بررسی مکانیسم‌های امنیتی در سیستم‌های اطلاعات بیمارستانی بر اساس استاندارد امنیتی هیپا (Health insurance portability and accountability act) در بیمارستان‌های آموزشی دانشگاه علوم پزشکی شیراز*

رکسانا شریفیان[۱]، محترم نعمت‌الهی[۲]، حسین منعم[۳]، فاطمه ابراهیمی[۴]

مقاله پژوهشی

چکیده

مقدمه: یکی از ویژگی‌های اساسی سیستم اطلاعات بیمارستانی، حفظ محرمانگی می‌باشد. تحقیقات نشان می‌دهد که در کشور ما الزامات امنیتی پرونده‌ی الکترونیک سلامت به طور کامل و دقیق به کار گرفته نمی‌شود. این پژوهش، با هدف تعیین درصد اعمال مکانیسم‌های حفاظتی استانداردهای امنیتی (Health insurance portability and accountability act یا HIPAA) در بیمارستان‌های منتخب آموزشی دانشگاه علوم پزشکی شیراز در سال ۱۳۸۹ انجام پذیرفت.

روش بررسی: تحقیق حاضر از نوع توصیفی- مقطعی بود. جامعه‌ی پژوهش، بیمارستان‌های آموزشی دانشگاه علوم پزشکی شیراز مجهز به سیستم اطلاعات بیمارستانی بود. ابزار جمع‌آوری داده‌ها، چک لیستی بر اساس قانون استاندارد امنیتی HIPAA بود. روایی ابزار با روش روایی محتوی سنجیده شد. نحوه‌ی جمع‌آوری داده‌ها به صورت مصاحبه با مسؤولین فن‌آوری اطلاعات بیمارستان‌های مورد مطالعه بود. تحلیل داده‌های جمع‌آوری شده با استفاده از آمار توصیفی انجام شد.

یافته‌ها: از هفت مورد مکانیسم حفاظتی مدیریتی الزامی (تحلیل خطر، مدیریت خطر، خط‌مشی مجازات، بررسی فعالیت‌های سیستم اطلاعات، طرح پشتیبان داده‌ها، طرح بهبودی سانحه، طرح عملیات شیوه‌ی اورژانسی)، دو مورد مدیریت خطر و طرح پشتیبان داده‌ها، به طور کامل در همه‌ی بیمارستان‌ها و دو مورد مکانیسم حفاظتی فیزیکی الزامی (منهدم کردن و استفاده‌ی مجدد از رسانه‌ها) در اکثر بیمارستان‌ها اعمال می‌شد. از دو مورد مکانیسم فنی الزامی، شناسایی کاربر واحد، به طور کامل و رویه‌ی دسترسی اورژانسی، تنها در یک بیمارستان اعمال می‌شد.

نتیجه‌گیری: در جهت افزایش میزان اعمال مکانیسم حفاظتی مدیریتی الزامی، می‌بایست برنامه‌ریزی اجرایی انجام گیرد. اعمال کامل مکانیسم‌های حفاظتی فیزیکی الزامی که فاصله‌ی چندانی تا اجرای کامل آن در همه‌ی بیمارستان‌های تحت مطالعه وجود نداشت و مکانیسم حفاظتی فنی الزامی، گام‌های مهمی در جهت ارتقای سیستم امنیتی در نظام اطلاعات بیمارستان‌ها خواهد بود.

واژه‌های کلیدی: هیپا؛ سیستم‌های اطلاعات بیمارستانی؛ محرمانگی

دریافت مقاله: ۱۳۹۱/۳/۲۲ اصلاح نهایی: ۱۳۹۱/۱۰/۲۷ پذیرش مقاله: ۱۳۹۱/۱۱/۳۰

ارجاع: شریفیان رکسانا، نعمت‌الهی محترم، منعم حسین، ابراهیمی فاطمه. **بررسی مکانیسم‌های امنیتی در سیستم‌های اطلاعات بیمارستانی بر اساس استاندارد امنیتی هیپا (Health insurance portability and accountability act) در بیمارستان‌های آموزشی دانشگاه علوم پزشکی شیراز.** مدیریت اطلاعات سلامت ۱۳۹۲؛ ۱۰ (۱): ؟؟

* این مقاله حاصل تحقیقی دانشجویی در مقطع کارشناسی است.

۱- استادیار، مدیریت اطلاعات سلامت، دانشکده‌ی مدیریت و اطلاع‌رسانی پزشکی، دانشگاه علوم پزشکی شیراز، شیراز، ایران (نویسنده‌ی مسؤول)
Email: sharifianr@sums.ac.ir
۲- استادیار، مدیریت اطلاعات سلامت، دانشکده‌ی مدیریت و اطلاع‌رسانی پزشکی، دانشگاه علوم پزشکی شیراز، شیراز، ایران
۳- دانشجوی دکتری، کامپیوتر، دانشکده‌ی کامپیوتر و سیستم‌های اطلاعاتی، دانشگاه فن‌آوری مالزی، کوالالامپور، مالزی
۴- کارشناس، مدارک پزشکی، دانشگاه علوم پزشکی شیراز، شیراز، ایران

مقدمه

سیستم اطلاعات بیمارستانی (HIS یا Hospital information system)، پیاده‌سازی سیستم یکپارچه‌ی تولید اطلاعات لازم برای مدیریت تمامی فعالیت‌های مربوط به سلامت از قبیل برنامه‌ریزی، نظارت، هماهنگی و تصمیم‌گیری است. هدف از استقرار یک نظام اطلاعات بیمارستانی، به کارگیری رایانه و وسایل ارتباطی برای جمع‌آوری، ذخیره، پردازش، بازیابی و ارتباط دادن مراقبت بیمار و اطلاعات اداری برای تمامی فعالیت‌های مربوط به بیمارستان است (۱). در همین راستا پرونده‌ی الکترونیک سلامت، اطلاعات مراقبت بهداشتی طول حیات فرد را به صورت الکترونیکی و با هدف پشتیبانی از فعالیت‌های بیمارستان نگهداری می‌کند (۲). در این ارتباط، نگرانی زیادی در مورد حفظ حریم شخصی و تأمین امنیت اطلاعات وجود دارد، زیرا مدارک پزشکی بیمار شامل برخی از خصوصی‌ترین و محرمانه‌ترین اطلاعات بیمار می‌باشد و اطلاعات رایانه‌ای از مکان‌های متعددی قابل دسترس است. نقص امنیتی این سیستم‌ها خطر افشای اطلاعات را به دنبال خواهد داشت. امنیت اطلاعات به معنای کنترل دسترسی و حفظ اطلاعات از افشای تصادفی یا غیر عمدی به افراد غیر مجاز و جایگزینی، دستکاری یا فقدان اطلاعات می‌باشد (۳).

