Requirements of Information Security in a Telemedicine Network: Review of IT Managers' Opinion

Hosseinian V[1], Ayatollahi H[2], Haghani H[3], Mehraeen E[4]

Abstract

Purpose: The requirements of information security in a telemedicine network can be categorized in four areas, namely; data storage and data accessibility, data transfer, human resources, and equipment for medical diagnosis. The purpose of this study was to determine the importance of each of the above areas from the perspective of information technology (IT) managers in teaching hospitals affiliated to Tehran and Shahid Beheshti Universities of Medical Sciences, and the experts in the field who worked in the Ministry of Health.

Methods: This was a survey study conducted in 2013. The participants of the study included 41 information technology (IT) managers in teaching hospitals and seven experts who worked in the Ministry of Health. Data were collected using a five-point Likert scale questionnaire and were analyzed using descriptive statistics. The content and face validity of the questionnaire were confirmed by the experts in the field. The reliability of the questionnaire was calculated using Cronbach's coefficient alpha (α= 0/75).

Results: The results of the present study showed that among the requirements of information security in a telemedicine network, human resources were of high importance (mean = 87.50). The requirements related to the medical diagnostic equipment and those related to data storage and data accessibility were in the second (mean=87.04) and the third place (mean=85.97) of importance respectively. The requirements of information security in the area of data transfer were in the fourth place of importance.

Conclusion: Considering the degree of importance that human resources gained compared to the importance of other requirements of information security in a telemedicine network, it seems that employing experts in the field of information security and training health care professionals in the application of telemedicine technology, may facilitate efficient deployment of this technology in the healthcare settings.

Keywords: Information security, Telemedicine, Information technology

دریافت مقاله: ۹۳/۱۱/۲۰ تایید مقاله: ۹۴/۰۲/۱۵

الزامات امنیت اطلاعات در شبکه پزشکی از راه دور از دیدگاه مدیران فن‌آوری اطلاعات

ولی اله حسینیان[۱]، هاله آیت اللهی[۲]، حمید حقانی[۳]، اسماعیل مهرآیین[۴]

هدف: الزامات امنیت اطلاعات در شبکه پزشکی از راه دور را می‌توان از جنبه‌های ذخیره‌سازی و دسترسی به اطلاعات، انتقال اطلاعات، منابع انسانی و تجهیزات تشخیص پزشکی مورد بررسی قرار داد. هدف از این مطالعه تعیین درجه اهمیت هر یک از جنبه‌های ذکر شده در به کارگیری فن‌آوری پزشکی از راه دور از دیدگاه کارشناسان واحد فن آوری اطلاعات وزارت بهداشت و مراکز آموزشی درمانی وابسته به دانشگاه های علوم پزشکی تهران و شهید بهشتی بود.

روش بررسی: این پژوهش به روش توصیفی در سال ۱۳۹۲ انجام شد. مدیران واحد فن‌آوری اطلاعات مراکز آموزشی درمانی وابسته به دانشگاه‌های علوم پزشکی تهران و شهید بهشتی (۴۱ نفر) و کارشناسان حوزه انفورماتیک پزشکی وزارت بهداشت (۷ نفر) در این مطالعه شرکت داشتند. داده‌ها با استفاده از پرسشنامه پنج گزینه‌ای Likert گردآوری و با استفاده از آمار توصیفی تحلیل گردیدند. روایی محتوا و ساختار ابزار توسط اساتید و صاحب نظران تایید شد. پایایی پرسشنامه مورد نظر نیز با استفاده از آزمون همبستگی درونی تعیین گردید (α=۰/۷۵).

یافته‌ها: یافته‌های پژوهش حاضر نشان داد از جمله مهمترین الزامات امنیتی در زمینه انتقال اطلاعات پیاده سازی پروتکل‌های شبکه‌ای برای اطمینان از ارسال اطلاعات و بررسی یکپارچگی آنها می‌باشد. اکثریت افراد شرکت‌کننده در پژوهش بر وجود نرم‌افزارهایی برای ذخیره‌سازی اطلاعات و دستورالعمل‌هایی برای محدود کردن دسترسی به سیستم اطلاعات سلامت بیماران تاکید داشتند.

نتیجه‌گیری: با توجه به درجه اهمیت منابع انسانی در میان سایر الزامات امنیت اطلاعات در شبکه پزشکی از راه دور، به نظر می‌رسد به کارگیری افراد متخصص در زمینه امنیت اطلاعات و آموزش استفاده از فن‌آوری پزشکی از راه دور به متخصصان حوزه سلامت، به کارگیری کارآمد این فن آوری را در مراکز مراقبت سلامت تسهیل خواهد ساخت.

کلمات کلیدی: پزشکی از راه دور، فناوری اطلاعات، امنیت اطلاعات

نویسنده مسئول: هاله آیت اللهی، ayatollahi.h@iums.ac.ir

آدرس: تهران، دانشگاه علوم پزشکی تهران، دانشکده پیراپزشکی

۱- کارشناس ارشد آموزش مدارک پزشکی،دانشکده مدیریت و اطلاع رسانی پزشکی،دانشگاه علوم پزشکی ایران، تهران، ایران

۲- استادیار انفورماتیک پزشکی، دانشکده مدیریت و اطلاع‌رسانی پزشکی، دانشگاه علوم پزشکی ایران، تهران، ایران

۳- مربی گروه ریاضی و آمار، دانشکده بهداشت، دانشگاه علوم پزشکی ایران، تهران، ایران

۴- دانشجوی دکترای مدیریت اطلاعات سلامت، دانشکده پیراپزشکی، دانشگاه علوم پزشکی تهران، تهران، ایران

