۰)	۱۳(۴۰/۶)	۲(۶/۳)	۱(۳/۱)	۰	۴/۳۷±۰/۷۵
به‌کارگیری معیارهای کنترل کیفی داده‌ها	۱۶(۵۰)	۱۳(۴۰/۶)	۲(۶/۳)	۱(۳/۱)	۰	۴/۳۷±۰/۷۵

در ارتباط با الزامات امنیت اطلاعات در شبکه پزشکی از راه دور در زمینه‌ی انتقال اطلاعات مطابق جدول ۲ یافته‌های پژوهش بیانگر آن بود که بیشترین میانگین ۴/۶۹±۰/۴۷ مربوط به«رمزگذاری فایل‌ها و اطلاعات مهم و حساس» و کمترین میانگین ۴/۲۸±۰/۹۶ مربوط به«استفاده از ترکیب اعداد، حروف بزرگ و کوچک جهت رمزگذاری سیستم‌های شبکه پزشکی از راه دور» بودند.

جدول ۳: درجه اهمیت الزامات امنیت اطلاعات در شبکه پزشکی از راه دور در زمینه‌ی منابع انسانی

الزامات امنیت اطلاعات در شبکه پزشکی از راه دور در زمینه‌ی منابع انسانی	بسیار مهم	مهم	نظری ندارم	کم‌اهمیت	بی‌اهمیت	میانگین±انحراف‌معیار
	تعداد(٪)	تعداد(٪)	تعداد(٪)	تعداد(٪)	تعداد(٪)	
تفویض اختیار به کاربران در جهت ارایه خدمات بر اساس قوانین حرفه‌ی خود	۱۲(۳۷/۵)	۱۴(۴۳/۸)	۴(۱۲/۵)	۲(۶/۳)	۰	۴/۱۲±۰/۸۷
پیاده‌سازی روش‌هایی برای اطمینان از دسترسی به موقع تمام کاربران به اطلاعات	۱۱(۳۴/۴)	۱۸(۶۵/۳)	۳(۹/۴)	۰	۰	۴/۲۵±۰/۶۲
پیاده‌سازی سیاست‌ها و روش‌های مناسب برای دسترسی به اطلاعات الکترونیکی سلامت درموارد اورژانسی	۱۵(۴۶/۹)	۱۳(۴۰/۶)	۳(۹/۴)	۱(۳/۱)	۰	۴/۳۱±۰/۷۸
به‌کارگیری افراد متخصص برای پشتیبانی از فناوری مورد استفاده در روش‌های پزشکی از راه دور	۱۸(۵۶/۳)	۱۱(۳۴/۴)	۱(۳/۱)	۲(۶/۳)	۰	۴/۴۱±۰/۸۴
آگاهی دادن به کاربران در خصوص قوانین و استانداردهای محرمانگی و حریم خصوصی بیماران	۱۷(۵۳/۱)	۱۰(۳۱/۳)	۳(۹/۴)	۲(۶/۳)	۰	۴/ ۳۱±۰/۸۹
آگاهی دادن به کاربران در خصوص عواقب قانونی ناشی از افشای اسرار بیماران	۱۹(۵۹/۴)	۹(۲۸/۱)	۲(۶/۳)	۲(۶/۳)	۰	۴/۴۱±۰/۸۷
ارایه مستندات دقیق و راهنماهای آموزشی برای کاربران سیستم‌های شبکه پزشکی از راه دور	۱۶(۵۰)	۱۵(۴۶/۹)	۱(۳/۱)	۰	۰	۴/۴۷±۰/۵۸
همکاری با افراد مسئول جهت کنترل و بررسی موارد امنیتی در شبکه پزشکی از راه دور	۱۸(۵۶/۳)	۹(۲۸/۱)	۳(۹/۴)	۱(۳/۱)	۱(۳/۱)	۴/۳۱±۰/۹۹

جدول ۳ الزامات امنیت اطلاعات در شبکه پزشکی از راه دور در زمینه‌ی منابع انسانی را نشان می‌دهد که طبق این جدول«ارایه مستندات دقیق و راهنماهای آموزشی برای کاربران سیستم‌های شبکه پزشکی از راه دور» با میانگین ۴/۴۷±۰/۵۸ و تفویض اختیار به کاربران در جهت ارایه خدمات بر اساس قوانین حرفه‌ی خود با میانگین ۴/۱۲±۰/۸۷، بیشترین و کمترین میانگین را به خود اختصاص دادند.

[DOR: 20.1001.1.17358132.1401.16.6.8.5]

