بررسی عملکرد امنیت در سیستم‌های اطلاعات بیمارستانی بر اساس استاندارد مدل عملکردی EHR در مراکز آموزشی –درمانی شهرستان تبریز

زکیه پیری[1]، شهلا دمنابی[2]، هیرو خضری[3*]، ناصر شیخی[4]

تاریخ دریافت 1393/04/15 تاریخ پذیرش 1393/06/25

چکیده

پیش‌زمینه و هدف: با توجه به سیاست‌های ابلاغی وزارت بهداشت و درمان و آموزش پزشکی کشور مبنی بر الزام بیمارستان‌ها و مراکز درمانی به تشکیل پرونده الکترونیک سلامت لزوم ایجاد محیط امن بیش‌ازپیش نمایان می‌شود. در این پژوهش ضمن معرفی استاندارد مدل عملکردی به ارزیابی عملکرد امنیت در سیستم‌های اطلاعات بیمارستانی مراکز آموزشی_ درمانی شهرستان تبریز پرداخته شده است.

مواد و روش کار: پژوهش حاضر از نوع مطالعات توصیفی پیمایشی بوده که به‌صورت مقطعی در سال ۹۲ انجام گرفت. جامعه پژوهش کلیه مراکز آموزشی-درمانی شهرستان تبریز بود که در بین آن‌ها نمونه‌گیریی انجام نگرفت. ابزار جمع‌آوری داده‌ها پرسشنامه‌ای بر اساس استاندارد مدل عملکردی بود. پرسشنامه ازنظر روایی و پایایی مورد ارزیابی قرار گرفت. تجزیه‌وتحلیل داده‌ها با استفاده از نرم‌افزار آماری SSPS16 و به کمک T تک نمونه‌ای (به‌منظور مقایسه میانگین نمونه آماری با میانگین جامعه آماری) صورت گرفته شد.

یافته‌ها: میانگین کلی عملکرد امنیت در مراکز آموزشی-درمانی شهرستان تبریز ۳/۸۴±۰/۵۹ هست. این امر نشانگر وضعیت مطلوب این مؤلفه‌ها در سیستم‌های اطلاعات بیمارستانی هست. در این میان عملکرد فرعی "تصدیق موجودیت" با میانگین ۴/۴۷±۰/۴۹ بیشترین میانگین و عملکرد فرعی "مدیریت دسترسی بیمار "با میانگین ۲/۲۰±۰/۶۳ کمترین میانگین را در مراکز آموزشی-درمانی دارد .تفاوت معنی‌داری در خصوص رعایت مؤلفه‌های امنیت به‌استثنای مؤلفه ایمنی در تبادل اطلاعات در سیستم‌های اطلاعات بیمارستانی وجود داشته است(P=۰/۰۰۲).

بحث و نتیجه‌گیری: نظر به اینکه عملکرد فرعی "مدیریت دسترسی بیمار" در وضعیت نامطلوب قرار داشت. لذا پیشنهاد می‌گردد شرکت‌های نرم‌افزاری و بیمارستان‌ها ضمن ملحوظ داشتن کلیه مؤلفه‌های مدل عملکردی مدیریت دسترسی بیمار را بیشتر موردتوجه قرار دهند.

کلیدواژه‌ها: محرمانگی، سیستم اطلاعات بیمارستانی، مدل عملکردی

مجله دانشکده پرستاری و مامایی ارومیه، دوره دوازدهم، شماره هشتم، پی‌درپی 61، آبان 1393، ص ۶۱۲-۶۰۶

آدرس مکاتبه: دانشکده مدیریت و اطلاع‌رسانی، دانشگاه علوم پزشکی تبریز، تلفن: ۰۹۱۴۴۸۱۴۹۷۲