اطلاعاتی که بین پزشک و بیمار رد و بدل می‌شود، باید تا حد امکان محرمانه باقی بماند تا بیمار بتواند با آرامش اطلاعات خود را با پزشک در میان بگذارد و بتواند مؤثرترین و کاراترین درمان را دریافت نماید (۴). ویژگی‌های اساسی سیستم اطلاعات بیمارستانی که باید حتی بین تیم‌های مراقبت‌های اجتماعی به اشتراک گذاشته شود، حفظ محرمانگی و حریم شخصی بیمار و احترام گذاشتن به خواست او در خصوص افشا یا عدم افشای سوابق او است (۵). مطالعات موجود، رعایت اصول و استانداردها حفظ محرمانگی اطلاعات سلامت را کامل مناسب نمی‌دانند. صدوقی و همکاران اظهار داشته‌اند که وضعیت مدارک پزشکی، محرمانه‌سازی و سطوح دسترس به مدارک پزشکی در ایران با استانداردهای جهانی فاصله‌ی زیادی دارد، ایشان رعایت اصول محرمانگی را در این ارتباط امری ضروری می‌دانند (۶). در نتایج مطالعه‌ی فرزندی‌پور و همکاران نیز آمده است که با توجه به تحقیقات انجام شده در ایران به مدت ده سال، همچنان ضوابط و اصول خاصی بر افشای اطلاعات بیماران حاکم نیست و متولیان امر نسبت به ایجاد ضوابط بی‌تفاوت یا بی‌اطلاع بوده‌اند (۴). ایشان در مطالعه‌ی دیگری (به نقل از صدوقی و همکاران) به این نکته اشاره دارند که با توجه به این که ایمنی اطلاعات پرونده‌ی الکترونیک سلامت یکی از ضروریات حرکت به سمت ایجاد و استفاده از پرونده‌ی الکترونیک سلامت در هر کشوری است، کشورمان فاقد الزامات جامعی در این خصوص می‌باشد (۷). حاجوی و همکاران نیز در تحقیق مشابهی آورده‌اند که با توجه به تفاوت وضعیت محرمانگی اکثر بیمارستان‌های کشور با استانداردهای جهانی توصیه می‌شود که به محرمانگی و افشای اطلاعات بیمار در موارد قانونی بیشتر توجه و در جهت بهبود و ارتقای قوانین آن‌ها اقدام گردد (۸). در حال حاضر مجموعه‌ای از استانداردهای مدیریتی و فنی ایمن‌سازی فضای تبادل اطلاعات سازمان‌ها ارایه شده است که از مهم‌ترین آن‌ها استانداردهای گنجانده شده در قانون امنیتی HIPAA (Health insurance portability and accountability act) می‌باشد. «قانون امنیتی HIPAA» در دولت فدرال امریکا تصویب و گسترش یافته است و مسؤول حفاظت از افشای غیر مجاز اطلاعات بهداشتی بیماران و اولین قوانین شناخته شده‌ی ملی جهت استفاده و افشای اطلاعات بهداشتی افراد است (۹). این قانون به سه بخش اصلی امنیت مدیریتی، امنیت فیزیکی و امنیت فنی تقسیم می‌شود (جدول ۱). بخش «مکانیسم‌های امنیتی مدیریتی» شامل نه استاندارد کلی همراه با جزییات فرعی است. در این مکانیسم، موارد: تحلیل خطر (Risk analysis)، مدیریت خطر (Risk management)، خط‌مشی مجازات (Sanction policy)، بررسی فعالیت‌های سیستم اطلاعات (Information system activity review)، طرح پشتیبان داده‌ها (Data backup plan)، طرح بهبودی سانحه (Disaster recovery plan) (۱۰، ۱۱) و طرح عملیات شیوه‌ی اورژانسی (حفاظت از اطلاعات

الکترونیکی بهداشتی در یک وضعیت بحرانی یا Emergency mode operationplan) از موارد الزامی محسوب می‌شود (۱۱، ۱۰). در بخش «مکانیسم‌های امنیتی فیزیکی» چهار استاندارد کلی همراه با جزییات فرعی وجود دارد که از جمله موارد الزامی آن می‌توان به استفاده‌ی مجدد از رسانه‌ها (Media reuse) و منهدم کردن (Disposal) اشاره نمود. بخش «مکانیسم امنیت فنی» دارای پنج استاندارد است. در این قسمت موارد: شناسایی کاربر واحد (Unique use identification) و یکپارچگی (Integrity) و رویه‌ی دسترسی اورژانسی (Emergency access procedure)، الزامی می‌باشد. غیر از موارد الزامی مابقی را موارد آدرس‌پذیر (Addressable) می‌نامند (۱۱، ۱۰). Kline و همکاران پس از اجرای قانون امنیتی HIPAA در بخش اورژانس، ورود داده‌ها را توسط کارمندان با استفاده از سیستم‌های تحت شبکه بررسی نمودند و اعلام داشتند که جمع‌آوری اطلاعات بیماران ریوی در بخش اورژانس توسط تکنسین‌ها و با کامپیوتر شخصی که هر کدام از صفحات اطلاعاتی‌شان از قانون امنیتی تبعیت می‌کرد و اطلاعات حفاظت شده فقط در دسترس افراد مجاز قرار می‌گرفت، با صحت کامل انجام پذیرفت (۱۲). Kiel در نتیجه‌ی تحقیق خود به این نکته اشاره دارد که در ابتدا بسیاری از مدیران مراقبت سلامت، اجرای قانون HIPAA را بسیار هزینه‌بر و زمان‌بر می‌دانستند. اما امروزه چند سال پس از اجرای قانون HIPAA، مدیران مراقبت سلامت، این قانون را به عنوان یک استاندارد هزینه‌ی کارا و قابل مدیریت می‌شناسند (۱۳). تحقیقات در کشور ما نشان می‌دهد که نبود زیرساخت‌های فنی و اجرایی امنیتی مناسب و عدم انجام اقدام مؤثر در خصوص ایمن‌سازی فضای تبادل اطلاعات در بعضی مؤسسات موجب گردیده است که وضعیت امنیت تبادل اطلاعات کشور در سطح مطلوب قرار نگیرد (۷). همچنین بخش‌های بیمارستانی نیز از استانداردهای مربوط به امنیت و محرمانگی فاصله و انحراف دارد و کشور ما فاقد الزامات امنیتی پرونده‌ی الکترونیک سلامت می‌باشد (۴). با توجه به رویکرد کشورمان به سمت طراحی و ایجاد سیستم‌های اطلاعات بیمارستانی و پرونده‌ی الکترونیک سلامت و لزوم وجود مکانیسم‌های حفاظتی، بررسی وضعیت موجود از اهمیت خاصی برخوردار است. در مقاله‌ی حاضر، نتیجه‌ی بررسی مکانیسم‌های حفاظتی استانداردهای امنیتی HIPAA در بیمارستان‌های آموزشی دانشگاه علوم پزشکی شیراز ارایه و مورد بحث قرار گرفته است. امید است که ارایه‌ی نتایج این تحقیق گامی در جهت ارتقای سیستم امنیتی اطلاعات بیمارستانی باشد.