جدول ۴: درجه اهمیت الزامات امنیت اطلاعات در زمینه‌ی تجهیزات تشخیص پزشکی

الزامات امنیت اطلاعات در شبکه پزشکی از راه دور در زمینه‌ی تجهیزات تشخیص پزشکی	بسیار مهم	مهم	نظری ندارم	کم‌اهمیت	بی‌اهمیت	میانگین±انحراف‌معیار
	تعداد(٪)	تعداد(٪)	تعداد(٪)	تعداد(٪)	تعداد(٪)	
تبادل دیجیتالی سیگنال‌های ویدیویی و تصاویر آنالوگ	۱۳(۴۰/۶)	۱۵(۴۶/۹)	۳(۹/۴)	۰	۱(۳/۱)	۴/۲۲±۰/۸۷
وجود تجهیزات مخصوص برای ارتباط از راه دور با سیستم‌های اطلاعات	۱۹(۵۹/۴)	۱۰(۳۱/۳)	۲(۶/۳)	۱(۳/۱)	۰	۴/۴۷±۰/۷۶
پهنای باند و رابط‌های کاربری برای تجهیزات شبکه و تجهیزات تشخیصی پزشکی	۱۸(۵۶/۳)	۹(۲۸/۱)	۴(۱۲/۵)	۱(۳/۱)	۰	۴/۳۷±۰/۸۳
وجود رسانه‌های ذخیره‌سازی الکترونیکی	۱۷(۵۳/۱)	۱۳(۴۰/۶)	۲(۶/۳)	۰	۰	۴/۴۷±۰/۶۲
اطمینان از به‌روزرسانی مداوم تجهیزات شبکه	۱۳(۴۰/۶)	۱۵(۴۶/۹)	۳(۹/۴)	۱(۳/۱)	۰	۴/۲۵±۰/۷۶
به‌کارگیری استانداردها برای پیکربندی تجهیزات پزشکی از راه دور	۱۸(۵۶/۳)	۸(۲۵)	۶(۱۸/۸)	۰	۰	۴/۳۷±۰/۷۹
مجهز بودن سیستم‌های شبکه پزشکی از راه دور به برق اضطراری	۲۴(۷۵)	۷(۲۱/۹)	۱(۳/۱)	۰	۰	۴/۷۲±۰/۵۲
استفاده از اتاق سرور استاندارد و مجهز به سیستم‌های هشدار(از قبیل سیستم هشدار حریق)	۲۴(۷۵)	۶(۱۸/۸)	۱(۳/۱)	۰	۱(۳/۱)	۴/۶۲±۰/۸۳
وجود فرایندهایی برای اطمینان از ایمنی تجهیزات پزشکی از راه دور	۲۰(۶۲/۵)	۸(۲۵)	۳(۹/۴)	۱(۳/۱)	۰	۴/۴۷±۰/۸۰
اطمینان از در دسترس‌بودن تجهیزات پزشکی از راه دور برای پشتیبانی از نیازهای تشخیصی	۲۰(۶۲/۵)	۷(۲۱/۹)	۵(۱۵/۶)	۰	۰	۴/۴۷±۰/۷۶
اطمینان از عملکرد صحیح تجهیزات پزشکی از راه دور در زمان ارایه مراقبت بالینی	۲۱(۶۵/۶)	۷(۲۱/۹)	۴(۱۲/۵)	۰	۰	۴/۵۳±۰/۷۲
وجود دستورالعمل‌های مطابق با الزامات سازمانی، حقوقی و نظارتی	۱۵(۴۶/۹)	۱۱(۳۴/۴)	۴(۱۲/۵)	۲(۶/۳)	۰	۴/۲۲±۰/۹۱
وجود دستورالعمل‌هایی برای اطمینان از امنیت فیزیکی تجهیزات پزشکی از راه دور	۱۶(۵۰)	۱۱(۳۴/۴)	۲(۶/۳)	۳(۹/۴)	۰	۴/۲۵±۰/۹۵

بر اساس یافته‌های پژوهش که در جدول ۴ آمده است، از دیدگاه افراد شرکت‌کننده در پژوهش، بیشترین میانگین الزامات امنیت اطلاعات در شبکه پزشکی از راه دور در زمینه‌ی تجهیزات تشخیص پزشکی مربوط به«مجهز بودن سیستم‌های شبکه‌ی پزشکی از راه دور به برق اضطراری» با میانگین ۴/۷۲±۰/۵۲ و کمترین میانگین به«تبادل دیجیتالی سیگنال‌های ویدیویی و تصاویر آنالوگ» ۴/۲۲±۰/۸۷ و «وجود دستورالعمل‌های مطابق با الزامات سازمانی، حقوقی و نظارتی» ۴/۲۲±۰/۹۱ تعلق داشت.

جدول ۵: درجه اهمیت الزامات امنیت اطلاعات در شبکه پزشکی از راه دور در زمینه‌ی ذخیره و دسترسی به اطلاعات

الزامات امنیت اطلاعات در شبکه پزشکی از راه دور در زمینه‌ی ذخیره و دسترسی به اطلاعات	بسیار مهم	مهم	نظری ندارم	کم‌اهمیت	بی‌اهمیت	میانگین±انحراف‌معیار
	تعداد(٪)	تعداد(٪)	تعداد(٪)	تعداد(٪)	تعداد(٪)	
ذخیره‌ی اطلاعات سلامت شخصی تولیدشده بین ارایه‌دهنده و بیمار با هر ظرفیتی در سیستم پزشکی از راه دور	۱۱(۳۴/۴)	۱۳(۴۰/۶)	۷(۲۱/۹)	۱(۳/۱)	۰	۴/۰۶±۰/۸۴
ارایه راهنمایی از سمت سیستم پزشکی از راه دور به کاربران در مورد نحوه‌ی ذخیره‌سازی اطلاعات سلامت شخصی در شبکه و سیستم‌های پزشکی از راه دور	۱۰(۳۱/۳)	۱۴(۴۳/۸)	۷(۲۱/۹)	۱(۳/۱)	۰	۴/۰۳±۰/۸۲
نظارت بر ذخیره‌ی هریک از داده‌های منتقل‌شده در یک جلسه پزشکی از راه دور برای هر بیمار روی هارد یا دیسک کامپیوتر در شبکه پزشکی از راه دور	۱۰(۳۱/۳)	۱۲(۳۷/۵)	۶(۱۸/۸)	۴(۱۲/۵)	۰	۳/۸۷±۱/۰۱
پاک شدن اطلاعات ذخیره‌شده از راه دور در سیستم سلامت از راه دور در صورت استفاده از تلفن همراه در شبکه(مثل مفقود شدن یا خرابی تلفن همراه)	۱۶(۵۰)	۶(۱۸/۸)	۹(۲۸/۱)	۰	۱(۳/۱)	۴/۱۲±۱/۰۴
اتصال به شبکه‌های امن(مانندVPN) هنگام استفاده از سیستم‌ها در شبکه‌ی پزشکی از راه دور و اجتناب از ورود به شبکه‌های ناامن (Wi-Fi عمومی)	۱۹(۵۹/۴)	۱۰(۳۱/۳)	۲(۶/۳)	۱(۳/۱)	۰	۴/۴۷±۰/۷۶
استفاده از شبکه‌های خصوصی مجازی (VPN) برای دسترسی به وب‌سایت‌های مهم	۱۷(۵۳/۱)	۹(۲۸/۱)	۵(۱۵/۶)	۱(۳/۱)	۰	۴/۳۱±۰/۸۶
نصب آنتی‌ویروس‌ها و ضدبدافزارها بر روی تمامی سیستم‌ها در شبکه پزشکی از راه دور	۲۵(۷۸/۱)	۶(۱۸/۸)	۱(۳/۱)	۰	۰	۴/۷۵±۰/۵۱
اجازه‌ی دسترسی به افراد واجد شرایط(دارای گواهینامه‌ی مناسب در زمینه امنیت و حریم خصوصی) جهت ارزیابی اطلاعات ذخیره شده در شبکه پزشکی از راه دور	۱۶(۵۰)	۱۳(۴۰/۶)	۳(۹/۴)	۰	۰	۴/۴۱±۰/۶۶
اجازه دسترسی بیمار به اطلاعات جهت افشای اطلاعات در صورت ارایه مجوز کتبی	۱۱(۳۴/۴)	۷(۲۱/۹)	۱۱(۳۴/۴)	۲(۶/۳)	۱۱(۳/۱)	۳/۷۸±۱/۱