Email: Hkhit2012@yahoo.com

مقدمه

استفاده از قابلیت‌های فناوری اطلاعات در صنعت سلامت، به شکل کاربردهای مختلف سلامت الکترونیک، روز به روز گسترده‌تر می‌شود (۱). راه‌اندازی پرونده‌های الکترونیکی و سیستم اطلاعات بیمارستانی با استفاده از کامپیوتر برای جمع‌آوری، ذخیره، پردازش، بازیابی و ارتباط اطلاعات مدیریتی و مراقبتی بیمار از اهداف اساسی هست (۲). سیستم‌های اطلاعات بیمارستانی ابزاری الکترونیک هستند که اطلاعات مالی، اداری و بالینی بیماران را جمع‌آوری، طبقه‌بندی، نگهداری و با استفاده از قابلیت‌های کامپیوتر بازیابی می‌کنند و در اختیار تصمیم‌گیرندگان در هر زمان و هر مکان قرار می‌دهند (۳). در همین راستا پرونده الکترونیک سلامت دربرگیرنده اطلاعات مراقبت بهداشتی، در طول حیات فرد، ذخیره‌شده به‌صورت الکترونیکی، با هدف پشتیبانی از مراقبت مستمر، آموزش و پژوهش است (۴).

[1] استادیار گروه فن‌آوری اطلاعات سلامت تبریز، دکتری مدیریت اطلاعات بهداشتی درمانی، دانشکده مدیریت و اطلاع رسانی، دانشگاه علوم پزشکی تبریز

[2] مربی گروه فن‌آوری اطلاعات سلامت تبریز، کارشناس ارشد مدارک پزشکی، دانشکده مدیریت و اطلاع رسانی، دانشگاه علوم پزشکی تبریز

[3] دانشجوی کارشناسی ارشد فن‌آوری اطلاعات سلامت، دانشکده مدیریت واطلاع رسانی، دانشگاه علوم پزشکی تبریز (نویسنده مسئول)

[4] کارشناس ارشد آمار، دانشگاه علوم پزشکی ارومیه

در طراحی پرونده الکترونیک سلامت در هر کشوری یکی از عوامل مهم موردتوجه، ایجاد زیرساخت مناسب اطلاعات سلامت است (۵). عملکرد صحیح زیرساخت اطلاعات سلامت به محرمانگی و امنیت داده‌ها و قابلیت تبادل پیام بستگی دارد (۶). ازآنجاکه امنیت و کنترل اطلاعات بهداشتی مربوط به بیمار یک جزء اساسی در تمام سیستم‌های اطلاعاتی مراقبت بهداشتی است (۷). دراین‌ارتباط نگرانی زیادی در مورد حفظ حریم شخصی و تأمین امنیت اطلاعات به وجود آورده است زیرا مدارک پزشکی بیمار شامل برخی از خصوصی‌ترین و محرمانه‌ترین اطلاعات بیمار بوده و اطلاعات رایانه‌ای از مکان‌های متعددی قابل‌دسترس است. نقص امنیتی این سیستم‌ها خطر افشای اطلاعات را به دنبال خواهد داشت (۸). در حوزه مراقبت سلامت، حریم خصوصی به معنی حق افراد برای محدود کردن دسترسی سایرین به اطلاعات مراقبت سلامت آن‌هاست. از طرفی بیماران انتظار دارند تا اطلاعاتی که در طول دوره مراقبت در اختیار اعضای تیم مراقبت گذاشته‌اند تنها برای مقاصد درمانی مورداستفاده قرار گیرد. از این موضوع به‌عنوان محرمانگی یاد می‌شود (۹). بررسی انجام‌شده در سال ۲۰۰۴ در آمریکا حاکی از آن است که نگرانی‌های ایمنی و محرمانگی اطلاعات، بزرگ‌ترین مانع اجرای گسترده سیستم‌های پرونده کامپیوتری و توزیع داده‌ها شده است (۱۰). راهکارهای فراوانی جهت حفظ حقوق محرمانگی اطلاعات موجود در پرونده‌های بیماران ارائه گردیده است فرزندی پور در سال ۱۳۸۶ به طراحی الگوی اصول محرمانگی اطلاعات پرونده سلامت الکترونیک برای ایران پرداخته است که این الگو بر محوریت رضایت بیمار در اصول محرمانگی پرونده سلامت الکترونیک تأکید دارد (۱۱). شریفیان در پژوهشی با عنوان بررسی مکانیسم‌های حفاظتی در سیستم‌های اطلاعات بیمارستانی بر اساس استانداردهای امنیتی HIPAA در دانشگاه علوم پزشکی شیراز نشان داد که از هفت مورد مکانیسم حفاظتی مدیریتی دو مورد مدیریت خطر و طرح پشتیبان داده‌ها، به‌طور کامل در همه بیمارستان‌ها و دو مورد مکانیسم حفاظتی فیزیکی الزامی در اکثر بیمارستان‌ها اعمال می‌شد. از دو مورد مکانیسم فنی الزامی، تنها در یک بیمارستان‌ها اعمال می‌شد (۱۲)