روش بررسی

پژوهش از نوع توصیفی- مقطعی است که در سال ۱۳۸۹ انجام شد. جامعه‌ی پژوهش شامل کلیه‌ی بیمارستان‌های آموزشی دانشگاه علوم پزشکی شیراز مجهز به سیستم اطلاعات بیمارستانی در زمان انجام تحقیق بود. این مراکز عبارت از بیمارستان‌های نمازی، حافظ، شهید چمران و شهید فقیهی می‌باشد. سایر بیمارستان‌های آموزشی دانشگاه علوم پزشکی شیراز به دلیل مجهز نبودن به سیستم اطلاعات بیمارستانی در زمان انجام تحقیق، حذف گردیدند. ابزار جمع‌آوری داده‌ها چک‌لیست است که توسط محققین و بر اساس قانون استاندارد امنیتی HIPAA می‌باشد (۱۵، ۱۴، ۱۱، ۱۰، ۳) و مشتمل بر سه بخش کلی مکانیسم‌های امنیت مدیریتی، مکانیسم‌های امنیت فیزیکی و مکانیسم‌های امنیت فنی، با ۴۵ مورد تهیه گردید (جدول ۱). روایی چک‌لیست از طریق روایی محتوا تعیین شد. ضمن مصاحبه و پرسش موارد موجود در چک‌لیست (در قالب وجود (اعمال و یا عدم اعمال) و عدم وجود موارد)، از مسؤولین فن‌آوری مراکز مورد مطالعه و درج همزمان پاسخ آنان، اطلاعات گردآوری شد. تحلیل داده‌های جمع‌آوری شده با استفاده از آمار توصیفی انجام گردید.

یافته‌ها

یافته‌ها در ارتباط با "اعمال مکانیسم‌های امنیتی مدیریتی ..." نشان داد که «فعالیت مدیریت امنیت»، «مدیریت خطر»، «تصدیق یا نظارت» و «طرح پشتیبان داده‌ها» به طور کامل در تمامی بیمارستان‌ها اعمال می‌شد. موارد «پاسخ‌گویی

جدول ۱: عناوین مکانیسم‌های امنیتی (مدیریتی، فیزیکی و فنی) هیپا

شماره	مکانیسم‌های امنیتی / Security safeguards
	موارد الزامی هر مکانیسم highlight شده است
	I- مکانیسم‌های حفاظتی مدیریتی
۱	**فعالیت مدیریت امنیت / Security management function**
۲	تحلیل خطر / Risk analysis
۳	مدیریت خطر / Risk management
۴	خط‌مشی مجازات / Sanction policy
۵	بررسی فعالیت‌های سیستم اطلاعات / Information system activity review
۶	**پاسخ‌گویی امنیتی / Assigned security responsibility**
۷	**امنیت نیروی کار / Workforce security**
۸	تصدیق یا نظارت / Authorization and/or supervision
۹	اقدام تعیین صلاحیت نیروی کار / Workforce clearance procedures
۱۰	رویه‌های خاتمه / Termination procedures
۱۱	**مدیریت دسترسی به اطلاعات / Information access management**
۱۲	تصدیق دسترسی / Access authorization
۱۳	**آگاهی و آموزش امنیت / Security awareness and training**
۱۴	**گزارش‌دهی واقعه‌ی امنیتی / Security incident procedures**
۱۵	**طرح احتمالی / Contingency plan**
۱۶	طرح پشتیبان داده‌ها / Data backup plan
۱۷	طرح بهبودی سانحه / Disaster recovery plan
۱۸	طرح عملیات شیوه‌ی اورژانسی / Emergency mode operation plan
۱۹	آزمایش و تجدید نظر رویه‌ها / Testing and revision procedures
۲۰	تحلیل وخامت برنامه‌های کاربردی و داده‌ها / Application and data criticality analysis
۲۱	**ارزیابی / Evaluation**
۲۲	**قراردادها و سایر توافقات مشترک تجاری / Business Associate Contracts**
	II- مکانیسم‌های حفاظتی فیزیکی
۲۳	**کنترل دسترسی مؤسسه / Facility Access Control**
۲۴	عملیات احتمالی / Contingency operations
۲۵	طرح امنیت مؤسسه / Facility security plan
۲۶	کنترل و تصدیق دسترسی / Access control and validation
۲۷	نگه‌داری اسناد / Maintenance records
۲۸	**استفاده از ایستگاه کاری / Workstation use**
۲۹	**امنیت ایستگاه کاری / Workstation security**
۳۰	**کنترل ابزار و رسانه‌ها / Device and media control**
۳۱	منهدم کردن / Disposal
۳۲	استفاده‌ی مجدد از رسانه‌ها /Media re use
۳۳	مسؤولیت‌پذیری / Accountability
۳۴	نسخه پشتیبان و ذخیره سازی داده ها / Data backup and storage
۳۵	**کنترل دسترسی / Access control**
۳۶	شناسایی کاربر واحد / Unique user identification
۳۷	رویه‌ی دسترسی اورژانسی / Emergency access procedures
۳۸	خروج خودکار /Automatic logoff
۳۹	رمزنگاری و رمزگشایی / Encryption and decryption
۴۰	**کنترل‌های ممیزی / Audit controls.**
۴۱	**یکپارچگی / Integrity**
۴۲	**تصدیق شخص یا موجودیت / Person or entity authentication**
۴۳	**امنیت انتقال / Transmission security**
۴۴	**کنترل یک‌پارچگی / Integrity control**
۴۵	**رمزنگاری / Encryption**

اقتباس از منابع (۱۵، ۱۴، ۱۱، ۱۰، ۳)

