مجله دانشکده علوم پزشکی نیشابور

www.journalnums.ac.ir

استانداردهای امنیت اطلاعات در سیستم اطلاعات بیمارستانهای دانشگاه علوم پزشکی نیشابور

حسن ابراهیم پور صدقیانی[1،*]، فاطمه حیدرپور[2]

۱- گروه فناوری اطلاعات سلامت، دانشکده بهداشت، دانشگاه علوم پزشکی نیشابور، نیشابور، ایران

۲- کمیته تحقیقات دانشجویی، دانشگاه علوم پزشکی نیشابور، نیشابور، ایران

مقاله پژوهشی اصیل

تاریخ دریافت: ۱۴۰۰/۱۱/۰۲

تاریخ پذیرش: ۱۴۰۱/۰۷/۱۱

***نویسنده مسئول:** حسن ابراهیم پور صدقیانی؛ گروه فناوری اطلاعات سلامت، دانشکده بهداشت و پیراپزشکی، دانشگاه علوم پزشکی نیشابور، نیشابور، ایران.

تلفن:

پست الکترونیک:

ebrahimpourh@nums.ac.ir

چکیده

مقدمه

با توجه به تنوع خطراتی که اطلاعات را تهدید می‌کنند، تقویت امنیت و محرمانگی داده‌ها و اطلاعات سلامت در سازمان‌های مراقبت بهداشتی با عنایت به گستردگی سیستم‌های اطلاعات بیمارستانی در مراکز درمانی ضروری است، مطالعه حاضر با هدف بررسی امنیت سیستم اطلاعات بیمارستان‌های آموزشی-درمانی دانشکده علوم پزشکی نیشابور بر اساس استانداردهای HIPAA و ISO/IEC27001 انجام شد.

مواد و روش‌ها

پژوهش حاضر از نوع توصیفی-مقطعی بود که در سال ۱۴۰۰ انجام شد. جامعه پژوهش سیستم اطلاعات بیمارستانی بیمارستان‌های حکیم و ۲۲ بهمن دانشکده علوم پزشکی نیشابور بود. ابزار گردآوری در این پژوهش چک لیست محقق ساخته بر مبنای استانداردهای HIPAA و ISO/IEC27001-2005 بود. جمع‌آوری داده‌ها، با مراجعه حضوری محققین به بیمارستان‌های مورد نظر و مشاهده و بررسی اسناد مربوط به استانداردها و پرسش از کارشناسان بخش HIS (در هر بیمارستان ۴ نفر) انجام گرفت.

یافته‌ها

یافته‌های مطالعه نشان داد که استانداردهای فنی ۱۰۰ درصد در بیمارستان ۲۲ بهمن و در بیمارستان حکیم استانداردهای خط مشی امنیت اطلاعات ۱۰۰ درصد و تشکیلات امنیت اطلاعات ۹۰ درصد بالاترین حد رعایت را داشتند.

نتیجه‌گیری

علی رغم مطلوب بودن، امنیت اطلاعات در بیمارستان‌های مورد مطالعه، از آنجائیکه که روزانه اطلاعات بسیار زیادی در بیمارستان‌ها تبادل می‌شوند، عدم رعایت امنیت در حد نانو می‌تواند زیان‌های جبران‌ناپذیری را متوجه بیمارستان‌ها کند. لذا مدیران بخش‌های مدیریت اطلاعات سلامت و فن‌آوری اطلاعات بیمارستان‌ها باید با شناسایی نقاط آسیب‌پذیر و برنامه‌ریزی مناسب جهت بهبود کاستی‌های امنیت اطلاعات بیمارستان تلاش کنند.