مقدمه

امروزه، سازمانهای مراقبت بهداشتی تلاش می‌کنند تا برای رقابت با سازمان های دیگر و کسب نمره قابل قبول در ممیزی‌ها، رضایت بیماران را کسب کنند. در سالهای اخیر این سازمانها برای ارائه خدمات به مشتریان خود استفاده از پیشرفته‌ترین دستاوردهای علوم مختلف را آغاز کرده‌اند (۱). هدف سازمانهای مراقبت بهداشتی از بکارگیری این دستاوردها و کاربرد سیستمهای مراقبت سلامت بهبود روندکاری، کاهش هزینه‌ها و در نهایت ارتقاء کیفیت خدمات مراقبتی می‌باشد (۲). از طرفی، دسترسی برابر بیماران به مراقبت‌های بهداشتی و ضرورت حضور فیزیکی ارائه دهنده مراقبت و دریافت کننده آن در یک محل، از جمله چالش‌هایی بوده که مدیران مؤسسات مراقبت سلامت با آن روبرو بوده‌اند. امروزه، با پیشرفت-های اخیر در فن‌آوری اطلاعات و ارتباطات و به منظور ارتقاء کیفیت و سرعت ارائه خدمات به بیماران، فن‌آوری پزشکی از راه دور به عنوان راهکاری جدید برای حل این مشکل مطرح گردیده است (۳).

پزشکی از راه دور یک اصطلاح کلی در حوزه فناوری اطلاعات سلامت است که روش‌های مختلف تبادل اطلاعات پزشکی را برای حفظ و یا بهبود وضعیت سلامت بیماران در بر می‌گیرد. از جمله این روش‌ها، می‌توان به تبادل الکترونیکی تصاویر رادیولوژی (Teleradiology)، پایش از راه دور (Remote monitoring)، یادآوری-های پزشکی (Medical reminders) از طریق ارسال پیام الکترونیکی بین پزشکان و بیماران و مشاهده، تشخیص و پیشنهاد درمان از طریق کنفرانس‌های ویدئویی (Videoconference) اشاره کرد (۴). اگر چه استفاده از این فناوری‌ها ممکن است صرفه‌جویی در هزینه و زمان، ثبت و انتقال سریع داده‌های بیماران و تسهیل دسترسی به اطلاعات را بدون در نظر گرفتن منطقه جغرافیایی در پی داشته باشد، اما حفظ امنیت اطلاعات بیماران و کنترل دسترسی‌های غیر مجاز به اطلاعات همواره از جمله مسائل مهم در به کارگیری این فن‌آوری بوده است(۵).

Wozak و همکاران (۶) در سال ۲۰۰۷ در مقاله‌ای بیان کردند که سازمانهای مراقبت سلامت و مؤسساتی که در زمینه ارائه خدمات پزشکی از راه دور فعالیت دارند، باید برای ارتقاء امنیت تبادل اطلاعات از استانداردهای موجود در این زمینه بهره برده و نیازهای امنیتی این حیطه را شناسایی نمایند. برای مثال، این مؤسسات می‌توانند از دستورالعمل‌های جهانی زیرساخت امنیتی (Security infrastructure) برای تبادل اطلاعات در پزشکی از راه دور استفاده کنند. براساس این زیر ساخت، حوزه‌های امنیتی که در پزشکی از راه دور باید مدنظر قرار گیرند عبارتند از شبکه پزشکی از راه دور

(Telemedicine network)، سیستم‌های تایید هویت و کنترل دسترسی (Authentication and access control systems) و امنیت انتقال اطلاعات (Transport security).

در واقع، از آنجا که فن‌آوری پزشکی از راه دور متکی بر انتقال داده‌ها است، حفظ امنیت شبکه به منظور محرمانه نگاه داشتن انتقال داده‌ها و حفظ حریم خصوصی (Privacy) بیماران امری حیاتی است (۷) و هر گونه احتمال تهدید یا حمله به شبکه های پزشکی از راه دور از قبیل ورود افراد غیرمجاز به شبکه و تغییر یا تخریب داده-های بیماران باید مورد بررسی قرار گیرد. به عبارت دیگر هرگونه ضعف در هر بخشی از شبکه‌ی پزشکی از راه دور می‌تواند کل سیستم را تحت تاثیر قرار دهد. بنابراین، برای ایجاد امنیت در زمینه ذخیره و تبادل اطلاعات در شبکه پزشکی از راه دور باید ساز و کارهای لازم با استفاده از استانداردهای مرتبط مد نظر قرار گیرد (۸).

در همین رابطه، نتایج مطالعه‌ای که در آفریقای جنوبی انجام شد، نشان داد که درک سنتی از رابطه پزشک و بیمار، استفاده از فن‌آوری پزشکی از راه دور را به چالش می‌کشد. رابطه از راه دور پزشک با بیمار خود این نگرانی را در پی دارد که اطلاعاتی که وی از طریق سیستمهای پزشکی از راه دور در اختیار کادر بالینی قرار می‌دهد تا چه حد محرمانه و ایمن خواهد بود. این نگرانی در بسیاری از کشورهای در حال توسعه که در حال استفاده و یا پیاده‌سازی فن آوری پزشکی از راه دور هستند، مدیران و سیاستگذاران را ملزم کرده که به فکر راه‌حل های مؤثرتر باشند (۹).