[DOR: 20.1001.1.17358132.1401.16.6.8.5]

لزوم کسب اطمینان از احراز هویت بیمار و ارایه‌دهنده جهت دسترسی و حضور در جلسات پزشکی از راه دور	(۵۹/٤)۱۹	(۱۲/۵)٤	(۲۸/۱)۹	۰	٤/۳۱±۰/۸۹
لزوم کسب اطمینان از رمزگذاری‌های قوی جهت دسترسی به سیستم‌های شبکه پزشکی از راه دور	(۵۹/٤)۱۹	(۳۱/۳)۱۰	(٦/۳)۲	(۳/۱)۱	٤/٤٤±۰/۸۸
اعمال کنترل‌های دسترسی از جمله کنترل دسترسی مبتنی بر نقش، کنترل مبتنی بر کار و کنترل مبتنی بر زمینه	(٤٦/۹)۱۵	(٤۰/٦)۱۳	(۱۲/۵)٤	۰	٤/۳٤±۰/۷۰
رمزگذاری تمامی دستگاه‌های هوشمند که دسترسی به جلسات پزشکی از راه دور دارند	(۵۳/۱)۱۷	(۳۱/۳)۱۰	(۱۵/٦)۵	۰	٤/۳۷±۰/۷۵
اخذ رضایت آگاهانه از بیمار جهت ذخیره و ضبط و عکس‌برداری از جلسات پزشکی از راه دور و اشتراک‌گذاری اطلاعات سلامت شخصی و با سایر درخواست‌کنندگان	(٦۸/۸)۲۲	(۲۱/۹)۷	(٦/۳)۲	(۳/۱)۱	٤/۵٦±۰/۷٦

طبق جدول ۵ که مربوط به الزامات امنیت اطلاعات در شبکه پزشکی از راه دور در زمینه‌ی ذخیره و دسترسی به اطلاعات بود، شرکت‌کنندگان«نصب آنتی‌ویروس‌ها و ضد بدافزارها بر روی تمامی سیستم‌ها در شبکه پزشکی از راه دور» با میانگین ٤/۷۵±۰/۵۱ را مهم‌ترین الزام می‌دانستند. «اجازه دسترسی بیمار به اطلاعات جهت افشای اطلاعات در صورت ارایه مجوز کتبی» نیز کمترین میانگین ۳/۷۸±۱/۱ را به خود اختصاص داده بود.

جدول ۶: درجه اهمیت الزامات امنیت اطلاعات در فناوری پزشکی از راه دور

ابعاد	بسیار مهم	مهم	میانگین
انتقال اطلاعات	۵۳/۵	۳۸/۳	٤۵/۹
منابع انسانی	٤۹/۲	۳۹/۸	٤٤/۵
تجهیزات تشخیص پزشکی	۵۷/۲	۳۰/۵	٤۳/۸
ذخیره و دسترسی به اطلاعات	٤٦/٤	۲۹/۹	۳۸/۱

براساس جمع‌بندی یافته‌های پژوهش که در جدول ٦ آمده است، از دیدگاه افراد شرکت‌کننده در پژوهش، الزامات امنیت اطلاعات در فناوری پزشکی از راه دور در زمینه‌ی انتقال اطلاعات و منابع انسانی از میانگین بالاتر و اهمیت بیشتری برخوردار بودند. سایر الزامات امنیت اطلاعات در شبکه پزشکی از راه دور در زمینه‌ی ذخیره‌سازی و دسترسی به اطلاعات و تجهیزات تشخیص پزشکی از نظر اهمیت در سطوح بعدی قرار داشتند.

بحث

پژوهش حاضر به‌منظور تعیین اهمیت الزامات امنیت اطلاعات در شبکه پزشکی از راه دور از دیدگاه مدیران و کارکنان واحد فناوری اطلاعات دانشگاه علوم پزشکی و بیمارستان‌های آموزشی شهر بیرجند انجام گرفت.