کلیدواژه‌ها

استاندارد، امنیت اطلاعات، سیستم اطلاعات بیمارستانی، HIPAA، ISO/IEC27001

مقدمه

منابع اطلاعاتی، مهمترین سرمایه هر سازمان است که حمایت از این دارایی از طریق یک فرآیند امنیت اطلاعات اهمیت ویژه‌ای دارد (۱). امروزه در محیط‌های کسب و کار با فرآیندهای الکترونیک، نگرانی‌ها در خصوص امنیت در حال افزایش هستند که این امر مستلزم مدیریت و کنترل امنیت اطلاعات است (۲، ۳). امنیت اطلاعات، محافظت از منابع اطلاعاتی در برابر تهدیدات مختلف می‌باشد که برای تحقق آن نیاز به حداقل رساندن ریسک در کسب و کار و به حداکثر رساندن بازده سرمایه گذاری‌ها و فرصت‌های شغلی است (۴) که از این بین، به در دسترس‌بودن، صداقت و محرمانه ماندن اطلاعات تاکید بیشتری شده است (۵). این حوزه بسیار گسترده، پیچیده و شامل راهکارهایی جهت حفاظت از سرمایه‌های اطلاعاتی و منابع تکنیکی موجود در سیستم‌های کامپیوتری و کاهش خطرات تهدیدکننده آنها می‌باشد (۶). امروزه فناوری‌اطلاعات، یک سرمایه اقتصادی اساسی محسوب می‌شود (۷) و بسیاری از سازمان‌ها به دنبال ایجاد سیستم‌های امنیتی برای جلوگیری از افشای اطلاعات‌شان جهت ایجاد و توسعه فرهنگ امنیتی هستند تا بتوانند مجموعه تحت رهبری خودشان را از تهدیدات موجود حفظ کنند (۸). یکی از حوزه‌های متاثر از فناوری‌اطلاعات، بهداشت و درمان است (۹، ۱۰). فناوری اطلاعات در بخش سلامت، تسریع در گردآوری و دستیابی به اطلاعات، پشتیبانی از فرایندهای سیستم سلامت و تصمیم‌گیری اثربخش در مدیریت این سیستم می‌باشد، زیرا فراهم نمودن و ارائه مراقبت‌های سلامتی برای جامعه، امری بسیار پیچیده و مستلزم اطلاعات است (۱۱). یکی از سامانه‌های مهمی که در بیمارستان‌های کشور مورد استفاده قرار می‌گیرد، سیستم اطلاعات بیمارستانی است که جهت کنترل تمامی فعالیت‌های مربوط به سلامت (برنامه‌ریزی، نظارت، هماهنگی و تصمیم‌گیری) استفاده می‌شود (۱۲). از ویژگی‌های اساسی سیستم اطلاعات بیمارستان، حفظ محرمانگی و حریم‌خصوصی بیمار و احترام به خواست او در خصوص افشا یا عدم افشای سوابقش است (۱۳). مرور مطالعات گذشته نشان می‌دهد وضعیت مدارک پزشکی، محرمانه سازی و سطوح دسترسی به مدارک پزشکی در ایران با استانداردهای جهانی فاصله زیادی دارد، به همین منظور ایشان تاکید به رعایت اصول محرمانگی را از الزامات به کارگیری سیستم‌های اطلاعات بیمارستانی بیان کردند (۱۴). از آنجایی که هیچ فرمولی به طور صددرصد امنیت را تضمین نمی‌کند، استفاده از محک‌ها و استانداردهای جهانی به منظور اطمینان از تأمین سطح کافی امنیت، استفاده مناسب از منابع، اتخاذ بهترین روش‌های امنیتی، اجرای نیازهای سازمانی و مجموعه‌ای از کنترل‌های روابط تجاری با سازمان‌های دیگرضروری می‌شود (۱۵، ۱۶).

بر اساس مطالعات صورت گرفته، استانداردهای HIPAA و ISO از استانداردهای مهم و کاربردی در زمینه محرمانگی و امنیت اطلاعات بهداشتی می‌باشند (۱۲، ۱۷). اولین استاندارد که در زمینه امنیت سیستم‌های اطلاعاتی مطرح می‌باشد، استاندارد HIPAA است. قانون امنیتی HIPAA در دولت فدرال آمریکا تصویب و گسترش یافته است. تمرکز اصلی این قوانین بر حفاظت از افشای غیرمجاز اطلاعات بهداشتی بیماران است. این قوانین، اولین قوانین شناخته شده‌ی ملی جهت استفاده و افشای اطلاعات بهداشتی افراد به شمار می‌روند (۱۲). استاندارد HIPAA در خصوص امنیت سیستم‌های اطلاعاتی به سه بخش اصلی امنیت مدیریتی، فیزیکی و فنی تقسیم‌بندی می‌شود. بخش امنیت مدیریتی استاندارد HIPAA، به مواردی همچون تحلیل خطر، مدیریت خطر، خط مشی مجازات، فعالیت‌های سیستم اطلاعات، طرح پشتیبان داده‌ها، طرح بهبودی سانحه و طرح

عملیات شیوه‌ی اورژانسی تاکید می‌کند (۱۲، ۱۸). بخش امنیت فیزیکی، به استفاده‌ی مجدد از رسانه‌ها و نحوه‌ی منهدم‌کردن آنها اشاره دارد. در بخش امنیت فنی نیز موارد شناسایی کاربرِ واحد، یکپارچگی و رویه‌ی دسترسی‌های اورژانسی بحث شده‌اند (۱۲). با توجه به خطرات تهدیدکننده اطلاعات و نیاز مبرم به رویه‌های ایجاد و تقویت امنیت و محرمانگی، سازمان بین المللی استاندارد ISO ، اقدام به تدوین استانداردی در زمینه امنیت اطلاعات تحت عنوان ISO/IEC27001 نموده است.کسب تأییدیه‌ی ممیزی این استاندارد، منافع بسیار زیادی از جمله شناسایی عیوب موجود در بخش‌ها و فرآیندهای اطلاعاتی، افزایش اعتبار سازمان در محیط رقابتی و توسعه فرآیند امنیت اطلاعات صحیح برای سازمان به همراه دارد (۱۷). با توجه به اهمیت استاندارد جهانی ISO/IEC27001 در استقرار فرآیندهای مبتنی بر امنیت اطلاعات (حفظ محرمانگی، یکپارچگی و دسترس پذیری)، سازمان‌های مراقبت بهداشتی می‌بایست توجه ویژه‌ای برای به‌کارگیری آنها در فرآیندهای خود داشته باشند (۱۹). سیستم اطلاعات بیمارستانی بیمارستان‌های دانشکده علوم پزشکی نیشابور در سال ۱۳۸۸ از شرکت تیراژه رایانه تهران خریداری شد و برای اولین بار در بیمارستان حکیم پیاده‌سازی شد و در حال حاضر از این سیستم در دو بیمارستان حکیم و ۲۲ بهمن استفاده می‌شود. بر اساس مطالعات اولیه سیستم اطلاعات بیمارستان‌های مورد نظر حدود ۳۰۰ نفر کاربر دارند که به طور واقعی ۵۰ درصد از کاربران بالینی عملا با سیستم درگیر هستند. سیستم اطلاعات بیمارستان‌های دانشکده علوم پزشکی نیشابور دارای زیرسیستم‌های پرونده الکترونیک بیمار، مدیریت رویه‌های اداری- مالی بیمارستان، سامانه‌های پشتیبانی تصمیم سازی مبتنی بر شواهد، نوبت دهی بیماران، زیر سیستم‌های پاراکلینیکی و مدیریت بخش‌ها می‌باشد. با عنایت به مطالب بیان شده و با توجه به اهمیت موضوع امنیت اطلاعاتی در سیستم‌های اطلاعات بیمارستانی، این پژوهش با هدف بررسی امنیت اطلاعات در سیستم اطلاعات بیمارستان‌های آموزشی-درمانی دانشکده علوم پزشکی نیشابور براساس استانداردهای HIPAA و ISO انجام شد.