در مطالعه‌ی دیگری مشخص شد که با وجود فواید بالقوه، استفاده از این فن‌آوری همواره موانع و نگرانی‌هایی نیز به همراه داشته است. مسئله‌ای که در سالهای اخیر چشمگیر بوده نگرانی در مورد امنیت و حریم خصوصی اطلاعات بیماران بوده است. هر چند قانون قابلیت انتقال و پاسخگویی بیمه سلامت جنبه‌های حفظ حریم خصوصی و امنیت اطلاعات بیماران را پوشش می‌دهد، اما این قانون به تنهایی پاسخگوی نیازهای امنیتی در حوزه پزشکی از راه دور نمی‌باشد. بنابراین در کشورهای توسعه یافته، برای پیش‌بینی خطرات امنیتی و رفع این خطرات، بیمارستان-ها و مراکز ارائه‌دهنده خدمات پزشکی از راه دور کوچکترین خطرات رخ داده را به وزارت بهداشت اعلام می‌کنند تا مورد ارزیابی قرار گیرد (۱۰).

در ایالات متحده آمریکا نیز امنیت فن‌آوری پزشکی از راه دور موضوعی است که توجه بیشتر متخصصان را به خود جلب کرده تا توصیه‌هایی برای سیاستگذاری مؤثر در این زمینه ارائه دهند. یکی از این سیاست‌ها پیاده‌سازی استانداردهای امنیتی به منظور اطمینان از ارائه ایمن و محرمانه خدمات پزشکی از راه دور می‌باشد (۱). به طور مشابه، در سال ۱۳۸۱ اسدی و اخلاقی در مطالعه‌ای مروری با عنوان "جنبه‌های اخلاقی و قانونی پزشکی از راه دور" بیان کردند که یکی از مشکلات اخلاقی و قانونی مطرح در حوزه فناوری پزشکی از راه دور، بحث امنیت شبکه پزشکی از راه دور می‌باشد (۱۲).

در ایران، با توجه به ضرورت استفاده از انواع فن‌آوری-ها از جمله فن‌آوری پزشکی از راه دور، بررسی پیش نیازها و الزومات این فن‌آوری خصوصاً در حوزه امنیت اطلاعات بیش از پیش احساس می شود. با توجه به اهمیت امنیت اطلاعات سلامت در بیمارستان‌ها و موسسات مراقبت بهداشتی و پیدایش فن‌آوری پزشکی از راه دور در کشورمان، ضرورت بررسی مسائل مربوط به امنیت اطلاعات در این حوزه، بیش از پیش احساس می‌شود. لذا، در این پژوهش درجه اهمیت الزامات امنیت اطلاعات در فن‌آوری پزشکی از راه دور مورد بررسی قرار گرفته است.

روش بررسی

پژوهش حاضر از نوع مطالعات مقطعی بود که به روش کمی در سال ۱۳۹۲ انجام شد. جامعه پژوهش را مدیران واحد فن‌آوری اطلاعات مراکز آموزشی درمانی وابسته به دانشگاه‌های علوم پزشکی تهران و شهید بهشتی در شهر تهران (۴۱ نفر) و دست‌اندرکاران حوزه انفورماتیک پزشکی و پزشکی از راه دور در وزارت بهداشت، درمان و آموزش پزشکی (۷ نفر) تشکیل می‌دادند که با توجه به محدود بودن نمونه‌ها از روش سرشماری استفاده و همه افراد مورد بررسی قرار گرفتند. نظر به محدود بودن تعداد افراد جامعه پژوهش، نمونه‌گیری انجام نشد و از کلیه افراد (۴۸ نفر) برای شرکت در پژوهش دعوت به عمل آمد.

ابزار گردآوری داده‌ها پرسشنامه‌ای بود که براساس معیارهای انجمن سیستم‌های مدیریت و اطلاعات مراقبت سلامت (Healthcare Information and Management Systems Society-HMISS) در

زمینه امنیت شبکه پزشکی از راه دور (۱۳)، استانداردهای امنیتی انجمن پزشکی از راه دور آمریکا (۱۱)، استانداردهای قانون قابلیت انتقال و پاسخگویی بیمه سلامت در زمینه امنیت شبکه پزشکی از راه دور (۱۴) و مطالعه سایر مقالات مرتبط طراحی شد (۱۶، ۱۵، ۵). محتوا و ساختار ابزار توسط پنج نفر از اساتید و صاحب نظران حوزه انفورماتیک سلامت بررسی و تایید شد. پایایی پرسشنامه مورد نظر نیز با استفاده از آزمون همبستگی درونی (آلفای کرونباخ) تعیین گردید (α=۰/۷۵). این پرسشنامه شامل پنج قسمت بود. قسمت اول سوالات مربوط به مشخصات فردی افراد شرکت‌کننده در پژوهش (۶ سوال) و قسمت‌های دوم تا پنجم سوالات مربوط به تعیین درجه اهمیت پیش نیازهای امنیت اطلاعات در فن آوری پزشکی از راه دور در زمینه ذخیره‌سازی و دسترسی به اطلاعات (۲۵ سوال)، انتقال اطلاعات (۷ سوال)، منابع انسانی (۸ سوال)، و تجهیزات تشخیص پزشکی و شبکه کامپیوتری (۱۳ سوال) را در بر می‌گرفت. این پرسشنامه براساس مقیاس پنج گزینه ای Likert طراحی شد و امتیاز هر یک از گزینه‌ها به شرح زیر بود: بسیار مهم (۵)، مهم (۴)، نظری ندارم (۳)، کم اهمیت (۲) و بی اهمیت (۱).