Dougherty در مقاله خود با عنوان چگونه EHR شما قانونی است؟ می‌نویسد پرونده پزشکی به‌عنوان شاهد در بسیاری از موارد دادخواهی شامل قصور پزشکی، غرامت دادن به کارکنان، استخدام و ... ارائه می‌شود. در روش سنتی ارائه‌دهندگان مراقبت پرونده کاغذی (و یا پرینت از سیستم الکترونیکی) را به‌عنوان شاهد ارائه می‌دهند؛ اما مراجع قانونی درباره سیستم‌های الکترونیکی حساسیت نشان می‌دهند. بنابراین سازمان‌های مراقبت سلامت باید بپذیرند که پرونده الکترونیک سلامت آن‌ها برای دادخواهی مورداستفاده قرار خواهد گرفت. آن‌ها باید گام‌هایی در این زمینه بردارند که این اطمینان را بدهد که سیستم آن‌ها مکانیسم‌های مناسبی برای حمایت از پرونده بی‌نقص قانونی فراهم می‌کند. معیارهای سازمان HL7 به سازمان‌ها در شناسایی عملکردهای EHR که پرونده بی‌نقص ازنظر قانونی را حمایت کند یاری می‌رساند. سازمان‌ها می‌توانند از مدل عملکردی EHR برای ارزیابی نرم‌افزارهای موجود و جدید و نرم‌افزارهای منحصربه‌فرد و یا تمام سیستم استفاده کنند (۱۳). مدل عملکردی EHR[1] از فعالیت‌های HL7 (Health Level 7) در زمینه EHR می‌باشد که به‌عنوان یک مجموعه عالی از عملکردهای است که در همه مراکز سلامت برای مستند کردن ارائه مراقبت سلامت موردنیاز است این مدل شامل مجموعه‌ای از عملکردها و توصیفات سازمان‌دهی شده است عملکردهای EHR در سه بخش اصلی در نظر گرفته می‌شوند:

عملکردهای مراقبت مستقیم

عملکردهای پشتیبانی

عملکردهای زیرساخت اطلاعاتی عناصر اصلی زیرساخت اطلاعاتی عناصر امنیت، محرمانگی، قابلیت انتقال، ثبت و واژگان می‌باشند (۱۴).

عملکرد امنیت شامل ۹ عملکرد فرعی می‌باشد شامل عملکرد فرعی تصدیق موجودیت، عملکرد فرعی صدور مجوز، عملکرد فرعی کنترل دسترسی موجودیت، عملکرد فرعی مدیریت دسترسی بیمار، عملکرد فرعی عدم انکار، عملکرد فرعی ایمنی تبادل اطلاعات، عملکرد فرعی مسیریابی امن دادها، عملکرد فرعی حریم شخصی بیمار و محرمانه بودن، عملکرد فرعی اطلاعات برای تصدیق می‌باشد (۱۵). با توجه به سیاست‌های ابلاغی وزارت بهداشت و درمان و آموزش پزشکی کشور مبنی بر الزام بیمارستان‌ها و مراکز درمانی به تشکیل پرونده الکترونیک سلامت لزوم ایجاد محیط امن بیش‌ازپیش نمایان می‌شود (۱۶). همچنین نظر به رویکرد کشورمان به سمت طراحی و ایجاد سیستم‌های اطلاعات بیمارستانی و پرونده الکترونیک سلامت و لزوم وجود مکانیسم‌های حفاظتی، بررسی وضعیت موجود از اهمیت خاصی برخوردار است (۱۲). در این راستا بررسی عملکرد امنیت در سیستم اطلاعات بیمارستانی بر اساس مدل عملکردی در بیمارستان‌های آموزشی دانشگاه علوم پزشکی تبریز موضوع این پژوهش قرار گرفت.