مواد و روش‌ها

پژوهش حاضر از نوع توصیفی-مقطعی می‌باشد که در سال ۱۴۰۰ انجام شد. سیستم اطلاعات بیمارستانی بیمارستان‌های حکیم و ۲۲ بهمن دانشکده علوم پزشکی نیشابور جامعه پژوهش مطالعه را تشکیل می‌دادند. ابزار گردآوری داده‌ها چک لیستی بر مبنای استانداردهای HIPAA و ISO/IEC27001 بود. چک لیست HIPAA مشتمل بر سه حیطه کلی استانداردهای امنیت مدیریتی، فیزیکی و فنی، درمجموع شامل ۱۲ گزاره استاندارد بود. حیطه امنیت مدیریتی با تعداد هفت گزاره استاندارد شامل مواردی چون تحلیل خطر، مدیریت خطر، خط مشی مجازات، بررسی فعالیت‌های سیستم اطلاعات، طرح پشتیبان داده‌ها، طرح بهبودی سانحه و طرح عملیات شیوه‌ی اورژانسی بود. در حیطه امنیت فیزیکی نیز، دو استاندارد استفاده‌ی مجدد از رسانه‌ها و نحوه منهدم‌کردن آنها با دو گویه بررسی شد. در حیطه امنیت فنی ۳ استاندارد نحوه شناسایی کاربر واحد، نحوه یکپارچگی و رویه‌های دسترسی اورژانسی بررسی شدند. چک لیست ISO مورد استفاده شامل تعداد ۱۲ گزاره استاندارد در دو حیطه کلی می‌باشد. حیطه‌های کلی عبارت بودند از: خط مشی امنیت اطلاعات و تشکیلات (ساختار) امنیت اطلاعات. هر سوال در چک لیست استاندارد خاصی را بررسی می‌کرد و شامل دو گزینه (استاندارد وجود دارد و استاندارد وجود ندارد) بود و در صورت وجود داشتن، "آیا اعمال می‌شود یا اعمال نمی‌شود"

بود و برای استانداردهای ISO گویه‌های "وجود دارد و وجود ندارد" مورد بررسی قرار گرفت. اعتبار علمی و محتوایی چک لیست توسط ده نفر از متخصصین فناوری اطلاعات سلامت، انفورماتیک پزشکی و همچنین کارشناسان فناوری اطلاعات و کامپیوتر مورد بررسی و با (CVR-.80) مورد تائید قرار گرفت. این مطالعه توسط کمیته اخلاق پژوهش دانشکده علوم پزشکی نیشابور با شماره IR.NUMS.REC.1400.022 مورخ ۱۴۰۰/۰۶/۰۸تأیید و با گرنت شماره ۱۲۱ تأمین مالی شد. برای جمع‌آوری داده‌ها، محققین به صورت حضوری به بخش فناوری اطلاعات بیمارستان‌های مورد نظر مراجعه کردند. ابتدا، هدف از تحقیق، توسط پژوهشگران برای کارشناسان فناوری اطلاعات که چهار نفر بود، توضیح داده شد. پس از کسب رضایت آگاهانه، از آنها خواسته شد تا برای تکمیل چک لیست‌ها با پژوهشگران همکاری کنند. همه مراحل تحقیق و مسائل اخلاقی و مقررات مربوطه مورد توجه قرار گرفت و حق محرمانگی اطلاعات و حق انصراف از تحقیق برای مشارکت‌کنندگان توضیح داده شد. پژوهشگران با مشاهده و بررسی اسناد مربوط به استانداردها و پرسش از کارشناسان بخش فناوری اطلاعات (در هر بیمارستان ۴ نفر)، چک لیست‌ها را تکمیل نمودند. تجزیه و تحلیل داده‌ها با استفاده از نرم افزار آماری SPSS نسخه ۲۲ و آمارهای توصیفی (فراوانی، درصد، میانگین و نمودار) انجام شد.

یافته‌ها

یافته‌های مطالعه نشان داد استانداردهای امنیت مدیریتی، فیزیکی و فنی به طور متوسط به ترتیب ۷۵ درصد، ۶۲/۵ درصد و ۱۰۰ درصد در بیمارستان ۲۲ بهمن به کارگرفته می‌شوند و در بیمارستان حکیم، ۶۴/۲ درصد استانداردهای امنیت مدیریتی، ۵۰ درصد استانداردهای امنیت فیزیکی و ۹۱/۷ درصد استانداردهای امنیت فنی، بطور متوسط رعایت می‌شدند (جدول ۱).