به منظور تحلیل داده‌ها از نرم افزار SPSS نسخه ۱۸ استفاده شد و نتایج با استفاده از آمار توصیفی (میانگین و انحراف معیار) در قالب جدول و نمودار گزارش گردیدند. برای محاسبه درجه اهمیت هر یک از الزامات امنیتی در کل و براساس امتیاز بندی، ابتدا مجموع امتیازات برای هر پرسشنامه به طور جداگانه و بر مبنای امتیاز ۱ تا ۵ محاسبه گردید. سپس با در نظر گرفتن حداقل امتیاز صفر و حداکثر امتیاز ۱۰۰، پنج سطح بسیار مهم (۱۰۰-۸۱)، مهم (۸۰-۶۱)، نظری ندارم (۶۰-۴۱)، کم اهمیت (۴۰-۲۱) و بی‌اهمیت (۲۰-۰) برای تعیین درجه اهمیت الزامات امنیتی از دیدگاه افراد شرکت‌کننده در پژوهش در نظر گرفته شد. در مرحله بعد مشخص گردید چند درصد از افراد شرکت‌کننده چه سطحی از اهمیت را برای هریک از الزامات در نظر گرفته‌اند و در نهایت، با توجه به میانگین امتیاز به دست آمده الزامات امنیتی شبکه پزشکی از راه دور رتبه بندی شدند.

یافته ها

جامعه پژوهش متشکل از ۴۸ نفر از صاحب نظران بود که از این تعداد ۴۶ نفر پرسشنامه را تکمیل نموده و عودت دادند. میانگین سنی افراد شرکت‌کننده در پژوهش ۳۱/۲۸ سال (۳۱/۲۸+۱۸/۰۱) و میانگین سابقه کاری آنها ۷/۱۳ سال بود (۱۱/۵+۷/۲۳). مدرک تحصیلی ۶۷/۴ درصد از پاسخ‌دهندگان کارشناسی و ۸۹/۱ درصد آنها فارغ التحصیل رشته کامپیوتر بودند.

یافته‌های پژوهش در مورد الزامات امنیتی شبکه پزشکی از راه دور در زمینه ذخیره‌سازی و دسترسی به اطلاعات بیانگرآن بود که در بین موارد مطرح شده بیشترین میانگین (۱/۰۲±۴/۸۰) مربوط به "وجود دستورالعمل‌هایی برای محدود کردن دسترسی به سیستم اطلاعات سلامت بیماران" و کمترین میانگین ۱/۰۵±۳/۹۷مربوط به "استفاده از برنامه یا سیستمی در شبکه پزشکی از راه دور برای حذف حساب های غیر فعال برای مدت زمان مشخص" بودند. بر اساس یافته‌های پژوهش که در جدول۱ آمده است، نتایج پژوهش در مورد نیازهای امنیتی شبکه پزشکی از راه دور در زمینه انتقال اطلاعات بیانگر آن بود که در بین نیازهای مربوط به انتقال اطلاعات بیشترین میانگین ۰/۵۷±۴/۶۰ را " پیاده‌سازی پروتکل‌های شبکه‌ای برای اطمینان از ارسال اطلاعات" کسب کرده و اهمیت آن در سطح بسیار مهم ارزیابی شد. این در حالی است که "استفاده از حروف بزرگ و کوچک برای رمزگذاری جهت دسترسی به سیستم‌های شبکه پزشکی از راه دور" کمترین میانگین ۱/۰۱±۴/۱۵ را به خود اختصاص داد.

در خصوص الزامات امنیتی در شبکه پزشکی از راه دور در زمینه منابع انسانی یافته‌های پژوهش نشان داد که در بین نیازهای مربوط به منابع انسانی بیشترین میانگین ۰/۶۵±۴/۶۵ به "آگاهی دادن به کاربران در خصوص عواقب قانونی ناشی از افشای اسرار بیماران" تعلق داشت و اهمیت آن در سطح بسیار مهم ارزیابی شد. در حالی که "ارائه مستندات دقیق و راهنماهای آموزشی برای استفاده از سیستمهای شبکه پزشکی از راه دور" کمترین میانگین ۰/۸۸±۴/۲۶ را به خود اختصاص داده بود (جدول۲). در مورد الزامات امنیتی شبکه پزشکی از راه دور در زمینه تجهیزات تشخیص پزشکی نیز یافته ها بیانگر آن بود که اهمیت "استفاده از اتاق سرور استاندارد و مجهز به

جدول۱: درجه اهمیت نیازهای امنیت اطلاعات در فن‌آوری پزشکی از راه دور در زمینه انتقال اطلاعات

انتقال اطلاعات	بسیار مهم تعداد (٪)	مهم تعداد (٪)	نظری ندارم تعداد (٪)	کم اهمیت تعداد (٪)	میانگین ± انحراف معیار
پیاده‌سازی پروتکل‌های شبکه ای برای اطمینان از ارسال اطلاعات و بررسی یکپارچگی آنها	۳۰(۶۵/۲)	۱۴(۳۰/۴)	۲(۴/۳)	۰(۰)	۴/۶۰ ± ۰/۵۷
ایجاد پروتکل ارتباطی برای به اشتراک گذاشتن اطلاعات بین نهادهای بهداشتی محلی	۲۳(۵۰)	۱۷(۳۷)	۶(۱۳)	۰(۰)	۴/۳۶ ± ۰/۷۱
رمزگذاری فایل ها و اطلاعات مهم و حساس	۲۸(۶۲/۲)	۱۶(۳۵/۶)	۰(۰)	۱(۲/۲)	۴/۵۴ ± ۰/۶۵
بررسی مکانیسم رمزگذاری توسط تیم فنی ارزیاب امنیت	۲۶(۵۶/۵)	۱۳(۲۸/۳)	۷(۱۵/۲)	۰(۰)	۴/۴۱ ± ۰/۷۴
استفاده از ترکیب اعداد و حروف برای رمزگذاری	۳۰(۶۸/۲)	۱۱(۲۵)	۳(۶/۸)	۰(۰)	۴/۵ ± ۰/۸۰
استفاده از حروف بزرگ و کوچک برای رمزگذاری جهت دسترسی به سیستمهای شبکه پزشکی از راه دور	۲۳(۵۰)	۱۱(۲۳/۹)	۸(۱۷/۴)	۴(۸/۷)	۴/۱۵ ± ۱/۰۱
روش‌هایی برای کنترل یکپارچگی اطلاعات برنامه‌های کاربردی	۲۴(۵۳/۳)	۱۶(۳۵/۶)	۴(۸/۹)	۱(۲/۲)	۴/۴ ± ۰/۷۵

*نظر به اینکه مقادیر ذکر شده در سطح بی اهمیت صفر بود، این سطح در جدول گزارش نشد.