امنیتی معین»، «امنیت نیروی کار»، «اقدام تعیین صلاحیت نیروی کار» و «گزارش‌دهی واقعه‌ی امنیتی» در سه بیمارستان اعمال می‌شد. «بررسی فعالیت‌های سیستم اطلاعات» تنها در یک بیمارستان وجود داشته است، ولی اعمال نمی‌شد. «تحلیل خطر»، «آگاهی و آموزش امنیتی»، «طرح بهبودی سانحه»، «طرح عملیات شیوه‌ی اورژانسی» و «آزمایش تجدید نظر رویه‌ها»، «تحلیل وخامت برنامه‌های کاربردی و داده‌ها» و «ارزیابی» در دو بیمارستان اعمال می‌شد. «خط‌مشی مجازات» و «رویه‌های خاتمه» و «قراردادها و سایر توافقات مشترک تجاری» در هیچ یک از بیمارستان‌ها وجود نداشت. از موارد مکانیسم امنیتی مدیریتی الزامی تنها «مدیریت خطر» در تمام بیمارستان‌ها اعمال می‌شد «بررسی فعالیت‌های سیستم اطلاعات» و «طرح پشتیبان داده‌ها» در سه بیمارستان و «تحلیل خطر»، «طرح بهبودی سانحه» و «طرح عملیات شیوه‌ی اورژانسی» در دو بیمارستان اعمال می‌گردید. «خط‌مشی مجازات» در هیچ یک از بیمارستان‌ها وجود نداشت. در میان بیمارستان‌های تحت مطالعه، بیمارستان چمران بیشترین میزان اعمال مکانیسم‌های امنیتی مدیریتی آدرس‌پذیر و الزامی را دارا بود (جدول ۲). در ارتباط با اعمال مکانیسم‌های حفاظتی فیزیکی، «نگه‌داری اسناد»، «استفاده از ایستگاه کاری» و «نسخه‌ی پشتیبان و ذخیره‌سازی داده‌ها» در تمام بیمارستان‌ها اعمال می‌شد. «کنترل‌های دسترسی سازمان»، «عملیات احتمالی» و «منهدم کردن» در سه بیمارستان اعمال می‌گردید. «طرح امنیت مؤسسه» در یک بیمارستان اعمال می‌شد. «استفاده‌ی مجدد از رسانه‌ها» و «مسؤولیت‌پذیری» در همه‌ی مراکز وجود داشته است، ولی در سه بیمارستان اعمال می‌شد. در میان بیمارستان‌های تحت مطالعه، بیمارستان حافظ بیشترین میزان اعمال مکانیسم‌های امنیتی فیزیکی را دارا بود. از موارد الزامی مکانیسم امنیتی فیزیکی «استفاده‌ی مجدد از رسانه‌ها» در تمام بیمارستان‌ها وجود داشته است و تنها در یک مورد از آن‌ها اعمال نمی‌گردید. «منهدم کردن» در سه بیمارستان وجود داشت و اعمال می‌شد (جدول ۳). در ارتباط با اعمال مکانیسم‌های امنیتی فنی، «شناسایی کاربر واحد» و «یکپارچگی» در تمام بیمارستان‌ها اعمال می‌شد. «رویه‌ی دسترسی اورژانسی»، «کنترل‌های ممیزی» و «تصدیق شخص یا موجودیت» در یک بیمارستان اعمال می‌گردید. «رویه‌ی دسترسی اورژانسی» و «خروج خودکار» و «رمزنگاری و رمزگشایی» در هیچ یک از بیمارستان‌ها وجود نداشت. در میان بیمارستان‌های تحت مطالعه بیمارستان‌های نمازی، شهید چمران و حافظ، مکانیسم‌های امنیتی فنی را اعمال می‌کردند. از موارد الزامی مکانیسم امنیتی فنی، «شناسایی کاربر واحد» و «یکپارچگی» در تمام بیمارستان‌ها اعمال و «رویه‌ی دسترسی اورژانسی» تنها در یکی از بیمارستان‌ها اعمال می‌گردید. در میان بیمارستان‌های تحت مطالعه، بیمارستان فقیهی بیشترین میزان اعمال مکانیسم‌های امنیتی فنی الزامی را دارا بود. در مجموع، در تمامی بیمارستان‌های تحت مطالعه به طور مشابه مکانیسم فیزیکی نسبت به سایر مکانیسم‌ها بیشتر رعایت شد و بالاترین درصد اعمال مکانیسم حفاظتی مدیریتی به ترتیب در دو بیمارستان شهید چمران و حافظ و بالاترین درصد اعمال مکانیسم حفاظتی فیزیکی در بیمارستان حافظ و درصد اعمال مکانیسم حفاظتی فنی در بیمارستان شهید چمران با پایین‌ترین میزان و در سه بیمارستان دیگر به طور مساوی و کمتر از نیمی از موارد به دست آمد (جدول ۴).

بحث

الف- مکانیسم‌های امنیتی مدیریتی

همان طور که یافته‌ها نشان می‌دهد، از جمله مکانیسم‌های امنیتی مدیریتی، موارد «مدیریت امنیت» و «مدیریت خطر» در همه‌ی بیمارستان‌های تحت مطالعه و «تحلیل خطر» و «بررسی فعالیت‌های سیستم اطلاعات» در نیمی از بیمارستان‌ها اعمال می‌شد و «خط‌مشی مجازات» در هیچ یک از بیمارستان‌ها وجود نداشت. فرزندی‌پور (به نقل از صدوقی و همکاران) بر انجام فعالیت‌هایی تحت عنوان مدیریت ایمنی در هر سازمان تأکید و آن را توصیه نموده است (۷) و به این نکته اشاره دارد که توجه به اهمیت و حساسیت اطلاعات الکترونیک در محیط درمانی یک امر

جدول ۲: توزیع فراوانی مطلق و نسبی اعمال مکانیسم‌های امنیتی مدیریتی الزامی استانداردهای امنیتی هیپا در بیمارستان‌های آموزشی دانشگاه علوم پزشکی شیراز ۱۳۸۹

	بیمارستان مورد مطالعه	نمازی			فقیهی			چمران			حافظ			جمع		جمع		جمع	
	معیارهای‌های امنیتی مدیریتی الزامی	وجود دارد		وجود ندارد	وجود دارد		وجود ندارد	وجود دارد		وجود ندارد	وجود دارد		وجود ندارد	تعداد موارد اعمال شده	درصد	تعدادموارد		تعداد موارد	
		اعمال می‌شود	اعمال نمی‌شود		اعمال می‌شود	اعمال نمی‌شود		اعمال می‌شود	اعمال نمی‌شود		اعمال می‌شود	اعمال نمی‌شود				اعمال نشده	درصد	وجود نداشته	درصد
۱	تحلیل خطر			✓			✓	✓		✓	✓			۲	۵۰	۰	۰	۲	۵۰
۲	مدیریت خطر	✓			✓			✓			✓			۴	۱۰۰	۰	۰	۰	۰
۳	خط‌مشی مجازات			✓			✓			✓			✓	۰	۰	۰	۰	۴	۱۰۰
۴	بررسی فعالیت‌های سیستم اطلاعات	✓					✓	✓			✓			۳	۷۵	۱	۲۵	۰	۰
۵	طرح پشتیبان داده‌ها	✓			✓			✓			✓			۴	۱۰۰	۰	۰	۰	۰
۶	طرح بهبودی سانحه			✓			✓	✓		✓	✓			۲	۵۰	۰	۰	۲	۵۰
۷	طرح عملیات شیوه‌ی اورژانسی			✓			✓	✓		✓	✓			۲	۵۰	۰	۰	۲	۵۰
جمع	تعداد	۳	۰	۴	۲	۰	۵	۶	۰	۱	۵	۱	۱						
	درصد	۴۲/۸۴	۰	۵۷/۱۲	۲۸/۵۶	۰	۷۱/۴	۸۵/۶۸	۰	۱۴/۲۸	۷۱/۴	۱۴/۲۸	۱۴/۲۸						

جدول ۳: توزیع فراوانی مطلق و نسبی اعمال مکانیسم‌های حفاظتی فیزیکی الزامی استانداردهای امنیتی هیپا در بیمارستان‌های آموزشی دانشگاه علوم پزشکی شیراز- ۱۳۸۹