جدول۱- میزان به کارگیری استانداردهای امنیتی HIPAA در سیستم اطلاعات بیمارستان‌ها از دیدگاه کارشناسان (۴ نفر)

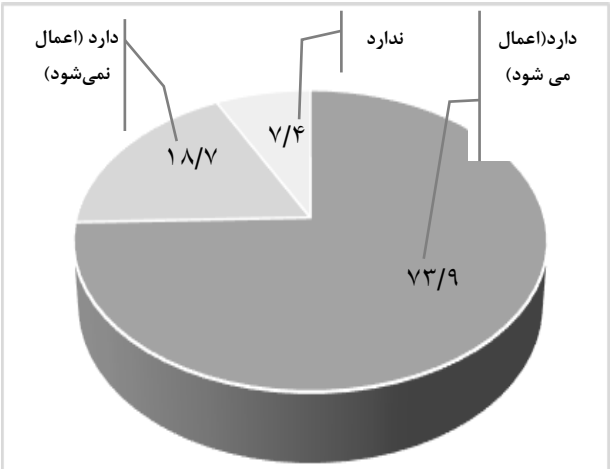
حیطه کلی استاندارد	بیمارستان‌ها / نوع اقدام/ استاندارد	۲۲ بهمن			حکیم		
		وجود دارد		وجودندارد	وجود دارد		وجود ندارد
		اعمال‌می‌شود	اعمال‌نمی‌شود		اعمال‌می‌شود	اعمال‌نمی‌شود	
امنیت مدیریتی	تحلیل خطر	۳(۷۵/۰)	۰(۰/۰)	۱(۲۵/۰)	۲(۵۰/۰)	۲(۵۰/۰)	۰(۰/۰)
	مدیریت خطر	۳(۷۵/۰)	۰(۰/۰)	۱(۲۵/۰)	۳(۷۵/۰)	۰(۰/۰)	۱(۲۵/۰)
	خط مشی مجازات	۳(۷۵/۰)	۰(۰/۰)	۱(۲۵/۰)	۲(۵۰/۰)	۰(۰/۰)	۲(۵۰/۰)
	بررسی فعالیت های سیستم اطلاعات	۳(۷۵/۰)	۰(۰/۰)	۱(۲۵/۰)	۳(۷۵/۰)	۰(۰/۰)	۱(۲۵/۰)
	طرح پشتیبان داده ها	۴(۱۰۰)	۰(۰/۰)	۰(۰/۰)	۴(۱۰۰)	۰(۰/۰)	۰(۰/۰)
	طرح بهبودی سانحه	۲(۵۰/۰)	۱(۲۵/۰)	۱(۲۵/۰)	۲(۵۰/۰)	۲(۵۰/۰)	۰(۰/۰)
	طرح عملیات شیوه اورژانسی	۳(۷۵/۰)	۱(۲۵/۰)	۰(۰/۰)	۲(۵۰/۰)	۲(۵۰/۰)	۰(۰/۰)
میانگین(درصد)		۳(۷۵/۰)	۰/۳(۷/۱)	۰/۷(۱۷/۹)	۲/۵(۶۴/۲)	۰/۸(۲۱/۴)	۰/۵(۲۱/۴)
امنیت فیزیکی	منهدم کردن	۲(۵۰/۰)	۱(۲۵/۰)	۱(۲۵/۰)	۲(۵۰/۰)	۲(۵۰/۰)	۰(۰/۰)
	استفاده مجدد از رسانه ها	۳(۷۵/۰)	۱(۲۵/۰)	۰(۰/۰)	۲(۵۰/۰)	۲(۵۰/۰)	۰(۰/۰)
میانگین(درصد)		۲/۵(۶۲/۵)	۱(۲۵/۰)	۰/۵(۱۲/۵)	۲(۵۰/۰)	۲(۵۰/۰)	۰(۰/۰)
امنیت فنی	شناسایی کاربر واحد	۴(۱۰۰)	۰(۰/۰)	۰(۰/۰)	۴(۱۰۰)	۰(۰/۰)	۰(۰/۰)
	رویه دسترسی اورژانسی	۴(۱۰۰)	۰(۰/۰)	۰(۰/۰)	۳(۷۵/۰)	۱(۲۵/۰)	۰(۰/۰)
	یکپارچگی	۴(۱۰۰)	۰(۰/۰)	۰(۰/۰)	۴(۱۰۰)	۰/۰	۰(۰/۰)
میانگین(درصد)		۴(۱۰۰)	۰(۰/۰)	۰(۰/۰)	۳/۶(۹۱/۷)	۰/۳(۸/۳)	۰(۰/۰)
میانگین کل درصدها		۷۹/۲	۱۰/۷	۱۰/۱	۶۸/۶	۲۶/۶	۴/۸

از نظر استانداردهای ISO، بطور متوسط استانداردهای خط مشی امنیت اطلاعات در بیمارستان ۲۲ بهمن و حکیم به ترتیب ۹۵ و ۱۰۰ درصد رعایت می‌شدند. استانداردهای مربوط به تشکیلات امنیت اطلاعات (برای واحدهای داخل سازمانی)، بطور متوسط در بیمارستان ۲۲ بهمن ۷۰ درصد و در بیمارستان حکیم ۸۰ درصد به کارگرفته می‌شدند و این استاندارد برای تشکیلات خارج سازمانی در هر دو بیمارستان ۱۰۰ درصد بود (جدول۲).