[1] Electoronic Health Record

مواد و روش‌ها

این پژوهش توصیفی از نوع پیمایشی بوده و به‌صورت مقطعی در سال ۱۳۹۲ انجام گرفته است. جامعه پژوهش کلیه بیمارستان‌های آموزشی- درمانی شهرستان تبریز بود این مراکز عبارت بودند از بیمارستان‌های مدنی، امام رضا، علوی، سینا، شهدا، رازی، کودکان، طالقانی، نیکوکاری و بابا باغی که به دلیل محدودیت تعداد نمونه، نمونه‌گیری انجام نگرفت. معیار ورود به مطالعه مجهز بودن به سیستم اطلاعات بیمارستانی در زمان انجام تحقیق بود. بیمارستان بابابغی به دلیل مجهز نبودن به سیستم اطلاعات بیمارستانی در زمان انجام تحقیق از مطالعه حذف گردید. ابزار گرداوری داده‌ها پرسشنامه‌ای بر اساس آخرین نسخه استاندارد مدل عملکردی بود که توسط پژوهشگر ترجمه‌شده و متشکل از ۹ عملکرد فرعی بوده است. به‌منظور تعیین روایان فرم اعتبارسنجی پرسشنامه بین ۸ نفر از افراد خبره در امر توزیع و از سه جنبه شفافیت، اهمیت و تناسب تأیید گردید و برای تعیین پایایی از روش آزمون باز آزمون استفاده شد. بدین‌صورت که دو بیمارستان خارج از جامعه پژوهش (مراکز خصوصی شهرستان تبریز) که داری سیستم اطلاعات بیمارستانی بود به‌عنوان نمونه آزمایشی انتخاب‌شده بود و در دو نوبت به فاصله دو هفته پرسشنامه مذکور تکمیل گردیده است. سپس ضریب همبستگی بین پاسخ‌های این دو نوبت محاسبه و R=۱ به دست آمد. شایان‌ذکر است هر دو بار پرسشنامه توسط پژوهشگر تکمیل گردیده بود و هیچ‌گونه تغییری در سیستم مکانیزه این مرکز در طول این مدت صورت نگرفته بود. پرسشنامه مذکور با روش مصاحبه با مسئولین بخش فناوری اطلاعات تکمیل گردید. تجزیه‌وتحلیل داده‌ها با استفاده از نرم‌افزار آماری SSPS16 و به کمک T تک نمونه‌ای (به‌منظور مقایسه میانگین نمونه آماری با میانگین جامعه آماری) صورت گرفته است. تصمیم‌گیری نهایی بر اساس مقیاس بازرگان صورت گرفته است. بر اساس استاندارد موردنظر نتایج به‌دست‌آمده حاصل از میانگین ۱ تا ۲/۳۳ را در وضعیت نامطلوب، ۲/۳۴ تا ۳/۶۷ را در سطح نسبتاً مطلوب و ۳/۶۷ تا ۵ را در وضعیت مطلوب ارزیابی می‌کنند (۱۷).

ملاحظات اخلاقی: ازآنجاکه سیستم‌های اطلاعات بیمارستانی از سوی شرکت‌های نرم‌افزاری متفاوت در بیمارستان‌ها ارائه‌شده بود جهت همکاری بیشتر مسئولین و جلوگیری از هرگونه سوگیری از ذکر اسامی شرکت‌ها خودداری شده است. همچنین ازآنجاکه جامعه پژوهش مراکز آموزشی – درمانی با تخصص‌های گوناگون که از بسیاری جهات (تعداد تخت؛ امکانات ...) تفاوت داشتند بنابراین از مقایسه مراکز خودداری شده است. ضمن اینکه به‌تمامی مراکز معرفی‌نامه از طرف دانشگاه شده است؛ و با واحد حراست مراکز هماهنگی لازم انجام گرفته است.

یافته‌ها

با توجه به نتایج جدول ۱ میانگین کلی امنیت ۳/۸۴±۰/۵۹ می‌باشد. تصدیق موجودیت با میانگین ۴/۴۷±۰/۴۹؛ صدور مجوز ۳/۹۰±۰/۶۹؛ کنترل دسترسی ۴/۱۰±۰/۵۱؛ عدم انکار ۴/۶۰±۰/۶۹؛ مسیریابی داده‌های امن ۳/۷۰±۰/۶۷؛ حریم شخصی بیمار ۴/۴۰±۰/۹۶ و اطلاعات وسیله‌ای برای تصدیق ۳/۹۷±۰/۹۳ قرار داشت. این امر نشانگر وضعیت مطلوب این مؤلفه‌ها در سیستم‌های اطلاعات بیمارستانی بوده است. مؤلفه ایمنی در تبادل اطلاعات با میانگین ۳/۲۵±۰/۴۸ در وضعیت نسبتاً مطلوب و مدیریت دسترسی بیمار با میانگین ۲/۲۰±۰/۶۳ در وضعیت نامطلوب قرار داشت. آماره T نشان می‌دهد که تفاوت معنی‌داری در خصوص رعایت مؤلفه‌های امنیت به‌استثنای مؤلفه ایمنی در تبادل اطلاعات مدل عملکردی EHR در سیستم‌های اطلاعات بیمارستانی وجود داشت.