هدف اول پژوهش، تعیین اهمیت الزامات امنیت اطلاعات در فناوری پزشکی از راه دور در زمینه‌ی انتقال اطلاعات از دیدگاه مدیران و کارکنان واحد فناوری اطلاعات دانشگاه علوم پزشکی و بیمارستان‌های آموزشی شهر بیرجند بود. یافته‌های به‌دست آمده این بود که مهم‌ترین نیاز امنیتی مربوط به رمزگذاری فایل‌ها و اطلاعات مهم و حساس و کم‌اهمیت‌ترین نیاز امنیتی، استفاده از ترکیب اعداد، حروف بزرگ و کوچک جهت رمزگذاری سیستم‌های شبکه پزشکی از راه دور بودند. پژوهش کرمی و همکاران(۱۳۹۲) که با هدف شناخت اقدامات امنیتی رایجی که برای کاهش خطرهای بالقوه برای اطلاعات بهداشتی می‌تواند به‌کار گرفته شود، انجام شد و به روش‌های تایید صلاحیت و سیستم‌های شناسایی بیومتریک اشاره کرد(۱۳). پژوهش فرزندی‌پور و همکاران(۱۳۸٦)، با هدف طراحی الگوی الزامات ایمنی اطلاعات پرونده الکترونیک سلامت برای ایران انجام گرفت و تاکید کرد که جهت طراحی پرونده الکترونیک سلامت باید برای تمام کاربران مجاز، نام کاربری و رمز عبور تعریف و در موارد لزوم از سیستم‌های بیومتریک استفاده شود تا امکان شناسایی کاربران اطلاعات و ردیابی داده‌ها فراهم شود(۱٤). پژوهش Zain و Clarke (۲۰۰۵) که با هدف ایمن‌سازی پزشکی از راه دور از نظر حملات به امنیت با مشاهده‌ی عملکرد سیستم‌های کامپیوتری انجام گرفت، به واترمارکینگ تصاویر پزشکی به‌عنوان یکی از ابزارهای امنیتی تاکید داشت(۱۵). همچنین Magdy و همکاران(۲۰۲۲) در پژوهشی که با هدف ارزیابی الگوریتم‌های مختلف در رابطه با امنیت تصاویر پزشکی انجام دادند، استگانوگرافی دیجیتال را برای جلوگیری از جاسوسی در داده‌های ارسال شده ایمن پیشنهاد دادند و واترمارکینگ را یک راه‌حل مناسب

[DOR: 20.1001.1.17358132.1401.16.6.8.5]

برای اطمینان از تشخیص دستکاری و تایید مالکیت دانستند(۱۶). بنابراین نتایج پژوهش‌های کرمی و همکاران(۱۳)، فرزندی‌پور و همکاران(۱۴)، Zain و Clarke (۱۵) و Magdy و همکاران(۱۶) با یافته‌های پژوهش حاضر همسوست. پژوهش Fernandez-Aleman و همکاران(۲۰۱۵) که با هدف ارزیابی رفتار امنیتی متخصصان مراقبت‌های بهداشتی در یک محیط بالینی واقعی در اسپانیا انجام شد، نشان داد که ۶۲ درصد کاربران سیستم‌های اطلاعاتی گذرواژه ضعیفی انتخاب کرده‌اند. همچنین، گذرواژه ۵۳/۹ درصد کاربران فاقد ترکیبی از حداقل ۸ کاراکتر شامل حروف بزرگ الفبایی، حروف کوچک الفبایی، اعداد و کاراکترهای مخصوص بود(۱۷). پژوهش احمدی و همکاران(۱۳۹۷) که با هدف مطالعه‌ی بررسی مطالعات انجام شده پیرامون پزشکی از راه دور در ایران انجام گرفت، ضعیف بودن روش‌های حفظ حریم خصوصی و محرمانگی را چالشی در برابر اجرای فناوری پزشکی از راه دور دانست(۱۸). پژوهش حسینیان و همکاران(۱۳۹۲) که با هدف تعیین اهمیت الزامات امنیت اطلاعات در شبکه پزشکی از راه دور انجام شد، مهم‌ترین نیاز امنیتی در زمینه‌ی انتقال اطلاعات را پیاده‌سازی پروتکل‌های شبکه‌ای برای اطمینان از ارسال اطلاعات می‌دانست که از این نظر با پژوهش حاضر همسو نیست(۱۲). پژوهشی که Garg و Brewer (۲۰۱۱) با هدف مروری بر امنیت پزشکی از راه دور انجام دادند، یکی از خطرات به‌کارگیری حسگرهای بیومتریک را ایجاد عفونت دانستند و همچنین برخی از حسگرهای بیومتریک، نیازمند مادون قرمز هستند که نگرانی‌های ایمنی را ایجاد می‌کنند(۱۹).