	بیمارستان مورد مطالعه	نمازی			فقیهی			چمران			حافظ			جمع		جمع		جمع	
	معیارهای‌های امنیتی فیزیکی الزامی	وجود دارد		وجود ندارد	وجود دارد		وجود ندارد	وجود دارد		وجود ندارد	وجود دارد		وجود ندارد	تعداد موارد اعمال شده	درصد	تعدادموارد		تعداد موارد	
		اعمال می‌شود	اعمال نمی‌شود		اعمال می‌شود	اعمال نمی‌شود		اعمال می‌شود	اعمال نمی‌شود		اعمال می‌شود	اعمال نمی‌شود				اعمال نشده	درصد	وجود نداشته	درصد
۱	منهدم کردن			✓	✓			✓			✓			۳	۷۵	۰	۰	۱	۲۵
۲	استفاده‌ی مجدد از رسانه‌ها		✓		✓			✓			✓			۳	۷۵	۱	۲۵	۰	۰
جمع	تعداد	۰	۱	۱	۲	۰	۰	۲	۰	۰	۲	۰	۰						
	درصد	۰	۵۰	۵۰	۱۰۰	۰	۰	۱۰۰	۰	۰	۱۰۰	۰	۰						

جدول ۴: درصد اعمال مکانیسم‌های حفاظتی امنیتی HIPAA در بیمارستان‌های آموزشی دانشگاه علوم پزشکی شیراز ۱۳۸۹

	بیمارستان مورد مطالعه	نمازی	فقیهی	چمران	حافظ
	مکانیسم‌های امنیتی	درصد اعمال	درصد اعمال	درصد اعمال	درصد اعمال
۱	مدیریتی	۳۱/۵۶	۳۱/۵۶	۸۴/۱۶	۷۸/۹
۲	فیزیکی	۵۵	۶۶	۸۸	۹۹
۳	فنی	۴۲/۸	۴۲/۸	۲۸/۵	۴۲/۸

ضروری است. در گزارش دبیرخانه شورای اطلاع‌رسانی ایران نیز لزوم وجود زیر ساختار «مدیریت مخاطرات امنیتی» اشاره و بر این نکته تأکید دارد که وجود نظام تحلیل و مدیریت مخاطرات امنیتی، اثر بسزایی در ایمن‌سازی فضای تبادل اطلاعات خواهد داشت (۱۶). کمیسیون مشترک اعتباربخشی آمریکا نیز بر مسؤولیت مدیر بخش مدارک پزشکی در حفاظت از این اطلاعات تأکید دارد (۴). در همین راستا Wager و همکاران در ارتباط با قانون امنیتی HIPAA، می‌نویسند که بر طبق این قانون «یک ارزیابی صحیح و کامل از خطرات بالقوه و آسیب‌پذیر بودن محرمانگی، یکپارچگی و قابلیت دسترسی اطلاعات حفاظت شده باید انجام شود (تحلیل خطر) و معیارهای امنیتی که خطرات و آسیب‌پذیری را در یک سطح منطقی و مناسب کاهش دهد (مدیریت خطر)، باید به کار گرفته شود. همچنین می‌بایست رویه‌هایی برای بررسی منظم پرونده‌های فعالیت سیستم اطلاعات مانند گزارشات دسترسی، گزارشات ردیابی و رویداد امنیتی (بررسی فعالیت سیستم اطلاعات) به کار گرفته شود» (۱۱). شجریات معتقد است که «سطح دسترسی اطلاعات مورد نیاز در هنگام مطالعه یا هر نوع استفاده از پرونده مراعات نمی‌شود و فرایند رفع نقص برای ارایه‌ی اطلاعات به کمیته‌های بیمارستانی و همچنین سازمان‌های خارج از بیمارستان مثل نیروی انتظامی رعایت امنیت اطلاعات را خدشه‌دار می‌سازد» (۱۷). در مورد خط‌مشی مجازات، قوانین HIPAA نیز چنین آورده است که «بایستی مجازات مناسبی را در برابر اعضای نیروی کار که در مطابقت با خط‌مشی‌های رویه‌ی امنیتی موجودیت‌های تحت پوشش قصور کرده‌اند، به کار گرفته شود» (۱۱). مورد خط‌مشی مجازات که در هیچ یک از بیمارستان‌ها اعمال نمی‌شد، در حالی که HIPAA این موارد را الزامی می‌داند. فرزندی‌پور (صدوقی و همکاران) اظهار می‌دارد که «در کشورهای مورد مطالعه‌ی ایشان سخنی از افشای اطلاعات برای دادگاه‌ها توسط بخش خصوصی و اعمال جریمه برای افشای غیر مجاز اطلاعات سخنی به میان نیامده است» (۷). بر اساس یافته‌ها در نیمی از بیمارستان‌های مورد مطالعه «پاسخ‌گویی امنیتی» معین اعمال می‌شد. Wager و همکاران می‌نویسند که «پاسخ‌گوی امنیتی معین باید در بیمارستان‌ها وجود داشته باشد و اطلاعات حفاظت شده را ملزم به شناسایی اشخاص مسؤول برای نظارت بر توسعه‌ی خط‌مشی‌ها و رویه‌های امنیتی سازمان می‌کند» (۱۱). هر چند این مورد از موارد الزامی قانون امنیتی HIPAA نیست، ولی انتظار می‌رفت که درصد بالاتری از مراکز در این خصوص فعال باشند. بر اساس یافته‌ها «تصدیق یا نظارت» در همه‌ی بیمارستان‌ها اعمال می‌شد. Wager و همکاران بر طبق قانون HIPAA این گونه اظهار می‌دارند که «فرایندی برای تضمین آن که نیروی کاری که با اطلاعات الکترونیکی حفاظت شده کار می‌کند، تصدیق یا نظارت مناسب را داشته باشد، بایستی ایجاد شود» (۱۱). «امنیت نیروی کار» و «اقدام تعیین صلاحیت نیروی کار» در سه بیمارستان اعمال می‌شد. در خصوص امنیت نیروی کار فرزندی‌پور و همکاران (۴) و صدوقی و همکاران (۷) آورده‌اند که کشورهای کانادا، استرالیا و انگلیس دارای الزاماتی هستند که با امضای قرارداد حفظ محرمانگی اطلاعات توسط کارکنان به عنوان بخشی از شرایط اولیه‌ی استخدام تمامی کارکنان و کاربران ثالث سازمان تأکید دارند. در قانون امنیتی HIPAA نیز به این نکته اشاره شده است که «موجودیت‌های بیمه شده بایستی فرایندی برای تضمین آن که نیروی کاری که با اطلاعات الکترونیکی سلامت حفاظت