جدول (۱): نتایج آزمون t تک متغیری میزان رعایت مؤلفه امنیت، مدل عملکردی EHR در سیستم‌های اطلاعات بیمارستانی

متغیر	میانگین	انحراف استاندارد	خطای استاندارد میانگین	آماره T	درجه آزادی	سطح معنی‌داری	تفاوت میانگین
امنیت	۳/۸۴	۰/۵۹	۰/۱۸	۴/۴۸	۹	۰/۰۰۲	۰/۸۴
تصدیق موجودیت	۴/۴۷	۰/۴۹	۰/۱۵	۹/۴۷	۹	۰/۰۰۰	۱/۴۷
صدور مجوز	۳/۹۰	۰/۶۹	۰/۲۲	۴/۰۷	۹	۰/۰۰۳	۰/۹۰
کنترل دسترسی	۴/۱۰	۰/۵۱	۰/۱۶	۶/۷۳	۹	۰/۰۰۰	۱/۱۰
مدیریت دسترسی بیمار	۲/۲۰	۰/۶۳	۰/۲۰	۰۴/۰۰	۹	۰/۰۰۳	-۰/۸۰
عدم انکار	۴/۶۰	۰/۶۹	۰/۲۲	۷/۲۳	۹	۰/۰۰۰	۱/۶۰
ایمنی در تبادل اطلاعات	۳/۲۵	۰/۴۸	۰/۱۵	۱/۶۲	۹	۰/۱۳	۰/۲۵
مسیریابی داده‌های امن	۳/۷۰	۰/۶۷	۰/۲۱	۳/۲۸	۹	۰/۰۱	۰/۷۰
حریم شخصی بیمار	۴/۴۰	۰/۹۶	۰/۳۰	۴/۵۸	۹	۰/۰۰۱	۱/۴۰
اطلاعات وسیله‌ای برای تصدیق	۳/۹۷	۰/۹۳	۰/۲۹	۳/۲۸	۹	۰/۰۰۹	۰/۹۷

جدول شماره ۱ نشان می‌دهد که در میان عملکردهای فرعی عملکرد امنیت عملکرد فرعی تصدیق موجودیت با میانگین ۴/۴۷±۰/۴۹ بیشترین میانگین و عملکرد فرعی مدیریت دسترسی بیمار با میانگین ۲/۲۰±۰/۶۳ کمترین میانگین را در مراکز آموزشی-درمانی دارد.