هدف دوم پژوهش، تعیین اهمیت الزامات امنیت اطلاعات در فناوری پزشکی ازراه دور در زمینه‌ی منابع انسانی از دیدگاه مدیران و کارکنان واحد فناوری اطلاعات دانشگاه علوم پزشکی و بیمارستان‌های آموزشی شهر بیرجند بود. در این رابطه پژوهش حاضر نشان داد که مهم‌ترین نیاز امنیتی، ارایه مستندات دقیق و راهنماهای آموزشی برای کاربران سیستم‌های شبکه پزشکی از راه دور بود درحالی‌که تفویض اختیار به کاربران در جهت ارایه خدمات بر اساس قوانین حرفه‌ی خود، کم‌اهمیت‌ترین نیاز امنیتی بود. فرزندی‌پور و همکاران(۱۳۸۶) در پژوهش خود به آموزش رویه‌های ایمنی به تمامی کارکنان و کاربران ثالث اطلاعات سازمان، گنجاندن نقش‌ها و وظایف ایمنی موجود در سیاست ایمنی سازمان در تعاریف شغلی کارکنان ایمنی اطلاعات سازمان و تعیین مسئولیت و وظایف کارکنان در قبال ایمنی اطلاعات در شرایط استخدام تاکید داشتند(۱۴). حسینیان و همکاران(۱۳۹۲) در پژوهش خود ارایه آموزش‌های لازم جهت حفظ صحت و یکپارچگی اطلاعات را به پرسنل و بیماران و همچنین آگاهی دادن به کاربران در خصوص عواقب قانونی ناشی از افشای اسرار بیماران را از جمله مهم‌ترین نیازهای امنیتی در زمینه‌ی امنیت منابع انسانی می‌دانستند(۱۲). پژوهش کاهویی و عباسی(۱۳۹۲) که با هدف اولویت‌بندی عوامل موثر بر امنیت اطلاعات الکترونیکی سلامت انجام گرفت، برگزاری دوره‌های آگاه‌سازی، ترویج و توسعه‌ی برنامه‌های آموزشی دقیق در راستای نیروی انسانی کارآمد و توسعه‌ی روال‌های صحیح را ضروری می‌دانند(۲۰). از نظر احمدی و همکاران(۱۳۹۷) دستورالعمل‌های خاص و قوانین مدون حمایت قوانین و سیاست‌های دولت از برنامه‌های پزشکی از راه دور، منابع انسانی آموزش‌دیده به تعداد کافی، دسترسی به منابع مالی پایدار، ارایه تعاریف شفاف از قوانین، به خصوص مقرارت فرایندهای ارجاع به پزشکی از دور در موفقیت برنامه‌های پزشکی از راه دور ارزشمند می‌باشند(۱۸). نتایج مطالعات فرزندی‌پور و همکاران(۱۴)، حسینیان و همکاران(۱۲)، کاهویی و عباسی(۲۰) و احمدی و همکاران(۱۸) با یافته‌های پژوهش حاضر همسوست. پژوهش میدانی و همکاران(۱۳۹۶) که با هدف ارزیابی امنیت سیستم‌های اطلاعات بیمارستانی از نظر سه حوزه‌ی مدیریتی، فنی و فیزیکی انجام گرفت، علت پایین بودن سطح امنیتی الزامات در ایران را به عدم سازماندهی یک تیم«مسئولیت امنیت اطلاعات» با نقش‌ها و مسئولیت‌های امنیتی مشخص نسبت داد(۲۱). ازاین‌رو مطالعه‌ی میدانی و همکاران(۲۱) با پژوهش حاضر همسوست. Kim و همکاران(۲۰۲۰) در پژوهشی که با هدف تجزیه‌وتحلیل خطرات و تهدیدات امنیتی انجام دادند، تاکید داشتند که پرسنل بدون پیشینه‌ی امنیتی پزشکی از راه دور به شدت مستعد حملات سایبری هستند(۲۲). پژوهش مافی‌مرادی و همکاران(۱۳۹۷) که با هدف تعیین فرصت‌ها و چالش‌های پیش‌روی نظام سلامت کشورهای مختلف در به‌کارگیری فناوری پزشکی از راه دور انجام گرفت، ضعف در تعریف دامنه مسئولیت‌پذیری پزشکان در قبال عملکرد خود، ضعف در تعریف و تعیین راهنماها و دستورالعمل‌ها را از جمله چالش‌های مرتبط با نیروی انسانی در شبکه پزشکی از راه دور برشمرد(۲۳).

هدف سوم پژوهش حاضر، تعیین اهمیت الزامات امنیت اطلاعات در فناوری پزشکی از راه دور در زمینه‌ی تجهیزات تشخیص پزشکی از دیدگاه مدیران و کارکنان واحد فناوری اطلاعات دانشگاه علوم پزشکی و بیمارستان‌های آموزشی شهر بیرجند بود که در این رابطه یافته‌های حاصل این بود که مهم‌ترین

[DOR: 20.1001.1.17358132.1401.16.6.8.5]