جدول۲: درجه اهمیت نیازهای امنیت اطلاعات در فن‌آوری پزشکی از راه دور در زمینه منابع انسانی

منابع انسانی	بسیار مهم تعداد (٪)	مهم تعداد (٪)	نظری ندارم تعداد (٪)	کم اهمیت تعداد (٪)	میانگین ± انحراف معیار
تفویض اختیار به کاربران در جهت ارائه خدمات بر اساس قوانین حرفه خود	۲۳(۵۰)	۲۰(۴۳/۵)	۳(۶/۵)	۰(۰)	۴/۴۳ ± ۰/۶۲
پیاده‌سازی روش‌هایی برای اطمینان از دسترسی مناسب تمام کاربران به اطلاعات	۲۲(۴۸/۹)	۲۱(۴۶/۷)	۲(۴/۴)	۰(۰)	۴/۳۹ ± ۰/۶۸
پیاده‌سازی سیاست‌ها و روش‌های مناسب برای دسترسی به اطلاعات الکترونیکی سلامت در موارد اورژانسی	۲۸(۶۰/۹)	۱۸(۳۹/۱)	۰(۰)	۰(۰)	۴/۶۱ ± ۰/۴۹
حضور افراد متخصص برای پشتیبانی از فن‌آوری مورد استفاده در روش های پزشکی از راه دور	۳۱(۶۶)	۱۲(۲۶/۱)	۲(۴/۳)	۱(۲/۲)	۴/۶۳ ± ۰/۵۷
آگاهی دادن به کاربران در خصوص قوانین و استانداردهای محرمانگی و حریم خصوصی بیماران	۳۱(۶۷/۴)	۱۴(۳۰/۴)	۱(۲/۲)	۰(۰)	۴/۶۵ ± ۰/۵۳
آگاهی دادن به کاربران در خصوص عواقب قانونی ناشی از افشای اسرار بیماران	۳۲(۷۱/۱)	۱۱(۲۴/۴)	۱(۲/۲)	۱(۲/۲)	۴/۶۵ ± ۰/۶۵
ارائه مستندات دقیق و راهنماهای آموزشی برای سیستمهای شبکه پزشکی از راه دور	۲۲(۴۸/۹)	۱۶(۳۵/۶)	۴(۸/۹)	۳(۶/۷)	۴/۲۶ ± ۰/۸۸
همکاری با افراد مسئول جهت کنترل و بررسی موارد امنیتی در شبکه پزشکی از راه دور	۲۶(۵۶/۵)	۱۶(۳۴/۸)	۴(۸/۷)	۰(۰)	۴/۴۸ ± ۰/۶۶

*نظر به اینکه مقادیر ذکر شده در سطح بی اهمیت صفر بود، این سطح در جدول گزارش نشد.

جدول۳: درجه اهمیت نیازهای امنیت اطلاعات در فن‌آوری پزشکی از راه دور در زمینه تجهیزات تشخیص پزشکی از دیدگاه افراد شرکت-کننده در پژوهش

تجهیزات تشخیص پزشکی	بسیار مهم تعداد (٪)	مهم تعداد (٪)	نظری ندارم تعداد (٪)	کم اهمیت تعداد (٪)	میانگین ± انحراف معیار
تبادل دیجیتالی سیگنال های ویدئویی و تصاویر آنالوگ	۲۰(۴۳/۵)	۱۶(۳۴/۸)	۸(۱۷/۴)	۲(۴/۳)	۴/۱۷±۰/۸۸
وجود تجهیزات مخصوص برای ارتباط از راه دور با سیستم‌های اطلاعاتی	۲۸(۶۰/۹)	۱۴(۳۰/۴)	۲(۴/۳)	۲(۴/۳)	۴/۴۸±۰/۷۸
پهنای باند و رابط های کاربری برای تجهیزات شبکه و تجهیزات تشخیصی پزشکی	۲۶(۵۷/۸)	۱۵(۳۳/۳)	۳(۶/۷)	۱(۲/۲)	۴/۴۷±۰/۷۳
وجود رسانه های ذخیره سازی الکترونیکی	۲۱(۴۸/۸)	۱۶(۳۷/۲)	۵(۱۱/۶)	۱(۲/۳)	۴/۱۷±۰/۹۵
اطمینان از به روز رسانی مداوم تجهیزات شبکه	۲۳(۵۱/۱)	۱۷(۳۷/۸)	۴(۸/۹)	۱(۲/۲)	۴/۳۸±۰/۷۵
به کارگیری استانداردها برای پیکر بندی تجهیزات پزشکی از راه دور	۳۰(۶۶/۷)	۱۰(۲۲/۲)	۴(۸/۹)	۱(۲/۲)	۴/۵۳±۰/۷۶
مجهز بودن سیستم های شبکه پزشکی از راه دور به برق اضطراری	۳۴(۷۵/۶)	۹(۲۰)	۲(۴/۴)	۰(۰)	۴/۷۱±۰/۵۵
استفاده از اتاق سرور استاندارد و مجهز به سیستم های هشدار (از قبیل سیستم هشدار حریق)	۴۱(۸۹/۱)	۵(۱۰/۹)	۰(۰)	۰(۰)	۴/۸۹±۰/۳۱
وجود فرآیندهایی برای اطمینان از ایمنی تجهیزات پزشکی از راه دور	۲۶(۵۶/۵)	۱۶(۳۴/۸)	۳(۶/۵)	۱(۲/۲)	۴/۴۶±۰/۷۲
اطمینان از در دسترس بودن تجهیزات پزشکی از راه دور برای پشتیبانی از نیازهای تشخیصی	۲۶(۵۶/۵)	۱۸(۳۹/۱)	۲(۴/۳)	۰(۰)	۴/۵۲±۰/۵۹
اطمینان از عملکرد صحیح تجهیزات پزشکی از راه دور در زمان ارائه مراقبت بالینی	۳۳(۷/۷۱)	۱۱(۲۳/۹)	۱(۲/۲)	۱(۲/۲)	۴/۶۵±۰/۶۴
وجود دستورالعمل های مطابق با الزامات سازمانی، حقوقی و نظارتی	۳۰(۶۵/۲)	۱۵(۳۲/۶)	۰(۰)	۱(۲/۲)	۴/۶۱±۰/۶۱
وجود دستورالعمل هایی برای اطمینان از امنیت فیزیکی تجهیزات پزشکی از راه دور	۳۱(۶۷/۴)	۱۳(۲۸/۳)	۱(۲/۲)	۱(۲/۲)	۴/۶۰±۰/۶۵