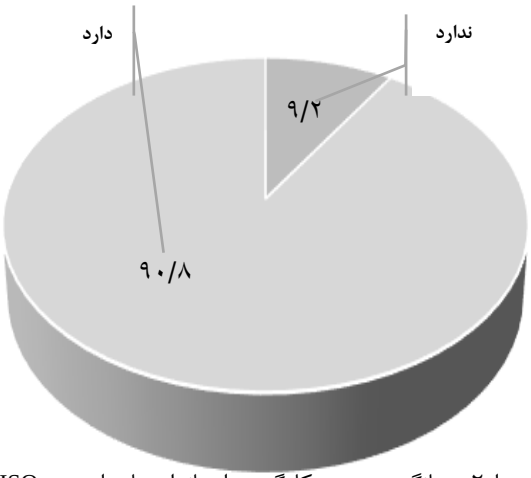
جدول۲- میزان به کارگیری استانداردهای امنیتی ISO در HIS بیمارستان ۲۲ بهمن

حیطه کلی استاندارد	بیمارستان‌ها / سوالات ممیزی / استاندارد	۲۲ بهمن		حکیم	
		دارد	ندارد	دارد	ندارد
خط مشی امنیت اطلاعات	آیا در سازمان سیاست امنیت اطلاعات که مورد تایید و استفاده مدیریت ارشد باشد و در اختیار تمامی کارکنان قرار گرفته باشد وجود دارد؟	۴(۱۰۰)	۰(۰/۰)	۴(۱۰۰)	۰(۰/۰)
	آیا سیاست حفاظت از اطلاعات در فواصل زمانی برنامه ریزی شده مورد بازبینی قرار می‌گیرد؟	۴(۱۰۰)	۰(۰/۰)	۴(۱۰۰)	۰(۰/۰)
	آیا سیاست حفاظت از اطلاعات دارای سرپرستی به منظور توسعه، بازبینی و ارزیابی سیاست حفاظت اطلاعات می‌باشد؟	۳(۷۵/۰)	۱(۲۵/۰)	۴(۱۰۰)	۰(۰/۰)
	آیا نتایج بازبینی مدیریت در سازمان مورد استفاده قرار می‌گیرد؟	۴(۱۰۰)	۰(۰/۰)	۴(۱۰۰)	۰(۰/۰)
	آیا تایید مدیریت ارشد برای تغییر سیاست حفاظت اطلاعات اخذ شده است؟	۴(۱۰۰)	۰(۰/۰)	۴(۱۰۰)	۰(۰/۰)
میانگین (درصد)		۹۵/۰	۵/۰	۱۰۰	۰/۰
تشکیلات امنیت اطلاعات (سازمان‌های داخلی)	آیا مدیریت برای سنجیدن و اندازه‌گیری امنیت درون سازمان حمایت فعالی نشان داده است؟	۲(۵۰/۰)	۲(۵۰/۰)	۴(۱۰۰)	۰(۰/۰)
	آیا فعالیت‌های امنیت اطلاعات به وسیله نمایندگانی از قسمت‌های مختلف هماهنگ و تعریف شده است؟	۲(۵۰/۰)	۲(۵۰/۰)	۳(۷۵/۰)	۱(۲۵/۰)
	آیا فرایند اختیارات مدیریت برای هر پردازش جدید اطلاعاتی مورد تعریف و اجرا در سازمان قرار گرفته است؟	۳(۷۵/۰)	۱(۲۵/۰)	۳(۷۵/۰)	۱(۲۵/۰)
	آیا الزام سازمانی برای یک قرارداد عدم افشای اطلاعات به منظور حفاظت از اطلاعات به طور شفاف تعریف گردیده؟	۴(۱۰۰)	۰(۰/۰)	۴(۱۰۰)	۰(۰/۰)
	آیا در سازمان دستورالعمل‌هایی در رابطه با تعریف اختیارات افراد وجود دارد؟	۳(۷۵/۰)	۱(۲۵/۰)	۲(۵۰/۰)	۲(۵۰/۰)
میانگین(درصدها)		۷۰/۰	۳۰/۰	۸۰/۰	۲۰/۰
تشکیلات امنیت اطلاعات (سازمان‌های بیرونی)	آیا ریسک‌ها و خطرات ناشی از اطلاعات سازمانی در مواجه با سطح دسترسی افراد بیرونی مورد شناسایی قرار گرفته است؟	۴(۱۰۰)	۰(۰/۰)	۴(۱۰۰)	۰(۰/۰)
	آیا دستورالعمل‌های برقراری ارتباط مشتری و یا قرارداد با اشخاص ثالث با الزامات امنیتی تطابق دارد؟	۴(۱۰۰)	۰(۰/۰)	۴(۱۰۰)	۰(۰/۰)
میانگین (درصد)		۱۰۰	۰/۰	۱۰۰	۰/۰
میانگین کل درصدها		۸۸/۳۳	۱۱/۶۷	۹۳/۳۳	۶/۶۷

همچنین نتایج مطالعه در رابطه رعایت استانداردها در بیمارستان‌های دانشگاه علوم پزشکی نشان داد که استانداردهای امنیت اطلاعات HIPA و ISO به ترتیب ۷۳/۸۹ درصد و ۹۰/۸۳ درصد رعایت می‌شدند (نمودار شماره ۱ و ۲).



نمودار۱- میانگین درصد بکارگیری استانداردهای امنیتی HIPA در بیمارستان‌های دانشگاه علوم پزشکی نیشابور



نمودار۲- میانگین درصد بکارگیری استانداردهای امنیتی ISO در بیمارستان‌های دانشگاه علوم پزشکی نیشابور

بحث

برنامه‌ریزی برای ایجاد و اجرای مکانیسم‌ها و استانداردهای امنیت اطلاعات در سازمان‌ها، در صورت داشتن چارچوب کلی جهت اجرای این استانداردها برای پایه‌ریزی و توسعه فرهنگ امنیت در کل سازمان کار دشواری نمی‌باشد (۲۰، ۲۱). سازمان‌های ارائه کننده استاندارد HIPAA و ISO با تعیین این چارچوب‌ها راه رسیدن به امنیت اطلاعات را در سازمان‌ها هموار کرده‌اند.