نیاز امنیتی مربوط به مجهزبودن سیستم‌های شبکه پزشکی از راه دور به برق اضطراری و کم‌اهمیت‌ترین نیاز امنیتی به تبادل دیجیتالی سیگنال‌های ویدیویی و تصاویر آنالوگ و وجود دستورالعمل‌های مطابق با الزامات سازمانی، حقوقی و نظارتی تعلق داشت. میدانی و همکاران(۱۳۹۶) در پژوهش خود، قطعی یا نقص برق را مهم‌ترین تهدید HIS (سیستم اطلاعات سلامت) دانستند که علت آن نقص برق سرور، نقص سیستم تهویه سرور و نیز نقص و یا قطعی برق در نتیجه‌ی عملکرد نادرست کارکنان فنی واحد برق و کامپیوتر بود(۲۱). کرمی و همکاران(۱۳۹۲) در پژوهش خود از جمله دستورالعمل‌های حفاظتی و نظارتی از تجهیزات را نصب ابزارهای ضدسرقت به شکل استفاده از زنجیرها برای بستن کامپیوترها به میز و نصب هشداردهنده‌ها در ایستگاه‌های کاری می‌دانستند(۱۳). پژوهش jalali و همکاران(۲۰۲۱) که با هدف بررسی امنیت اطلاعات و حریم خصوصی در زمان شیوع ویروس کووید انجام گرفت، تاکید داشت که زمینه‌های نوظهور مانند هوش مصنوعی، اینترنت اشیا و بلاک چین نیز می‌توانند به‌عنوان ابزارهای پیشگیری و شناسایی برای مبارزه‌ی موثرتر با تهدیدات سایبری استفاده شوند؛ در نتیجه مدیران باید مایل به سرمایه‌گذاری کامل در امنیت سایبری در سراسر سازمان باشند(۲۴). حسینیان و همکاران(۱۳۹۲) نیز در پژوهش خود کم‌اهمیت‌ترین الزامات امنیتی در زمینه‌ی تجهیزات پزشکی را تبادل دیجیتالی سیگنال‌های ویدیویی و تصاویر آنالوگ دانستند(۱۲). پژوهش میدانی و همکاران(۱۳۹۶) نشان داد که سیستم‌های قفل و کلید در بیش از ۹۰ درصد موسسات مراقبت سلامت ناکافی است، که این امر علاوه بر به‌کارگیری سخت افزار نامناسب، در نتیجه‌ی ضعف مدیریتی نیز هست(۲۱). در همین زمینه، بیمارستان‌ها باید تدابیری را در خصوص کنترل فیزیکی تسهیلات، ایجاد حصارهای امنیتی برای نواحی حاوی اطلاعات، به‌کارگیری حفاظت فیزیکی برای مقابله با خسارت‌های انسانی و بلایای طبیعی و درگیری‌های احتمالی و همچنین قرار دادن تجهیزات کامپیوتری در مکان مناسب به‌کار گیرند. به‌طورکلی بی‌توجهی به امنیت تجهیزات و ابزارهای ارایه خدمات، به کیفیت پایین مراقبت، عدم‌اعتماد به نفس ارایه‌دهندگان و دریافت‌کنندگان مراقبت سلامت و نیز تخطی از قوانین مرتبط با حفظ محرمانگی و حریم خصوصی اطلاعات بیماران منجر خواهد شد. در نتیجه، مطالعات حسینیان و همکاران(۱۲)، کرمی و همکاران(۱۳)، میدانی و همکاران(۲۱) و jalali و همکاران(۲۴) با یافته‌های پژوهش حاضر هم‌راستا هستند.

هدف چهارم پژوهش، تعیین اهمیت الزامات امنیت اطلاعات در فناوری پزشکی از راه دور در زمینه‌ی ذخیره و دسترسی به اطلاعات از دیدگاه مدیران و کارکنان واحد فناوری اطلاعات دانشگاه علوم پزشکی و بیمارستان‌های آموزشی شهر بیرجند که در این رابطه یافته‌های حاصل نشان داد که مهم‌ترین نیاز امنیتی مربوط به نصب آنتی‌ویروس‌ها و ضدبدافزارها بر روی تمامی سیستم‌ها در شبکه پزشکی از راه دور بود و کم‌اهمیت‌ترین نیاز امنیتی به اجازه‌ی دسترسی بیمار به اطلاعات جهت افشای اطلاعات در صورت ارایه مجوز کتبی تعلق داشت.

کرمی و همکاران(۱۳۹۲) در پژوهش خود بر محافظت با دیواره آتش و چک‌کردن ویروس‌ها تاکید داشتند(۱۳). فرزندی‌پور و همکاران(۱۳۸۸) نیز اخذ مجوز دسترسی کاربران از راه دور و دسترسی مستقیم کاربران فقط به سرویس‌های مجاز را به‌عنوان الزامات کنترل دسترسی برشمردند(۲۵) و از این نظر، نتایج هر دو پژوهش با یافته‌های پژوهش حاضر همسوست. پژوهش مافی‌مرادی و همکاران(۱۳۹۷)، ضعف در حفظ قابلیت دسترسی مداوم به اطلاعات مبادله‌شده بین کاربران و ضعف در تامین ملاحظات محرمانگی داده‌های پزشکی بیماران و رعایت حریم خصوصی کاربران را از جمله چالش‌های پیش‌روی نظام سلامت برشمرد(۲۳).

در پژوهش حسینیان و همکاران(۱۳۹۲) نیز همانند پژوهش حاضر، رعایت امنیت در زمینه‌ی ذخیره‌سازی و دسترسی به اطلاعات از اهمیت بسیاری برخوردار بود(۱۲). از دیدگاه افراد شرکت‌کننده در پژوهش الزامات امنیت اطلاعات در فناوری پزشکی از راه دور در زمینه‌ی انتقال اطلاعات و منابع انسانی از میانگین بالاتر و اهمیت بیشتری برخوردار بودند. سایر الزامات امنیت اطلاعات در شبکه پزشکی از راه دور از نظر اهمیت در سطوح بعدی قرار داشتند. اکثریت افراد شرکت‌کننده در پژوهش بر وجود نرم‌افزارهایی برای ذخیره‌سازی اطلاعات و دستورالعمل‌هایی برای محدودکردن دسترسی به سیستم اطلاعات سلامت بیماران تاکید داشتند. بنابراین می‌توان گفت به‌طورکلی، مقوله ذخیره‌سازی صحیح و دسترسی ایمن به اطلاعات سلامت و وجود کنترل‌های کافی جهت حفاظت از فایل‌ها و اطلاعات مهم و حساس در شبکه پزشکی از راه دور از جمله الزاماتی است که پیش از راه‌اندازی این شبکه باید مورد توجه قرار گیرد.