شده کار می‌کند، تصدیق یا نظارت مناسب را داشته باشد، ایجاد نماید. همچنین بایستی فرایندی برای تعیین این که کدام دسترسی برای هر عضو نیروی کار مناسب است، وجود داشته باشد» (۱۱). رویه‌ی خاتمه در هیچ یک از بیمارستان‌ها وجود نداشت، در حالی که در استاندارد HIPAA آمده است که «باید فرایندی برای خاتمه‌ی دسترسی به اطلاعات الکترونیکی حفاظت شده هنگامی که یک عضو نیروی کار مدت زمان زیادی وجود نداشته است و یا مسؤولیت‌هایش تغییر یافته، موجود باشد» (۱۱). «آگاهی و آموزش امنیتی» فقط در نیمی ار بیمارستان‌ها اعمال می‌شد. Young و کوک (فرزندی‌پور و همکاران) می‌نویسند که «مدیریت باید از طریق سرمایه‌گذاری در آموزش نیروی کار به کاهش احتمال خطر در سازمان کمک کند» (۴). «گزارش‌دهی واقعه» امنیتی در سه بیمارستان اعمال می‌شد. Wager و همکاران بر این نکته اشاره دارند که «موجودیت‌های بیمه شده باید خطمشی‌ها و رویه‌هایی برای مورد توجه قرار دادن وقایع امنیتی داشته باشند»، «طرح پشتیبان داده‌ها» در همه‌ی بیمارستان‌ها اعمال می‌شد و بر طبق قوانین HIPAA از موارد الزامی است (۱۱). «طرح بهبود سانحه»، «شیوه‌ی عملیات اورژانسی»، «آزمایش و تجدید نظر رویه‌ها» و «تحلیل وخامت برنامه‌های کاربردی داده‌ها» و «ارزیابی» در نیمی از بیمارستان‌ها اعمال می‌شد که طرح بهبود سانحه و عملیات شیوه‌ی اورژانسی از موارد الزامی است و باید در همه‌ی بیمارستان‌ها اعمال شود. Wager و همکاران با توجه به قانون HIPAA بر «آزمایش، ارزیابی و اصلاح دوره‌ای همه طرح‌های احتمالی و وخامت نسبی برنامه‌های کاربردی، در پاسخ به تغییراتی که ممکن است تا امنیت اطلاعات الکترونیکی محافظت شده را تحت تأثیر قرار دهد، تأکید دارد» (۱۱). «قراردادها و سایر توافقات تجاری» در هیچ یک از بیمارستان‌ها وجود نداشت، در حالی که فرزندی‌پور (به نقل از صدوقی و همکاران) در تحقیق خود به این نتیجه رسیده است که «در کشورهای استرالیا، کانادا و انگلیس الزاماتی در مورد ایمنی مدیریت ارتباطات و وجود توافقنامه‌ی رسمی بین سازمان و سایر مراکز برای تبادل الکترونیکی داده‌ها وجود دارد» (۷). Wager و همکاران نیز در این ارتباط می‌نویسند که بر طبق قانون HIPAA «می‌بایست توافق رسمی با انجمن‌های تجاری برای تبادل اطلاعات الکترونیکی محافظت شده طرح‌ریزی شود» (۱۱).

ب- مکانیسم‌های حفاظتی فیزیکی

بر اساس یافته‌ها «تسهیل کنترل دسترسی» و «طرح عملیات احتمالی» در سه بیمارستان و «طرح امنیت مؤسسه» در یک بیمارستان اعمال می‌شد. با توجه به اظهارات Wager و همکاران در قانون امنیتی HIPAA آمده است که «بایستی فرایندی برای اجازه‌ی دسترسی مؤسسات به حمایت و بازگرداندن داده‌های مفقود شده تحت طرح بهبود بلایا و طرح عملیات به شیوه‌ی اورژانسی (عملیات احتمالی) و همچنین فرایندی برای امن نگه‌داشتن مؤسسه و تجهیزات آن از دسترسی غیر مجاز، سرقت و دستکاری (امنیت مؤسسه) وجود داشته باشد» (۱۱). بدین ترتیب «طرح امنیت مؤسسه» در مراکز مورد بررسی نیاز به توجه بیشتر دارد. قضوی نیز بر این نکته تأکید دارد که در هر مؤسسه‌ی مراقبت بهداشتی خطمشی‌های امنیت اطلاعات می‌بایست آماده شود و به وضوح مسؤولیت تمامی کادر پزشکی و سازمانی در حفظ محرمانه‌ی اطلاعات بیماران را مشخص نماید (۱۸). حبیبی‌فرد معتقد است که باید اطلاعات بیماران بر اساس درجه‌ی محرمانگی به سه طبقه‌ی اطلاعات اداری، تشخیصی درمانی و مالی و در سه طبقه‌ی داخلی، محرمانه و سری تقسیم‌بندی شود و ضمن تعریف میزان دسترسی به هر طبقه، ساز و کارهایی جهت حفاظت از اطلاعات به اجرا درآید (۱۹). «استفاده از ایستگاه کاری» نیز در همه‌ی بیمارستان‌ها اعمال می‌شد. در قانون امنیتی HIPAA آمده است که باید خطمشی‌هایی وجود داشته باشد که وظایف یک ایستگاه کاری، شیوه‌های دسترسی به اطلاعات الکترونیکی محافظت شده و ویژگی فیزیکی ایستگاه‌های کاری را مشخص کند (۱۱). «منهدم کردن اطلاعات» در سه بیمارستان اعمال می‌شد. صدوقی و همکاران اظهار می‌دارند که «جهت امحای پرونده‌های پزشکی در کشورهای منتخب قوانینی وجود دارد» (۶). Wager و همکاران نیز می‌نویسند که «برای انهدام

اطلاعات الکترونیکی، سخت‌افزار و رسانه‌های الکترونیکی که در آن ذخیره شده است، فرایند مشخصی وجود داشته باشد» (۱۱). با توجه به این که این قانون از موارد الزامی هیپا است، باید در همه‌ی بیمارستان‌ها اعمال شود. «قوانین استفاده‌ی مجدد از رسانه‌ها»، «مسؤولیت‌پذیری» و «پشتیبانی و ذخیره‌سازی داده‌ها» در همه‌ی بیمارستان‌ها اعمال می‌شد. قانون امنیتی HIPAA نیز بر «وجود فرایندی برای حذف اطلاعات الکترونیکی از رسانه‌های الکترونیک قبل از استفاده‌ی مجدد از آن‌ها تأکید دارد. بایستی مدارکی از انتقال سخت‌افزار و رسانه‌های الکترونیک و هر نوع شخص مسؤول این اقلام نگه‌داری شود (مسؤولیت‌پذیری). همچنین باید یک کپی قابل بازیابی و کپی کامل از اطلاعات الکترونیکی برای هنگام نیاز قبل از انتقال تجهیزات تهیه شود (پشتیبانی و ذخیره‌سازی داده‌ها)» (۱۱).