بر اساس یافته‌های پژوهش حاضر، از نظر استانداردهای امنیتی HIPAA (حیطه امنیت مدیریتی، امنیت فیزیکی و امنیت فنی)، در حیطه امنیت مدیریتی، بیمارستان ۲۲ بهمن وضعیت بهتری نسبت به بیمارستان حکیم داشت. حیطه اصلی امنیت مدیریتی HIPAA شامل موارد تحلیل خطر، مدیریت خطر، خط مشی مجازات، بررسی فعالیت‌های سیستم اطلاعات، طرح پشتیبان داده‌ها، طرح بهبودی سانحه، و طرح عملیات شیوه‌ی اورژانسی می‌باشد (۲۲). از بین موارد مطروحه، پشتیبانی داده‌ها در هر دو بیمارستان به صورت کامل اجرا می‌شد در حالی که در زمینه جلوگیری از سوانح احتمالی و وجود زیر ساخت‌های لازم در مراکز مذکور در وضعیت مطلوبی قرار نداشت. در راستای مطالعه حاضر، در مطالعه‌ای که شریفیان و همکاران انجام دادند مدیریت خطر و طرح پشتیبانی داده‌ها در بیمارستان‌های مورد مطالعه بطور کامل اعمال می‌شدند (۱۲). همچنین در گزارش دبیرخانه شورای اطلاع‌رسانی ایران بر وجود یک چارچوب مشخص برای تحلیل و مدیریت خطر به منظور ایمن‌سازی تبادل اطلاعات تاکید می‌شود (۲۳). "مدیریت خطر" و "فعالیت‌های سیستم اطلاعات" در بیمارستان‌های مورد مطالعه به میزان ۷۵ درصد اعمال می‌شود. وَگِر و همکاران در ارتباط با "مدیریت خطر" قانون امنیتی HIPAA بیان کردند که باید معیارهایی برای کاهش دادن

خطرات و آسیب‌های امنیتی وجود داشته باشد. همچنین به وجود دستورالعمل‌هایی برای بررسی فعالیت‌های سیستم اطلاعات از جمله گزارشات دسترسی، گزارشات ردیابی و رویدادهای امنیتی اشاره کرده‌اند (۱۸).

حیطه امنیت فیزیکی استانداردهای HIPAA شامل استفاده‌ی مجدد از رسانه‌ها و نحوه منهدم‌کردن آنها می‌باشد. بیشتر از نصف موارد بررسی شده در رابطه با این حطیه از استاندارد HIPAA در بیمارستان‌های مورد مطالعه رعایت می‌شد و نسبت به سایر حیطه‌ها وضعیت مناسبی نداشت. شاید از دلایل این موضوع بتوان به آموزشی بودن بیمارستان‌ها و وجود مدیریت ضعیف در آنها اشاره نمود. در این خصوص صدوقی و همکاران در مطالعه خود قوانین و مقرراتی را پیشنهاد کرده‌اند که سازمان‌ها می‌توانند در مدیریت خود استفاده نمایند (۱۴). طیق نتایج مطالعه شریفیان و همکاران قوانین استفاده مجدد از رسانه‌ها در اغلب بیمارستان‌ها اعمال می‌شود ولی میزان رعایت این استاندارد را ۵۰ درصد گزارش کردند (۱۲). بنابراین، تدوین راهکارهایی در رابطه با مدت زمان نگهداری داده‌های الکترونیک، نحوه انهدام آن‌ها و استفاده مجدد از رسانه‌ها الزامی و نیاز به توجه بیشتر دارد (۲۴).

شناسایی کاربر واحد، یکپارچگی و رویه دسترسی اورژانسی از جمله استانداردهای الزامی و مهم HIPAA در حیطه امنیت می‌باشند. میزان رعایت این استانداردها در بیمارستان ۲۲ بهمن و حکیم به ترتیب ۱۰۰و ۹۱ درصد بوده است. بر اساس یافته‌های مطالعه حاضر "شناسایی کاربر واحد" در همه مراکز اعمال می‌شد و طبق قانون HIPAA به کارگیری نام و شماره اختصاصی برای هر کاربر به منظور شناسایی و ردیابی مشخصات کاربر الزامیست (۱۸). الزامات مربوط به "یکپارچگی" در مراکز مذکور از سطح بالایی برخوردار بود که این مورد در پژوهش میدانی در سطح متوسطی قرار داشت. اما طبق پژوهش شریفیان و همکاران، یکپارچگی در هیچ کدام از بیمارستان‌ها اعمال نمی‌شد (۱۲). وَگِر و همکاران طبق قانون HIPAA اشاره کردند که در مواقع اورژانسی باید رویه‌هایی برای دسترسی به اطلاعات الکترونیک ضروری وجود داشته باشد (۱۸). خوشبختانه بر اساس یافته‌های مطالعه، "رویه دسترسی اورژانسی" در بیمارستان‌های مورد مطالعه به میزان قابل توجهی (بالای ۸۵ درصد) اعمال می‌شد. پیشرفت و بهبود کیفیت طراحی سیستم‌های اطلاعات بیمارستانی در دهه‌های اخیر می‌تواند یکی از دلایل مهم این امر باشد. در حال حاضر حدود بیست و دو شرکت در زمینه طراحی سیستم‌های اطلاعات بیمارستانی در ایران فعال هستند که به دلیل وجود رقابت در این صنعت، وضعیت طراحی این سامانه‌ها و اثربخشی آنها در بهبود مراقبت نسبت به قبل بسیار بهبود یافته است (۲۵).