در این پژوهش تنها به نظرسنجی از مدیران و کارکنان واحد فناوری اطلاعات دانشگاه علوم پزشکی و بیمارستان‌های آموزشی شهر بیرجند بسنده شد. با وجود این، به نظر می‌رسد که نظرسنجی از مدیران واحد فناوری اطلاعات در

[DOR: 20.1001.1.17358132.1401.16.6.8.5]

سایر مراکز درمانی و در بین تعداد بیشتری از افراد امکان تعمیم‌پذیری نتایج را افزایش خواهد داد.

نتیجه‌گیری

به‌کارگیری هر فناوری جدید، مستلزم پیاده‌سازی زیرساخت‌های امنیتی کامل و مورد اعتماد می‌باشد. با توجه به اهمیت الزامات امنیت اطلاعات در شبکه پزشکی از راه دور به نظر می‌رسد که در درجه‌ی اول باید حوزه‌ها و زیرمجموعه‌های مرتبط با امنیت اطلاعات شناسایی گردد تا با بررسی الزامات امنیتی در هر یک از حوزه‌های مطرح شده بتوان راهکارهای موثر و عملی را جهت ارتقای سطح امنیت اطلاعات در فناوری پزشکی از راه دور ارایه نمود. براساس نتایج پژوهش ازآن‌جاکه الزامات مربوط به انتقال اطلاعات از اهمیت بالاتری نسبت به سایر الزامات برخوردار است، به‌کارگیری روش‌های جدید رمزگذاری و تایید صلاحیت و همچنین ارایه آموزش‌های لازم و بسترسازی فنی جهت استفاده از فناوری پزشکی از راه دور، راه را برای به‌کارگیری کارآمد این فناوری هموار خواهد ساخت.

نظر به اهمیت الزامات امنیتی در شبکه پزشکی از راه دور پیشنهاد می‌گردد که مکانیسم رمزگذاری توسط تیم فنی ارزیاب امنیت بررسی گردد و پروتکل‌های ارتباطی و شبکه‌ای جهت اشتراک‌گذاری اطلاعات بین موسسات بهداشتی محلی و ملی و اطمینان از ارسال اطلاعات، پیاده‌سازی گردد و معیارهای کنترل کیفی داده‌ها و استانداردهای بین‌المللی لازم جهت بهبود فرایند مراقبت در فناوری پزشکی از راه دور به‌کارگرفته شود و همچنین برنامه‌های آموزشی در زمینه‌ی مدیریت امنیت اطلاعات و جنبه‌های قانونی فناوری پزشکی از راه دور برگزار گردد.

تشکر و قدردانی

این مقاله حاصل طرح پژوهشی با شناسه اخلاق IR.BUMS.REC.1400.434 مصوب دانشگاه علوم پزشکی بیرجند در سال ۱۴۰۰ می‌باشد. نویسندگان برخود لازم می‌دانند تا از کلیه مدیران وابسته به دانشگاه علوم پزشکی بیرجند که در انجام این پژوهش همکاری نموده‌اند تشکر و قدردانی نمایند.

References

1. Rezaei P, Maserrat E & Torab-Miandoab A. Specialist physicians' perspectives about telemedicine and barriers to using it in Tabriz teaching hospitals. Iranian South Medical Jurnal 2018; 20(6): 562-72[Article in Persian].

2. Zargar M, Alizadeh-Otaghvar HR, Danaei A & Babaei M. Factors affecting of telemedicine technology acceptance among technology specialists in Iranian hospitals. Razi Journal of Medical Sciences 2017; 24(161): 88-98[Article in Persian].

3. Karimi A, Rahimipour I & Hassani M. Telemedicine crimes resulted from electronic health. Medical law Journal 2010; 4(14): 47-69[Article in Persian].

4. Saeedi-Tehrani S & Noroozi M. Telemedicine: Benefits, disadvantages and ethical challenges. Iranian Journal of Medical Ethics and History of Medicine 2015; 8(2): 29-40[Article in Persian].

5. Karimi Z & Peikari HR. Information security management: The impacts of organizational commitment and perceived consequences of security breachon the intention of patients' information security violation. Quarterly Journal of Medical Ethics 2019; 13(44): 1-10[Article in Persian].

6. Rafati H & Molavi-Taleghani Y. Feasibility study for the establishment of telemedicine: A review study and a suggestion for Iran. Journal of Health and Biomedical Informatics 2019; 5(4): 507-19[Article in Persian].

7. Khara R & Saremian M. Comprehensive overview of the health information security risks in mobile devices. Journal of Health and Biomedical Informatics 2015; 2(1): 48-56[Article in Persian].

8. Hajrahimi N, Hejazi-Dehaghani SM & Sheikhtaheri A. Health information security: A case study of three selected medical centers in Iran. Acta Informatica Medica 2013; 21(1): 42-5.

9. Mehraeen E, Ayatollahi H & Ahmadi M. A study of information security in hospital information systems. Journal of Health Information Management 2014; 10(6): 779-88[Article in Persian].

10. Samy GN, Ahmad SR & Ismail Z. Threats to health information security. China: Fifth International Conference on Information Assurance and Security. Computer Science, Medicine, Political Science, 2009.

[DOR: 20.1001.1.17358132.1401.16.6.8.5]

11. Mirabootalebi N, Ahmadi M, Dehghani M, Khani Sh & Azad M. Electronic medical records, a new step in technology of health system: Administrators and physiciansperspective. Journal of Payavard Salamat 2017; 10(5): 409-18[Article in Persian].

12. Hosseinian V, Ayatollahi H, Haghani H & Mehraeen E. Requirements of information security in a telemedicine network: Review of IT managers' opinion. Journal of Paramedical Sciences and Rehabilitation 2015; 4(2): 31-40[Article in Persian].

13. Karami M, Safdari R & Soltani A. Patient's information rights: Strategies for information security in the electronic environment. Quarterly Journal of Medical Ethics 2013; 7(25): 83-96[Article in Persian].