ج- مکانیسم‌های حفاظتی فنی

در این خصوص مورد «شناسایی کاربر واحد» در همه‌ی بیمارستان‌ها اعمال می‌شد. این مورد از موارد الزامی است که در قانون امنیتی HIPAA در این ارتباط چنین آمده است که «اختصاص یک نام یا شماره‌ی واحد برای شناسایی و ردیابی هویت هر کاربر ضروری است» (۱۱). شجریات در ارتباط با مسایل امنیتی در زمینه‌های تصویربرداری از مستندات پرونده این گونه اظهار می‌دارد که تصویربرداری از اصل پرونده به دلیل عدم وجود دستگاه‌های کپی رعایت نمی‌گردد و سطح دسترسی اطلاعات مورد نیاز در هنگام مطالعه یا هر نوع استفاده از پرونده مراعات نمی‌شود و فرایند رفع نقص برای ارایه‌ی اطلاعات به کمیته‌های بیمارستانی جهت بررسی مواردی از قبیل مرگ و میر، عفونت و همچنین سازمان‌های خارج از بیمارستان مثل نیروی انتظامی، رعایت امنیت اطلاعات را خدشه‌دار می‌سازد (۱۷). «رویه‌ی دسترسی اورژانسی» تنها در یک بیمارستان اعمال می‌شد. Wager و همکاران با توجه به قانون امنیتی HIPAA بر لزوم ایجاد رویه‌هایی برای کسب اطلاعات الکترونیکی ضروری در یک وضعیت اورژانسی تأکید دارد (۱۱). با توجه به الزامی بودن «رویه‌ی دسترسی اورژانسی» بررسی‌های لازم جهت اجرای آن در بیمارستان‌ها ضروری است. «خروج خودکار» و «رمزنگاری و رمزگشایی» در هیچ یک از بیمارستان‌ها وجود نداشت، در حالی که قانون امنیتی HIPAA آمده است که «بایستی فرایندهای الکترونیکی که به یک نشست الکترونیک بعد از دوره‌ی زمانی از پیش تعیین شده عدم فعالیت خاتمه می‌دهد، به کار گرفته شود. همچنین باید مکانیسمی برای رمزنگاری و رمزگشایی اطلاعات الکترونیکی هنگام نیاز ایجاد شود» (۱۱). هر چند HIPAA این موارد را جزء موارد الزامی نمی‌داند، ولی اعمال آن موجب ارتقای سطح امنیتی مؤسسه خواهد شد. «کنترل ممیزی» در یکی از بیمارستان‌ها اعمال نمی‌شد. در قانون امنیتی HIPAA آمده است که «باید موجودیت‌های محافظت شده ملزم به کارگیری سخت‌افزار، نرم‌افزار و رویه‌هایی باشد که فعالیت در سیستم اطلاعاتی در بردارنده‌ی اطلاعات الکترونیکی را ثبت و بررسی نماید» (۱۱). با توجه به میزان اعمال این قانون در مراکز مورد بررسی، اعمال کنترل ممیزی و ثبت دقیق اطلاعات در بیمارستان‌ها امری لازم است. Wikham مدیران و صاحبان سیستم‌ها را مسؤول تعیین کنترل‌های اعمال شده برای دسترسی به اطلاعات در سیستم خود می‌داند. همچنین به این نکته اشاره می‌کند که دسترسی به سیستم‌ها و اطلاعات نیاز به دانستن و استفاده از پایه و بررسی منظم دارد. وی قوانین و مقررات ایزو را برای راه‌اندازی، نگهداری و کنترل دستیابی در سیستم پیشنهاد می‌کند (۲۰). «یکپارچگی» در هیچ یک از بیمارستان‌ها و «تصدیق شخص یا موجودیت» تنها در یک بیمارستان اعمال می‌شد. بر طبق قانون امنیتی HIPAA «باید رویه‌هایی برای تصدیق آن که یک شخص یا موجودیت تقاضا کننده دسترسی به اطلاعات الکترونیکی در حقیقت شخص یا موجودیت دعوی کننده است، به کار گرفته شود» (۱۱). این مورد از جمله موارد الزامی است و اعمال آن موجب ارتقای سطح امنیتی مؤسسه خواهد شد.

نتیجه‌گیری

با توجه به بررسی انجام شده در ارتباط با مکانیسم‌های حفاظتی مدیریتی به جز مورد «مدیریت خطر» که به طور

کامل در همه‌ی بیمارستان‌ها اعمال می‌شد و بقیه‌ی موارد نیاز به توجه دارد. از این رو برای مواردی از جمله تحلیل خطر، خط‌مشی مجازات، بررسی فعالیت‌های سیستم اطلاعات، طرح پشتیبان داده‌ها، طرح بهبودی سانحه و طرح عملیات شیوه‌ی اورژانسی باید برنامه‌ریزی شود و راه‌کارهایی جهت افزایش میزان اعمال آن‌ها در بیمارستان‌ها به کار گرفته شود. ایجاد برنامه‌ی مدون مدیریت خطر کارامد و برنامه‌ریزی جهت تحلیل خطرهایی که سیستم‌های اطلاعات بیمارستانی را تهدید می‌کند (شامل هشت گام: تعریف مرز، شناسایی تهدید، تعریف آسیب‌پذیری، تحلیل کنترل امنیت، تعیین احتمال خطر، تحلیل اثر، تعیین خطر و توصیه‌های کنترل امنیت) به عنوان اقداماتی لازم در ارتقای مکانیسم‌های حفاظتی مدیریتی سیستم‌های اطلاعات بیمارستانی می‌بایست مد نظر مسؤولین مربوط قرار گیرد. در خصوص مکانیسم‌های امنیتی فیزیکی الزامی، با وجودی که فاصله‌ی چندانی تا اجرای کامل آن در همه‌ی بیمارستان‌های تحت مطالعه وجود نداشت، بررسی‌های دوره‌ای جهت کنترل ابزار و رسانه‌ها، امنیت و استفاده از ایستگاه کاری و کنترل دسترسی می‌بایست در نظر گرفته شود. از مکانیسم‌های فنی الزامی، مورد "رویه‌ی دسترسی اورژانسی" نیاز به بررسی و برنامه‌ریزی جهت اجرای دقیق و کامل در کلیه‌ی مراکز وجود دارد.

به طور کلی انجام اقداماتی مانند بازرسی دوره‌ای از اطلاعات شبکه به منظور اطمینان از رعایت سیاست‌های امنیتی مربوط، پشتیبان‌گیری منظم و ایمن از اطلاعات و ذخیره‌ی داده‌های پشتیبان‌گیری شده در یک محیط به طور فیزیکی امن و خارج از جایگاه اصلی، به کارگیری نرم‌افزار و تمهیداتی که بتوان اطلاعاتی را که در یک حادثه یا رخداد از بین رفته است، بازگردانی کند، استفاده از دستورالعمل‌های مربوط به مدت زمان نگه‌داری داده‌های الکترونیکی و نحوه‌ی انهدام آن‌ها، به کارگیری فرایندی برای حذف اطلاعات از رسانه‌های الکترونیک پیش از آن که از رسانه‌ها استفاده‌ی مجدد شود، تعیین جرایم جنایی و مدنی برای انواع موارد افشای اطلاعات بیماران و عدم رعایت محرمانگی اطلاعات پرونده‌های پزشکی بیماران توسط یک مرجع ذی‌صلاح و به کارگیری رویه‌هایی برای کسب اطلاعات ضروری در یک وضعیت اورژانس مانند از بین بردن محدودیت دسترسی در یک وضعیت اورژانسی، جهت ارتقای وضعیت امنیتی سیستم‌های اطلاعات بیمارستانی و پرونده‌ی الکترونیکی بیمار توصیه می‌شود.