استاندارد ISO دارای سه حیطه اصلی خط مشی امنیت اطلاعات و تشکیلات امنیت اطلاعات (داخلی و خارج سازمانی) می‌باشد. میزان رعایت استاندارد در دو حیطه خط مشی امنیت اطلاعات و تشکیلات امنیت برون سازمانی در هر دو بیمارستان از وضعیت مطلوب و قابل قبولی برخوردار بودند. این درحالی است که یافته‌های ابومسعودی و همکاران بر خلاف یافته‌های مطالعه حاضر، به کارگیری این استاندارد در مراکز مورد پژوهش ۳۱ درصد گزارش کردند (۱۷). کولویل در مطالعه‌ی خود تحت عنوان "عوامل انسانی و امنیت اطلاعات" اشاره کردند که کارکنان سازمان چون به اطلاعات و بخش‌های مختلف سازمان دسترسی‌های قانونی دارند، خطرات امنیتی جدی برای سازمان نسبت به افراد بیرون از سازمان محسوب می‌شوند که باید برای کاهش خطرات داخلی سازمان، پیشگیری‌ها و تدابیر فنی اندیشیده شود (۸). توجه به جنبه‌های نظری و سیاستی امنیت

اطلاعات در واقع از نقاط قوت اکثر سازمان‌ها می‌باشد. اما متاسفانه در جنبه ساختار و تشکیلات معمولا این سازمان‌ها با ضعف تشکیلاتی مواجه هستند و یافته‌های این مطالعه نیز موید این حقیقت است؛ بطوری که میزان رعایت استانداردهای ساختار و تشکیلات امنیت اطلاعات در حوزه ساختار داخلی در بیمارستان ۲۲ بهمن و حکیم نسبت به دو حیطه دیگر در سطح بسیار پائینی قرار داشت که پیشنهاد می‌گردد در این رابطه کارشناسان فنی تدابیر و برنامه‌ریزی مهم و لازم طرح نمایند. از نظر رعایت استانداردهای امنیتی HIPPA و ISO رعایت استانداردهای ISO نسبت به HIPAA بیشتر رعایت می‌شد. در مطالعاتی که شریفیان و همکاران و ابومسعودی و همکاران داشتند درصد رعایت این استانداردها را برای HIPAA برابر ۵۷/۱ و برای ISO برابر ۴۹ درصد گزارش کردند (۱۲، ۱۷) که در مقام مقایسه، بیمارستان‌های مورد مطالعه در مطالعه حاضر از وضعیت بسیار مطلوبی برخوردار بودند.

نتیجه‌گیری

در مجموع، یافته‌های این تحقیق نشان داد که علی رغم مطلوب بودن رعایت برخی از استانداردهای امنیت اطلاعات در بیمارستان‌های مورد مطالعه، وضعیت به کارگیری استانداردهای امنیت اطلاعات در حیطه‌های امنیت مدیریتی، امنیت فیزیکی و تشکیلات مربوط به سازمان داخلی نیازمند توجه بیشتری است. با توجه به این که امروزه اطلاعات بزرگترین دارایی سازمان‌ها محسوب می‌شوند و روزانه تبادل اطلاعات با حجم وسیعی در سازمان‌ها بویژه در بیمارستان‌ها صورت می‌گیرد، انتظار می‌رود اجرای مطالعاتی مانند پژوهش حاضر، به مدیران بخش‌های مدیریت اطلاعات سلامت و فن آوری اطلاعات بیمارستان‌ها کمک کند تا نقاط آسیب‌پذیر را یافته و برنامه‌ریزی مناسبی در جهت بهبود موارد کاستی امنیتی داشته باشند.

تشکر و قدردانی

این مطالعه حاصل طرح تحقیقات دانشجویی با شماره ۱۲۱ و با کد اخلاق NUMS.REC.1400.022 دانشکده علوم پزشکی نیشابور می‌باشد. از حمایت‌های مالی و علمی دانشکده علوم پزشکی نیشابور و کارشناسان فناوری اطلاعات که به نحوی ما را در انجام این پژوهش یاری نمودند، صمیمانه سپاسگزاری می‌شود.

تعارض منافع

نویسندگان اظهار می‌دارند که هیچ گونه تضاد منافعی نداشتند.

References

1. Sheikhpour R, Modiri NJIJoS, Applications I. An approach to map COBIT processes to ISO/IEC 27001 information security management controls. 2012;6(2):13-28.

2. Kankanhalli A, Teo H-H, Tan BC, Wei K-K. An integrative study of information systems security effectiveness. International journal of information management. 2003;23(2):139-54.

3. Thomson K-L, Von Solms R. Information security obedience: a definition. Computers & Security. 2005;24(1):69-75.

4. Schweizerische S. Information technology-Security techniques-Information security management systems-Requirements. ISO/IEC International Standards Organization. 2013.

5. Safa NS, Von Solms R, Furnell S. Information security policy compliance model in organizations. computers & security. 2016;56:70-82.

6. Crossler RE, Johnston AC, Lowry PB, Hu Q, Warkentin M, Baskerville R. Future directions for behavioral information security research. computers & security. 2013;32:90-101.