*نظر به اینکه مقادیر ذکر شده در سطح بی اهمیت صفر بود، این سطح در جدول گزارش نشد.

جدول ۴: درجه اهمیت الزامات امنیت اطلاعات در فن‌آوری پزشکی از راه دور

الزامات امنیت اطلاعات	بسیار مهم	مهم	نظری ندارم	میانگین ±انحراف معیار
نیازهای مربوط به ذخیره سازی و دسترسی به اطلاعات	۷۳/۹۱	۲۳/۹۱	۲/۱۷	۸۵/۹۷±۱۱/۳۲
نیازهای مربوط به انتقال اطلاعات	۷۳/۹۱	۱۹/۵۷	۶/۵۲	۸۵/۳۳±۱۳/۹۷
نیازهای مربوط به منابع انسانی	۸۰/۴۳	۱۷/۳۹	۲/۱۷	۸۷/۵۰±۱۰/۵۲
نیازهای مربوط به تجهیزات تشخیص پزشکی	۷۸/۲۶	۱۷/۳۹	۴/۳۵	۸۷/۰۴±۱۱/۲۵

*نظر به اینکه مقادیر ذکر شده در سطح بی اهمیت صفر بود، این سطح در جدول گزارش نشد.

سیستمهای هشدار (از قبیل سیستم هشدار حریق) در سطح بسیار مهم (۰/۳۱±۴/۸۹) ارزیابی شد. "امکان تبادل دیجیتالی سیگنال‌های ویدئویی و تصاویر آنالوگ" کمترین میانگین را (۰/۸۸±۴/۱۷) به خود اختصاص داد(جدول ۳).

بر اساس یافته‌های پژوهش که در جدول۴ آمده است، از دیدگاه افراد شرکت‌کننده در پژوهش الزامات امنیت اطلاعات در فن‌آوری پزشکی از راه دور در زمینه منابع انسانی و تجهیزات تشخیص پزشکی از میانگین بالاتر و اهمیت بیشتری برخوردار بودند. سایر الزامات امنیت اطلاعات در شبکه پزشکی از راه دور در زمینه ذخیره‌سازی، دسترسی و انتقال اطلاعات از نظر اهمیت در سطوح بعدی قرار داشتند.

بحث و نتیجه‌گیری

در قرن حاضر با پیشرفت هایی که در حوزه فن‌آوری اطلاعات و ارتباطات[1] ایجاد شده، بسیاری از مؤسسات مراقبت بهداشتی برای ارتقاء کیفیت خدمات خود و رقابت با سایر سازمانها، به استفاده از دستاوردهای این فن‌آوری روی آورده‌اند. ظهور این دستاوردها سرعت انجام فعالیت-ها و ارائه خدمات در سازمانها را بهبود بخشیده و در نتیجه منجر به رضایت بیشتر مشتریان شده است. پزشکی از راه دور یکی از این دستاوردها است که تا حد زیادی مشکلات مربوط به بعد مسافت و دسترسی به خدمات مراقبت سلامت را مرتفع کرده است (۱۷).

امروزه، اگرچه سیستمهای پزشکی از راه دور در حال پیشرفت و گسترش هستند، اما مسائل و مشکلات مربوط به امنیت و محرمانگی اطلاعات در آنها همچنان مورد توجه طراحان و کاربران این سیستمها بوده است (۱۸). مؤسسات و سازمانهایی که در زمینه امنیت شبکه پزشکی از راه دور و استانداردهای امنیت اطلاعات فعالیت دارند پیوسته بر این امر مهم تاکید دارند که قبل از توسعه و بهره‌برداری سیستمهای پزشکی از راه دور باید الزامات امنیتی این سیستمها مورد بررسی و برنامه‌ریزی قرار گیرد (۱۰، ۹).

نتایج پژوهش حاضر نشان داد که رعایت امنیت در زمینه ذخیره‌سازی و دسترسی به اطلاعات از اهمیت بسیاری برخوردار بود. اکثریت افراد شرکت‌کننده در پژوهش بر وجود نرم‌افزارهایی برای ذخیره‌سازی اطلاعات و دستورالعمل‌هایی برای محدود کردن دسترسی به سیستم اطلاعات سلامت بیماران تاکید داشتند. به طور مشابه، در مطالعه‌ای که توسط Rialle و همکاران (۱۷) انجام شد، استفاده از رمزنگاری اطلاعات یا لایه ایمن (SSL-Secure Sockets Layer) به عنوان آسان-ترین راه برای حصول اطمینان از انتقال و ذخیره‌سازی مطمئن اطلاعات پزشکی از راه دور مطرح گردید. در این پژوهش داده‌های مربوط به مراقبت‌های ارائه شده به بیماران در منزل جمع‌آوری، تحلیل و براساس آن نرم افزاری به منظور کنترل بیماری و علائم حیاتی بیماران در خانه طراحی شده بود. در مطالعه دیگری Olanrewaju و همکاران (۱۸) بر حفاظت از تصاویر پزشکی که از طریق اینترنت ارسال می‌شوند و دسترسی به این تصاویر از طریق روش‌های تصدیق هویت تاکید نمودند .