بحث و نتیجه‌گیری

عملکرد فرعی" تصدیق موجودیت "به تأیید هویت کاربران قبل از دسترسی و همچنین جلوگیری از دسترسی همه کاربران غیرمجاز و به‌کارگیری مکانیسم‌های تأیید اشاره دارد (۱۶، ۱۸). این مورد در مراکز آموزشی – درمانی شهرستان تبریز در وضعیت مطلوبی قرار دارد در این رابطه صفدری می‌نویسد پروسه تصدیق و تأیید مسئولیت قانونی ثبت اطلاعات است که متفاوت از امضای معمولی پزشک روی کاغذ است (۱۹). شریفیان در پژوهش خود بیان می‌کند" تصدیق شخص یا موجودیت" تنها در یک بیمارستان از بیمارستان‌های موردمطالعه اعمال می‌شد (۱۲). این مورد با نتایج پژوهش ما همخوانی ندارد. عملکرد فرعی" صدور مجوز" اشاره به این مهم که کاربران به چه منابع اطلاعاتی و چه اقداماتی روی آن‌ها مجاز به انجام هستند و این دسترسی بر مبنای هویت افراد و نقش یا وظایف کاری و... می‌باشد (۱۶،۱۸). این مورد در مراکز مذکور در وضعیت مطلوبی قرار داشت صفدری در این رابطه می‌نویسد که سیاست‌ها و رویه‌هایی باید برای دسترسی به پرونده‌های الکترونیکی تدوین شوند و نرم‌افزاری تهیه کند که تمام دسترسی‌های کاربران را تعریف و پشتیبانی کند و از استفاده غیرمجاز از یک منبع اطلاعاتی پرهیز کند (۱۹). عملکرد فرعی "کنترل دسترسی موجودیت" اشاره به این مورد که دسترسی به اطلاعات کنترل شود و افراد مجاز باید و افراد غیرمجاز نباید توانایی دسترسی داشته باشند دارد (۱۶،۱۸). این مورد در بیمارستان‌ها در وضعیت مطلوبی قرار دارد صفدری دراین‌باره بیان می‌کند که کنترل دسترسی ابزاری است که تعیین می‌کند که دسترسی به سیستم پرونده فقط به‌وسیله اشخاص مجاز امکان‌پذیر است و تعیین‌کننده آن است که اطلاعات بهداشتی شخصی محرمانه نگهداری می‌شود یعنی تنها برای اهداف تأییدشده و بین افراد مجاز و با رضایت آگاهانه تسهیم می‌شوند (۱۹). بررسی سال ۲۰۰۳ در کانادا نشان می‌دهد که ۸۰ درصد سازمان‌ها، دسترسی کارمندان و پزشکان را به پرونده‌های بالینی را فراهم می‌کنند. تمام سازمان‌ها برای کنترل و دسترسی به سیستم‌های بالینی شناسه کاربری و رمز عبور داشته و ۹۰ درصد سازمان‌ها شناسه کاربری و رمز عبور واحدی دارند (۲۰). عملکرد فرعی "مدیریت دسترسی بیمار "اشاره به مدیریت و اجازه دسترسی بیمار به اطلاعات سلامت شخصی بیمار دارد که در مراکز آموزشی – درمانی تبریز در وضعیت نامطلوب قرار داشت (۱۶). صفدری در این رابطه می‌نویسد بیمار باید مطابق با قوانین تدوین‌شده مجاز به اصلاح یا تغییر اطلاعات هویتی پرونده‌اش باشد و داده‌های غیر صحیح یا ناقص را تصحیح کند؛ و هر بیمار بزرگ‌سال یا نماینده قانونی بیمار مجاز باشند که مطابق با قوانین تدوین‌شده تمام اطلاعات ذخیره‌شده در پرونده را جستجو و کپی کند (۱۹). عملکرد فرعی" عدم انکار " اشاره به این مورد دارد که در انتقال اطلاعات و یا انجام عملی روی اطلاعات، گیرنده یا فرستنده و یا عمل‌کننده روی اطلاعات نباید قادر به انکار عمل خود باشد (۱۶،۱۸). در مراکز آموزشی – درمانی تبریز در وضعیت مطلوب قرار داشت. عملکرد فرعی "ایمنی در تبادل اطلاعات" به این نکته اشاره دارد که در تبادل اطلاعات امنیت و محرمانگی رعایت شود و مکانیسم‌های رمزگذاری مبتنی بر استاندارد برای مبادله ایمن داده‌ها استفاده شود (۱۶). این مورد در مراکز آموزشی – درمانی تبریز در وضعیت نسبتاً مطلوب قرار دارد. همچنین عملکرد فرعی "مسیریابی داده‌های امن" به معنی انجام مبادله الکترونیکی روتین داده‌ها با منابع و مقاصد شناخته‌شده و امن می‌باشد (۱۶). این مورد در مراکز آموزشی – درمانی تبریز در وضعیت مطلوب قرار دارد. عملکرد فرعی" حریم شخصی بیمار و محرمانه بودن" یعنی قوانین برای حفظ محرمانگی و امنیت بسته به آسیب‌پذیری بیمار و حساسیت پرونده متفاوت می‌باشد (۱۶). این مورد در مراکز آموزشی – درمانی تبریز در وضعیت مطلوب قرار داشت. حبیبی فرد معتقد است که لازم است اطلاعات بیماران بر اساس درجه محرمانگی به سه‌طبقه اطلاعات اداری، تشخیصی درمانی و مالی و در سه‌طبقه داخلی، محرمانه و سری تقسیم‌بندی شده و ضمن تعریف میزان دسترسی به هر طبقه، سازوکارهایی جهت حفاظت از اطلاعات به اجرا درآید (۲۱). عملکرد فرعی "اطلاعات وسیله‌ای برای تصدیق" اشاره به این مورد دارد که اطلاعات هویت نویسنده را نشان دهد و برای هر عمل، رویداد، تشخیص و ... مسئول تعیین کند (۱۶،۱۸)؛ که در مراکز آموزشی – درمانی تبریز در وضعیت مطلوب قرار داشت.