در انتها لازم است که از همکاری معاونت محترم پژوهشی دانشگاه علوم پزشکی شیراز و کارشناسان مربوط در اخذ مجوز و حمایت‌های لازم جهت جمع‌آوری اطلاعات و مسؤولین فن‌آوری اطلاعات دانشگاه و بیمارستان‌های مورد مطالعه تقدیر و تشکر گردد. مقاله‌ی حاضر حاصل پروژه‌ی دانشجویی خانم فاطمه ابراهیمی دانشجوی کارشناسی رشته‌ی مدارک پزشکی و عضو کمیته‌ی تحقیقات دانشجویی دانشکده‌ی مدیریت و اطلاع‌رسانی دانشگاه علوم پزشکی شیراز است.

References

1. Jantzen T. What is HIS [Online]. 2006; Available from: URL: http://www.crwr.utexas.edu/gis/gishydro06/GISandHIS/WhatIsHIS.htm/
2. Ahmadi M. Electronic Health Record, Structure, Content, and Evaluation. Tehran, Iran: Jafari Publication; 2008. [In Persian].
3. Huffman E. Electronic Medical Record. Trans. Langarizadeh M, Shahverdian N. Tehran, Iran: Dibagaran Publication; 2006.
4. Farzandipour M, Sadoughi F, Ahmadi M, Karimi I. Designing a Confidentiality Principles Model of Electronic Health Record for Iran 2007. J Health Adm 2008; 11(33): 33-46.
5. Torabi M, Safdari R. Electronic Medical Record. Tehran, Iran: Behineh Publication; 2004. [In Persian].
6. Sadoughi F, Khoshkam M, Behnam S. Acomparative investigation of the access levels and confidentiality of medical documents in Iran and selected countries. J Health Adm 2007; 10(28): 49-56. [In Persian].
7. Sadoughi F, Ahmadi M, Karimi I, Farzandipour M. Safety Requirements for Health Electronic File; Comparison between Selected Countries. Health Inf Manage 2007; 4(1): 1-10. [In Persian].

8. Hajavi A, Khoshgam 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. J Health Adm 2008; 11(33): 7-16.

9. University information technology services. What is electronic protected health information (ePHI) [Online]. 2009; Available from: URL: http://kb.iu.edu/data/ayyz.html/

10. Mastane Z, Ali Pour J. Health Care Information Systems. Bandar Abbas, Iran: Rasool Publication; 2010. [In Persian].

11. Wager KA, Lee FW, Glaser JP. ManagingHealth Care Information Systems: A Practical Approach for Health Care Executives. New Jersey, NJ: John Wiley & Sons; 2005.

12. Kline JA, Johnson CL, Webb WB, Runyon MS. Prospective study of clinician-entered research data in the Emergency Department using an Internet-based system after the HIPAA Privacy Rule. BMC Med Inform Decis Mak 2004; 4: 17.

13. Kiel JM. HIPAA: SOP: HIPAA as standard operating procedures. Health Care Manag (Frederick) 2010; 29(1): 80-2.

14. HIPAA. Complimentary Webcast: Exec Brief on the HIPAA Final Rule [Online]. 2009; Available from: URL: http://www.ecfirst.com/press/webcast_final_rule_feb2013.html/

15. HIPAA. Contingency Plan: Emergency Mode Operation Plan-What to Do and How to Do It [Online]. 2008; Available from: URL: http://www.hipaa.com/2009/04/contingency-plan-emergency-mode-operation-plan-what-to-do-and-how-to-do-it/. 2013.

16. Iranian Supreme Council of Information and Communication Technology report. Information Security System Management [Online]. 2007; Available from: URL: http://www.scict.ir/ [In Persian]

17. Shajariat Z. Study of the Medical Information Accessibility methods in Medical Record department. Proceedings of the 2nd Congress of Medical Record Students; 2006 Dec 23-24; Shiraz, Iran; 2006. [In Persian].

18. Ghazavi S. Health Information Systems Occupational Security. Proceedings of the 2nd Congress of Medical Record Students; 2006 Dec 23-24; Shiraz, Iran; 2006. [In Persian].

19. Habibifard V. Operational Model for Information Security System. Proceedings of the 1st Congress of IT Application in Health; 2011 Oct 19-20; Sari, Iran; 2011. [In Persian].

20. Wikham D. Information systems security policy. Information Governance [Online]. Available from: URL: http://www.ruh.nhs.uk/about/policies/documents/non_clinical_policies/black_infoman/Black_320_Information_Governance_Information_Security.pdf/.

Evaluating the Security Safeguards in Hospital Information Systemaccording to the Health Insurance Portability and Accountability Act of University Hospitals in Shiraz University of Medical Sciences*

Roxana Sharifian, PhD[1]; Mohtaram Nematollahi, PhD[2]; Hossein Monem[3]; Fatemeh Ebrahimi[4]

Original Article

Abstract

Introduction: One of the main characteristics of a hospital information system (HIS) is confidentiality. Studies have shown that the security requirements on electronic health records are not fully met in Iran. This study was conducted to determine the percentage of HIPAA (health insurance portability and accountability act) security safeguard application in university hospitals of Shiraz University of Medical Sciences in 2010.

Methods: This was a cross-sectional descriptive study. The study population included university hospitals of Shiraz University of Medical Sciences equipped with HIS. Data were collected by a checklist through interview with the IT authorities of the hospitals. The checklist was in accordance with HIPAA security standard rules. Tool validity was checked by the content validity method. Data were analyzed using descriptive statistics.

Results: The risk management and data backup plan, two out of seven required administrative security safeguards (i.e. risk analysis, risk management, sanction policy, information system activity review, data backup plan, disaster recovery plan, and emergency mode operation plan), were fully applied in all the hospitals. Both of two required physical security safeguards, disposal and media reuse, were applied in the majority of the hospitals. Of the two required technical security safeguards, unique user identifications, and emergency access procedure were applied only in one of the hospitals.

Conclusion: Operational planning must be implemented in order to increase the application of required administrative security safeguards. Full application of the required physical security safeguards, which are close to reach, and the required technical security safeguards could be the main steps in promoting security of the HIS.

Keywords: Health Insurance Portability and Accountability Act; Hospital Information System; Confidentiality

Received: 11 Jun, 2012 Accepted: 18 Feb, 2013

Citation: Sharifian R, Nematollahi M, Monem H, Ebrahimi F. **Evaluating the Security Safeguards in Hospital Information Systemaccording to the Health Insurance Portability and Accountability Act of University Hospitals in Shiraz University of Medical Sciences.** Health Inf Manage 2013; 10(1): ??

∗ This article derived from an MSc thesis.

1- Assistant Professor, Health Information Management, School of Management and Medical Information Sciences, Shiraz University of Medical Sciences, Shiraz, Iran (Corresponding Author) Email: sharifianr@sums.ac.ir
2- Assistant Professor, Health Information Management, School of Management and Medical Information Sciences, Shiraz University of Medical Sciences, Shiraz, Iran
3- PhD Student, School of Computer and Information System, University Technology Malaysia (UTM), KualaLumpur, Malaysia
4- Medical Records, Shiraz University of Medical Sciences, Shiraz, Iran