به طور مشابه، در مطالعه حاضر اکثریت افراد شرکت-کننده در پژوهش رمزگذاری اطلاعات سلامت برای جلوگیری از دسترسی غیر مجاز را به عنوان پیش‌نیازی بسیار مهم جهت حفظ امنیت اطلاعات در پزشکی از راه دور ارزیابی کردند. بنابراین می‌توان گفت به طور کلی، 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 راه اندازی این شبکه باید مورد توجه قرار گیرد.

یافته‌های پژوهش حاضر نشان داد از جمله مهمترین الزامات امنیتی در زمینه انتقال اطلاعات پیاده سازی پروتکل‌های شبکه‌ای برای اطمینان از ارسال اطلاعات و بررسی یکپارچگی آنها می‌باشد. در همین رابطه، یافته-های پژوهش Harnett در سال ۲۰۰۶ (۱۹) نیز نشان داد که ایمنی تجهیزات و رسانه های انتقال اطلاعات در شبکه پزشکی از راه دور از جمله مواردی است که قبل از تبادل اطلاعات باید مورد توجه قرار گیرد. در کنار آن آموزش‌های لازم نیز جهت حفظ صحت و یکپارچگی اطلاعات باید به پرسنل و بیماران ارائه گردد.

براساس یافته‌های پژوهش، آگاهی دادن به کاربران در خصوص عواقب قانونی ناشی از افشای اسرار بیماران از جمله مهمترین نیازهای امنیتی در زمینه منابع انسانی

[1] Information and Communication Technology (ICT)

بود. به نظر می‌رسد با در نظر گرفتن چارچوب قانونی لازم، بستری برای رعایت امنیت اطلاعات از سوی کاربران فراهم خواهد شد و این چارچوب باید پیش از به کارگیری فن‌آوری پزشکی از راه دور تدوین شده باشد. این مهم در مطالعه Das و همکاران (۲۰) نیز مطرح شد و پژوهشگران اشاره کردند که مدیریت منابع انسانی و کاربران سیستمهای پزشکی از راه دور از طریق آموزش و اعمال محدودیت‌های دسترسی، تاثیر زیادی بر ارتقاء سطح امنیت شبکه پزشکی از راه دور خواهد داشت. در این پژوهش اشاره شده است که اعمال فشار در چارچوب قوانین و دستورالعمل‌های موجود می‌تواند کاربران را به رعایت الزامات امنیتی وادار نماید. به طور مشابه، در مطالعه Pendergrass و همکاران (۲۱) نیز افشاء ناخواسته اطلاعات از طریق اینترنت به عنوان یکی از نگرانی‌های کاربران مطرح شد. لذا می‌توان گفت که نتایج پژوهش حاضر با سایر پژوهش‌ها همخوانی دارد.

براساس یافته‌های پژوهش حاضر، مهمترین نیازهای امنیت اطلاعات در زمینه تجهیزات تشخیص پزشکی عبارت بودند از استفاده از اتاق سرور استاندارد و مجهز به سیستمهای هشدار و مجهز بودن سیستمهای شبکه پزشکی از راه دور به برق اضطراری. یافته ها نشان داد که مواردی مثل امکان تبادل دیجیتالی سیگنال‌های ویدئویی و تصاویر آنالوگ از دیدگاه افراد شرکت کننده در پژوهش از اهمیت کمتری برخوردار بودند. در این خصوص Garg در مطالعه‌ای بیان می‌کند که امروزه با گسترش فن‌آوری-های ارائه خدمات سلامت از راه دور، امنیت این مقوله نیاز به توجه بیشتری دارد. براساس یافته‌های این مطالعه، بی‌توجهی به امنیت تجهیزات و ابزارهای ارائه خدمات، به کیفیت پایین مراقبت، عدم اعتماد به نفس ارائه دهندگان و دریافت‌کنندگان مراقبت سلامت و نیز تخطی از قوانین مرتبط با حفظ محرمانگی و حریم خصوصی اطلاعات بیماران منجر خواهد شد (۲۲). بنابراین، باید توجه داشت که مقوله امنیت اطلاعات در حوزه پزشکی از راه دور باید در حوزه فنی و تجهیزات نیز دنبال شود. پر واضح است که ناقص بودن تجهیزات از بعد امنیتی فرایند به کار گیری فن‌آوری پزشکی از راه دور را با مشکل مواجه خواهد ساخت و تلاش در سایر حوزه های مرتبط را بی نتیجه خواهد گذاشت.

در این پژوهش تنها به نظر سنجی از مدیران واحد فن‌آوری اطلاعات در بیمارستان‌های آموزشی وابسته به دو دانشگاه علوم پزشکی کشور و کارشناسان واحد فن‌آوری اطلاعات وزارت بهداشت بسنده شد. با این وجود، به نظر می‌رسد نظرسنجی از مدیران واحد فن‌آوری اطلاعات در سایر مراکز درمانی و در بین تعداد بیشتری از افراد امکان تعمیم‌پذیری نتایج را افزایش خواهد داد. نظر به اهمیت الزامات امنیتی در شبکه پزشکی از راه دور پیشنهاد می‌گردد برنامه‌های آموزشی در زمینه مدیریت امنیت اطلاعات و جنبه‌های قانونی فن‌آوری پزشکی از راه دور برگزار گردد.