با توجه به بررسی انجام‌شده در ارتباط با استاندارد مدل عملکردی EHR عملکردهای فرعی "ایمنی در تبادل اطلاعات " که در وضعیت نسبتاً مطلوب قرار داشت و"مدیریت دسترسی بیمار" که در وضعیت نامطلوب قرار داشت. این عملکردها نیاز به توجه بیشتر دارند. لذا پیشنهاد می‌گردد شرکت‌های نرم‌افزاری ضمن ملحوظ داشتن کلیه مؤلفه‌های مدل عملکردی این موارد را بیشتر موردتوجه قرار دهند؛ و با گنجاندن کامل عملکردهای مدل عملکردی EHR در بسته‌های نرم‌افزاری خود زمینه زیرساخت

پرونده الکترونیک سلامت را هموار سازند. همچنین بـه مسـئولین فن‌آوری اطلاعات بیمارستان‌ها و سایر کاربران پیشنهاد می‌شود در صورت وجود این قابلیت‌ها در جهت به‌کارگیری و استفاده از آن‌هـا اقدام نمایند. ازآنجاکه مدل عملکردی EHR دارای اسـتانداردهایی در زمینه پشتیبانی و مراقبت مستقیم نیز می‌باشد به پژوهشـگران پیشـنهاد مـی‌گـردد سیسـتم‌هـا اطلاعـات بیمارسـتانی را بـا ایـن استانداردها نیز ارزیابی نماینـد. همچنـین سـایر مراکـز آموزشـی- درمانی نیز پژوهشـی مشـابه ایـن پـژوهش بـر روی سیسـتم‌هـای اطلاعات بیمارستانی انجام دهند. از محدودیت‌هـای ایـن پـژوهش عدم دسترسی به آخـرین نسـخه اسـتانداردهای مـدل عملکـردی EHR، عدم وجود مطالعه‌ای در زمینه ارزیـابی بـا اسـتاندارد مـدل عملکردی بود.

تقدیر و تشکر

این مقاله حاصل بخشی از پایان‌نامه کارشناسی ارشد می‌باشد که با حمایت دانشگاه علوم پزشکی تبریز اجرا شده است همچنین پژوهشگران در پایـان از همکـاری کلیـه اسـاتید و صـاحب‌نظـران دانشگاه علوم پزشکی ارومیه و مراکـز آموزشـی- درمـانی تبریـز و جناب آقای آیرملو و آقای سلطان‌زاده مشاور محترم آماری نهایـت تشکر و قدردانی را دارند.

References:

1. Safari Mehr E. Prioritizing eHealth Applications with Respect to Technology Acceptance Factors (Dissertation). Tehran: Tarbiat Modares University, Faculty of Engineering; 2009. (Persian)
2. Shortliffe EH, Perreault LE. Medical informatics: computer applications in health care and biomedicine. New York: Springer; 2001.
3. Moradi GH. New Dimensions of HIM. Tehran: Vajehpardaz; 2002. (Persian)
4. Rezaei P, Ahmadi M, Sadogh F. A Study on Content, Structure & Nomenclature Standard of Electronic Health Record in Selected Organization & Suggested a Patern for Iran. J Health Adm 2007; 10(29). (Persian)
5. Farzandipour M, Ahmadi M, Sadoughi F, Karimi I. A comparative study on security reqierments of electronic health record in selected countries. Inf health Manag J 2009;5(2).
6. Jebraeeli M, Piri Z, Rahimi B, Ghasemzadeh M, Mahmoudi A. Administrative barriers to the implementation of electronic records. Health Inf Manag 2012;8(6):807.
7. Fakhrzad M, Fakhrzad N, Dehghani M. The Role of electoronic Health Record in presenting health information. Model for Iran. Excellence in e-learning progress Medical Te 2011;2(4).
8. Huffman E. Electronic Medical Record. Translated by Langarizadeh M. Tehran:Dibagaran; 2006. (Persian)
9. Wager K, Wickham F, Glaser J. Health Care Information Systems:a practical approach for health care executives. Translated by: Sheikhtaheri A, NaseriBooriabadi T, Sadegh Ahmadi M. Jafari pub;2013.
10. Himss. 2004 Himss National health information infrastructure survey. 2004 July. Available at:http://www.ncvhs.com
11. Farzandipour M. Designing an EHR information confidentially Model for Iran. J Health Info Manag 2008; (11):35. (Persian)
12. Sharifian R, Nematollahi M, Monem H, Ebrahimi F. Investigating the HIPAA Security Safeguards in theHIS of Shiraz University of Medical Sciences hospitals. Health Inf Mang 2013;10(1).
13. Dougherty M. How Legal Is Your HER?. J AHIMA 2008. 24-30.
14. Quinsey, Carol Ann. Using HL7 Standards to Evaluate an EHR. J AHIMA 2006; 77(4): 64A-C.
15. Devalt P, Fischetti L, Rowlands D, Speare C. HL7 HER TC Membership Level 2 Ballot on the EHR-S Functional Model, RELEASE 1.2007;[1-34] Available from: URL www. HL7.org
16. Vaghezinejad M, Information security.Tehran: 2012.

17. Bazrgan A, Sarmad Z, Hejazi E. Methods of Research in Scienc Behavioral Agah; 2008. (Persian)
18. Stevens love H, VanDyk P. HL7 EHR Work group Electronic Health record system Functional glossary. 2011; Available from: URL www. HL7.org.
19. Safdari R, Sieyed Farsjalah S. Strategies to protect the rights of patients in EHR systems. J Med Purification 2009;(74):48-56.
20. Canada Health infoway. Infoway pan-canadin HER survey phase I Results and Analysis.2003 January.availabel at: http://www.canadahealthinfoway.ca
21. Habibifard V. Operational Model for Information Security System. First congress of IT Application in Health. Sari: 2011.P.499.

Original Article

INVESTIGATING THE FUNCTIONAL MODEL EHR SECURITY SAFEGUARDS IN THE HIS OF TABRIZ UNIVERSITY OF MEDICAL SCIENCES

Piri Z[1],Damnabi SH[2], KHezri H[3],Naser SH[4]*

Received: 6 Jul , 2014; Accepted: 16 Sep , 2014

Abstract

Background &Aims :A safe environment for establishing an electronic health record is one of the priorities of Ministry of Health for all hospitals in Iran. The purpose of this study was to determine security standards, and to evaluate the hospital information systems according to that standards.

Materials & Methods*:* This is a cross-sectional descriptive study. Ten teaching hospitals with a hospital information system which were affiliated to Tabriz University of Medical Sciences were evaluated. The data were collected by using a self-constructed checklist according to the Functional Model of HER, and the interviews with the hospitals IT authorities. Data were analyzed using SPSS 16.

Results: The information infrastructure part of EHR functional model consists seven major parts, and security is one of them in which nine sub functions have been defined. The total rate for all security standards was 3/84 ±0/59. The higher rate was for authorization sub function (4/47±0/49), and the lower rate was for patient access management sub function (2/20±0/63). There was a significant relationship between the components rate of security part except for secure data exchange (P=0/002).

Conclusion: Considering the low rate of patient access management, it is recommended that HIS users and venders take into account this sub function besides their attention to all sub functions of EHR functional model.

Keywords: Functional Model Standard, hospital information system, confidentiality

Address: School of Health Services Management and Medical Informatics, Tabriz University of Medical Sciences
Tel: (+98)9144814972
Email: Hkhit2012@yahoo.com

[1]*Associate professor of Health Information Management, School of Health Services Management and Medical Informatics ,Tabriz University of Medical Sciences,Tehran,Iran*
[2] *Instructor of Health I nformation, School of Health Services Management and Medical Informatics,Tabriz University of Medical Sciences,Tehran,Iran*
[3]*Msc Student in Health Information Technology, School of Health Services Management and Medical Informatics,Tabriz University of Medical Sciences,Tehran,Iran; (Corresponding Author)*
[4]*Msc in statistics,Urmia University of Medical Sciences*