14. Farzandipour M, Sadoughi F, Ahmadi M & Karimi I. Safety requirements for health electronic file; Comparison between selected countries. Journal of Health Information Management 2007; 4(1): 1-9[Article in Persian].

15. Zain JM & Clarke M. Security in telemedicine: Issues in watermarking medical images, Tunisia: 3rd International Conference: Sciences of Electronic,Technologies of Information and Telecommunications, 2005.

16. Magdy M, Hosny KM, Ghali NI & Ghoniemy S. Security of medical images for telemedicine: A systematic review. Multimedia Tools and Applications Journal 2022; 81(18): 25101-45.

17. Fernandez-Aleman JL, Sanchez-Henarejos A, Toval A, Sanchez-Garcia AB, Hernandez-Hernandez 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.

18. Ahmadi M, Meraji M & Mashoof-Jafarabad E. Evidence on telemedicine in Iran-systematic review. Journal of Paramedical Sciences and Rehabilitation 2018; 7(1): 112-24[Article in Persian].

19. Garg V & Brewer J. Telemedicine security: A systematic review. Journal of Diabetes Science and Technology 2011; 5(3): 768-77.

20. Kahouei M & Abbasi Z. The prioritization of effective factors on electronic health information security in medical centers. Journal of Health Information Management 2015; 12(2): 162-70[Article in Persian].

21. Meidani Z, Assari MA, Moosavi SGh & Ataei-Andezag A. Evaluation of hospital information systems security. Journal of Health Information Management 2018; 14(5): 187-93[Article in Persian].

22. Kim DW, Choi JY & Han KH. Risk management-based security evaluation model for telemedicine systems. BMC Medical Informatics and Decision Making 2020; 20(106): 1-14.

23. Mafi-Moradi S, Doshmangir L & Kabiri N. Challenges and opportunities of telemedicine: A narrative review study. Journal of Health Information Management 2019; 15(6): 294-9[Article in Persian].

24. Jalali MS, Landman A & Gordon WJ. Telemedicine, privacy, and information security in the age of COVID-19. Journal of the American Medical Informatics Association 2021; 28(3): 671-2.

25. Farzandipour M, Ahmady M, Sadoughi F & Karimi I. Designing a model for security requirements of electronic health records in Iran. Journal of Inflammatory Diseases 2009; 13(1): 79-86[Article in Persian].

[DOR: 20.1001.1.17358132.1401.16.6.8.5]

Journal of Payavard Salamat
Vol. 16, No.6, Feb 2023

Determining Information Security Requirements in the Telemedicine Network from the Point of View of Managers and Employees of the Information Technology Unit of Birjand University of Medical Sciences and Teaching Hospitals

Fatemeh Bahador[1] (Ph.D.), Azam Sabahi[2] (Ph.D.), Somayeh Paydar[3] (Ph.D.), Fatemeh Zangooei Seno[4*] (B.S.)

1 Ph.D. Candidate in Health Information Management, School of Allied Medical Sciences, Tehran University of Medical Sciences, Tehran, Iran
2 Assistant Professor, Department of Health Information Technology, Ferdows School of Health and Allied Medical Sciences, Birjand University of Medical Sciences, Birjand, Iran
3 Assistant Professor, Department of Health Information Technology, School of Allied Medical Sciences, Kermanshah University of Medical Sciences, Kermanshah, Iran
4 Bachelor of Science in Health Information Technology, Ferdows School of Health and Allied Medical Sciences, Birjand University of Medical Sciences, Birjand, Iran

Abstract

Received: 14 Aug. 2022
Accepted: 31 Dec. 2022

Background and Aim: Today along with information technology development, telemedicine technology has expanded dramatically. Sinse telemedicine technology relies on data transmission, it is essential to pay attention to issues such as network security, confidentiality, and privacy of patients. Therefore, the aim of this study was to determine the importance of information security requirements in telemedicine networks based on managers and employees of the information technology unit of the University and teaching hospitals of Birjand city

Materials and Methods: This descriptive cross-sectional study was conducted in year 2021. The research population was The managers and employees of the information technology unit of the university and teaching hospitals of Birjand city (40 people), who were surveyed by the census. The study tool was a researcher-made questionnaire that confirmed its validity by faculty members and experts, and its reliability was calculated with Cronbach's alpha (0.83). After collecting the data, they were entered into the SPSS software and were analyzed using descriptive statistics.

Results: The results showed that the security requirement related to information transportation is more important than other requirements. Also in the field of human resources, providing detailed documentation and training guides for users of the systems was with an average of (4.47). In the medical diagnosis equipment field, telemedicine network systems are equipped with emergency power was with an average of (4.72). In the storage and access to information context, installing antiviruses and anti-malware on all systems was with an average of (4.75), and also in the field of information transfer, encryption of important and sensitive files and information was with an average of (4.69) were the most important security needs.

Conclusions: As the results showed, security requirements related to information transfer have more importance than other requirements; Initially, information security can be guaranteed by creating security policies, updating and monitoring their implementation, as well as training employees. However, in order to transfer sensitive medical information, encryption and qualification verification methods, secure information transfer protocols, virtual and private networks (VPN) and other new technologies can be used in this field. Of course, necessary preparations should be made to create appropriate technical infrastructure for the implementation of security policies in information transmission.

Keywords: Telemedicine, Information Security, Information Technology, Telemedicine Security, Medical Information Security, Telecare Security

*** Corresponding Author:**
Zangooei Seno F
Email:
zangoei.f@bums.ac.ir

[DOR: 20.1001.1.17358132.1401.16.6.8.5]