7. Susanto12 H, Almunawar MN, Tuan YC. Information security management system standards: A comparative study of the big five. International Journal of Electrical Computer Sciences IJECSIJENS. 2011;11(5):23-9.

8. Colwill C. Human factors in information security: The insider threat–Who can you trust these days? Information security technical report. 2009;14(4):186-96.

9. Ajami S, Ketabi S, Saghaeiannejad S, Heidari A. Requirements and areas associated with readiness assessment of electronic health records implementation. Journal of Health Administration. 2011;14(46).

10. Nasiripour AA, Rahmani H, Radfar R, Najafbeigi R. Effective elements on e-health deployment in Iran. African Journal of Business Management. 2012;6(16):5543-50.

11. Phunchongharn P, Hossain E, Niyato D, Camorlinga S. A cognitive radio system for e-health applications in a hospital environment. IEEE Wireless Communications. 2010;17(1):20-8.

12. 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.

13. Torabi M, Safdari R. Electronic Medical Record. Tehran, Iran: Behineh Publication. 2004.

14. Sadoughi F, KHOUSH KM, SIAVASH B. A comparative investigation of the access levels and confidentiality of medical document in Iran and selected countries. 2007.

15. Sheikhpour R, Modiri N. An approach to map COBIT processes to ISO/IEC 27001 information security management controls. International Journal of Security and Its Applications. 2012;6(2):13-28.

16. Tofan DC. Information security standards. Journal of Mobile, Embedded and Distributed Systems. 2011;3(3):128-35.

17. Abumasoudi RS, Habibi SK, Ataei M, Esmaeili N. Evaluation of Information Management Systems in Isfahan University of Medical Science by ISO/IEC 27001 Standard. Health Information Management, 2015; 12(3): 306-316. doi: 10.22122/him.v12i3.1897

18. Wager KA, Lee FW, Glaser JP. Managing health care information systems: a practical approach for health care executives: John Wiley & Sons; 2005.

19. Hajavi A, Khoushgam M, HATAMI M. A Comparative Study on regarding Rate of the Privacy Principles in legal Issues by WHO Manual at Teaching Hospitals of Iran, Tehran and Shahid Beheshti Medical Sciences Universities; 2007. 2008.

20. Colwill CJIstr. Human factors in information security: The insider threat–Who can you trust these days? 2009;14(4):186-96.

21. Vela FG, Montes JI, Rodríguez PP, Román MS, Valverde BJJSoCP. An architecture for access control management in collaborative enterprise systems based on organization models. 2007;66(1):44-59.

22. Baskerville RJACS. Information systems security design methods: implications for information systems development. 1993;25(4):375-414.

23. Hendelman-Baavur LJMERoIA. Promises and perils of Weblogistan: Online personal journals and the Islamic Republic of Iran. 2007;11(2):77-93.

24. MEIDANI Z, ASSARI MA, MOSAVI SG, ATAEI AA. Evaluation of hospital information systems security. 2017.

25. Mohammadpour A, Ghaemi MM, Darrudi R, Sadagheyani HE. Use of Hospital Information System to Improve the Quality of Health Care from Clinical Staff Perspective. Galen Medical Journal. 2021;10:e1830-e.

Journal of Neyshabur University of Medical Sciences

www.journalnums.ac.ir

Information security standards in the information system of hospitals of Neyshabur University of Medical Sciences

Hasan Ebrahimpour Sadageyani[1,*], Fateme Heidarpour[2]

1- Department of Health Information Technology, Neyshabur University of Medical Sciences, Neyshabur, Iran.
2- Students Research Committee, Neyshabur University of Medical Sciences, Neyshabur, Iran.

Original Article

Received: 22 Jan 2022
Accepted: 3 Oct 2022

***Corresponding Author:**
Hassan Ebrahimpour Sadagheyani, Neyshabur University of Medical Science, Neyshabur, Iran
TEL:
Email:
sadageyani@yahoo.com

A B S T R A C T

Introduction

Given the variety of risks that threaten information, it is necessary to strengthen the security and confidentiality of data and health information in health care organizations, given the breadth of hospital information systems in medical centers. The aim of this study was to investigate the security of the information system of Neyshabur University of Medical Sciences based on HIPAA and ISO / IEC27001 standards.

Method and material

The present study was a descriptive cross-sectional study that was conducted in 2021. The study population was the hospital information system of Hakim and 22 Bahman hospitals of Neyshabur University of Medical Sciences. The collection tool in this study was a researcher-made checklist based on HIPAA and ISO / IEC27001 standards. Data collection was done by visiting the researchers in person and observing and reviewing the documents related to the standards and asking questions from HIS experts (4 people in each hospital).

Results

The findings of the study showed that the technical standards of 100% in Bahman 22 Hospital and in Hakim Hospital had the highest standards of information security policy of 100% and information security organizations of 90%.

Conclusion

Despite the desirability of information security in the hospitals under study, because so much information is exchanged in hospitals on a daily basis, non-compliance with nano-level security can cause irreparable damage to hospitals. Therefore, the managers of health information management and information technology departments of hospitals should try to identify the vulnerabilities and plan to improve the shortcomings of hospital information security.

Keywords

Standard, Information Security, Hospital Information System, HIPAA, ISO/IEC27001

► ***Please cite this article as:*** Ebrahimpour Sadagheyani H, Heidarpour F. Information security standards in the information system of hospitals of Neyshabur University of Medical Sciences. J Neyshabur Univ Med Sci 2022;10(1)131-142.