استفاده از 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 درجه اول باید حوزه‌ها و زیرمجموعه های مرتبط با امنیت اطلاعات شناسایی گردد تا با بررسی الزامات امنیتی در هر یک از حوزه های مطرح شده بتوان راهکارهای موثر و عملی را جهت ارتقاء سطح امنیت اطلاعات در فن‌آوری پزشکی از راه دور ارائه نمود. همچنین، براساس نتایج پژوهش، از آنجا که الزامات مربوط به منابع انسانی از درجه اهمیت بالاتری نسبت به سایر الزامات برخوردار بود، به نظر می‌رسد به کارگیری افراد با تجربه و متخصص، ارائه آموزش‌های لازم و بسترسازی فنی جهت استفاده از فن‌آوری پزشکی از راه دور، راه را برای به کارگیری کارآمد این فن‌آوری هموار خواهد ساخت.

سپاسگزاری

این مقاله حاصل پایان‌نامه تحت عنوان "بررسی نیازهای امنیت اطلاعات در فن‌آوری پزشکی از راه دور" در مقطع کارشناسی‌ارشد رشته مدارک پزشکی در سال ۱۳۹۲ و کد ۲۴۵ می‌باشد که با حمایت دانشگاه علوم پزشکی و خدمات بهداشتی درمانی ایران اجرا شده است.

منابع

1. Mehraeen E, Ayatollahi H, Ahmadi M. A study on information security in hospital information systems. Journal of Health Information Management 2014; 10(6): 788.

2. Mehraeen E, Ahmadi M, Shajarat M, Khoshgam M. Assessment of hospital information system in selected hospitals in tehran. Payavard Salamat 2013; 6(6):458-466.

3. Zain JM. Threats and challenges in securing telemedicine system. Int J Med Inform 2006; 15(2): 1-7.

4. Hein MA. Telemedicine: an important force in the transformation of healthcare. Int J Med Inform 2009; 9(2): 1-26.

5. Zhang GH, Poon CY, Li Y, Zhang YT. A biometric method to secure telemedicine systems. In:Proceedings of annual international conference of the IEEE EMBS Minneapolis; Minnesota USA; 2009: 2-6.

6. Wozak F, Schabetsberger T, Ammmenwerth E. End-to-end security in telemedical networks – A practical guideline. Int J Med Inform 2007; 76(1): 484-90.

7. Telemedicine Global. [Online]. [Accessed 2012 Sep 18]. Available from: http: // teledoctornet. lamula.pe/2009/11/03/telemedicine-in-healthcare-2-the-legal-and-ethical-aspects-of-using-new technology /unmedicoaventurero 2010.

8. Guillen E, Estupiñan P, Lemus C, Ramirez L. Analysis of security requirements in telemedicine networks. In:Proceedings of annual international conference of telecommunications engineering, Colombia: 2010.

9. Jack C, Mars M. Telemedicine a need for ethical and legal guidelines in South Africa. SA Fam Pract 2008; 50(2): 60-60d.

10. Broadband & Telemedicine. [Online]. 2011 [Accessed 2013 July 22]. Available from: http://www.nyls.edu/user_files/1/3/4/30/83/Broadband%20%20Telemedicine%20%20Policy%20Reccs.pdf.

11. Telemedicine, Telehealth, and Health Information Technology. [Online]. 2006 [Accessed 2013 July 20]. Available from: http://www.americantelemed.org/docs/default-source/policy/telemedicine-telehealth-and-health-information-technology.pdf?sfvrsn=8.

12. Asadi H, Akhlaghi H. Ethical and legal aspects of telemedicine and telecare tehran. In: proceedings of 1st international conference on information and knowledge technology, Iran, Tehran 2002.

13. Healthcare information and management systems society (HIMSS). Information systems security. [Online]. 2011 [Accessed 2011 Apr 14]. Available from:http://www.himss.org/content/files/applicationsecurityv2.3.pdf.

14. HIPAA related information security concerns in health care, HIPAA in health care: Information security in a health care environment. [Online].2010 [Accessed 2011 Apr 14]. Available from:http://www.infosecwriters.com/text_resources/pdf/InfoSec_In_ Health_Care_DJames.pdf.

15. Garg V, Brewer J. Telemedicine Security: A Systematic Review. J Diabetes Sci Technol 2011; 5(3): 768-77.

16. Rezgui Y, Marks A. Informatio security awareness in higher education: An exploratory study. Com and Sec 2008;27(7-8): 243.

17. Rialle V, Lamy JB, Noury N, Bajolle L. Telemonitoring of patients at home: a software agent approach. Com Meth & Prog Biomed 2003;72(1): 257-68.

18. Olanrewaju RF, Ali NB, Khalifa O, Manaf AA. ICT in Telemedicine: conquering privacy and security issues in health care services. electronic Journal of Computer Science and Information Technology (eJCSIT) 2013; 4(1): 19-24.

19. Harnett H. Telemedicine systems and telecommunications. J Telemed and Telecare 2006; 12: 1-12.

20. Das S, Mukhopadhyay A. Security and Privacy Challenges in Telemedicine. CSI Communications. [Online] .2011. [Accessed 2012 Nov 04]. Available from:http://www.definitions.net/definition/access+to+information.

21. Pendergrass JC, Heart K, Ranganathan C,Venkatakrishnan VN. A threat table based approach to telemedicine security. In: Transactions of the International Conference on Health

22. Garg V. Security concerns in telecare and telemedicine, [M.Sc. Dissertation]. Purdue University, Graduate School. 2009; 14-20.

Information Technology Advancement; 2013: Paper 38.