(مقاله پژوهشی)

ارائه مدل اطلاعاتی اولیه محرمانگی آرشیو الکترونیک پرونده پزشکی در بیمارستان

امیرعباس عزیزی[1]، سکینه بدوی [2]، سارا رشیدی[2]،
مرضیه باویر[2]، روژین براتی[2]، سحر زندی[2]، حدیث قاسمی [2]، احمد عزیزی[3*]

چکیده

زمینه و هدف: در سال‌های اخیر بیمارستان‌های سطح کشور جهت حل مسائل و مشکلات ذخیره و بازیابی پرونده پزشکی کاغذی اقدام به اسکن پرونده کاغذی با استفاده از سیستم آرشیو الکترونیک پرونده نموده‌اند. پیشرفت در فناوری های نوین امکان دسترسی کاربران غیرمجاز را فراهم می کند، لذا جهت ارتقاء محرمانگی اطلاعات بیمار، وجود قواعد و اصول حفاظت از داده ها لازم است. در این مطالعه قصد داریم با بررسی وضعیت محرمانگی سیستم آرشیو الکترونیک پرونده‌ی پزشکی بیماستان‌های شهر اهواز مدل اطلاعاتی اولیه در راستای ارتقاء محرمانگی اطلاعات ارائه دهیم.

روش بررسی: این پژوهش یک مطالعه توصیفی و از نوع مقطعی است که به بررسی وضعیت محرمانگی اطلاعات آرشیو پرونده پزشکی در بیمارستان های منتخب شهر اهواز درسال ۱۳۹۷ پرداخته است. جامعه پژوهش ۱۱ بیمارستان منتخب شهر اهواز می باشد. اطلاعات مورد نیاز از طریق چک لیست پژوهشگر ساخته که به صورت حضوری(مشاهده‌ای) در بخش های مدارک پزشکی و فناوری اطلاعات تکمیل شده است و برای تجزیه و تحلیل از نسخه‌ی اکسل ۲۰۱۶ استفاده شده است.

یافته‌ها: طبق مطالعه‌ی انجام شده علی رغم رعایت بسیاری از شاخص‌های امنیتی جهت حفظ محرمانگی اطلاعات، در تمامی مراکز تحت مطالعه به استثنای یک مورد، اخذ تعهدنامه‌ی کتبی جهت عدم افشای رمزعبور و نام کاربری افراد مورد توجه قرار نگرفته بود.

نتیجه‌گیری: با توجه به حساسیت اطلاعات سلامت توصیه می‌شود جهت بهبود حفظ محرمانگی، بیمارستان‌ها اقدام به طراحی فرم تعهدنامه‌ی کتبی نموده و پیش از دادن هرگونه حق دسترسی به اطلاعات، از مسئولین فناوری اطلاعات و مدارک پزشکی و کلیه‌ی کاربران، به اخذ آن عمل نمایند.

واژگان کلیدی: محرمانگی، امنیت، حریم خصوصی.

۱- استادیار گروه فناوری اطلاعات سلامت.
۲- کارشناس فناوری اطلاعات سلامت.
۳-مربی گروه فناوری اطلاعات سلامت.

۱و۲و۳-فناوری اطلاعات سلامت، دانشکده پیراپزشکی، دانشگاه علوم پزشکی جندی شاپور اهواز، اهواز، ایران.

* نویسنده مسئول:
احمد عزیزی؛ فناوری اطلاعات سلامت، دانشکده پیراپزشکی، دانشگاه علوم پزشکی جندی شاپور اهواز، اهواز، ایران.
تلفن: ۰۰۹۸۹۰۲۶۰۰۱۵۹۰
Email: azizimaster@gmail.com

دریافت مقاله: ۱۳۹۹/۱/۲۹ دریافت مقالهٔ اصلاح‌شده: ۱۳۹۹/۷/۲۰ اعلام قبولی: ۱۳۹۹/۷/۲۹

مقدمه

در سازمان‌های مراقبت، پرونده پزشکی بیمار منبع اصلی اطلاعات مراقبت بهداشتی و درمانی است (۱). پرونده پزشکی بیمار شامل اطلاعاتی برای شناسایی بیمار و توجیهی برای تشخیص، درمان و ثبت نتایج حاصل از آن است(۲)؛ بنابراین یکی از اصلی‌ترین محورها و موضوعات پزشکی حفظ محرمانگی اطلاعات مندرج در آن است (۳, ۴). در جامعه اطلاعاتی امروز، گردآوری، ذخیره و پردازش حجم زیادی از داده‌های شخصی که به شکل معنادار و مفیدی تعیین و تبیین شده‌اند اطلاعات نامیده می‌شوند (۵, ۶). اطلاعات همچون سایر دارایی‌های سازمان و به عنوان جزئی از سرمایه‌های سازمانی از اهمیت ویژه‌ای برخوردار هستند (۷). امروزه در عصر اطلاعاتی، در ایجاد ارزش افزوده هیچ عاملی قادر به رقابت با اطلاعات نیست (۳). در باب ارزش و اهمیت اطلاعات در جهان کنونی همین قدر کافی است که بتوان گفت نیمی از ارزش افزوده حاصله در ژاپن و ایالت متحده منشا اطلاعاتی دارد (۳).

کمبود فضای بایگانی (۸)، کاهش عمر مفید فرم‌های کاغذی به دلیل شرایط نگهداری نامناسب و افزایش خطر آسیب ناشی از عوامل طبیعی (۹) و از طرف دیگر افزایش روزافزون تولید اطلاعات بهداشتی موجب به کارگیری فن آوری‌های نوین برای بهره برداری مناسب از این اطلاعات در حوزه بهداشتی و درمانی شده است (۱۰). به دنبال این عوامل، در سال‌های اخیر بیمارستان‌های سطح کشور جهت حل مسائل و مشکلات ذخیره و بازیابی پرونده پزشکی کاغذی اقدام به اسکن پرونده کاغذی با استفاده از سیستم آرشیو الکترونیک پرونده نموده‌اند(۱۱). استفاده از تکنولوژی اطلاعات و ارتباطات موجب شده که سرعت و فعالیت‌های دسترسی به اطلاعات، روندی صعودی داشته باشد (۱۲). بسیاری از این اطلاعات دارای ماهیت حساسی هستند(۳). بی‌تردید پرونده پزشکی یکی از مهم‌ترین مدارک و حاوی حساس‌ترین اطلاعات پزشکی افراد می‌باشد(۳, ۱۳). اطلاعات موجود در پرونده پزشکی، باعث تداوم مراقبت بیمار می‌شود و موارد قانونی و اخلاقی مهمی را احاطه کرده‌است (۷).

پیشرفت در فناوری های نوین امکان دسترسی کاربران غیرمجاز را فراهم می کند، این امر می‌تواند امنیت و محرمانگی اطلاعات را به مخاطره بیندازد که در این صورت زمینه ایجاد مشکلات و تبعات را برای مشتریان سلامت فراهم می‌کند و نارضایتی بیماران را به همراه خواهد داشت (۱۰).

از آنجاییکه سرنوشت یک سازمان به سطوح فناوری اطلاعات و حفاظت از اطلاعات آن وابسته است بنابراین حافظت از این سیستم‌های اطلاعاتی در برابر تهدیدات داخلی و خارجی که مسئله امنیت داده‌ها را خدشه‌دار می کند مطرح می‌شود(۱۴) و در هر پروژه‌ای که نیازمند ذخیره‌سازی یا دستکاری اطلاعات شخصی حساس باشد، به وجود می‌آید (۱۵).

امنیت اطلاعات به عنوان بخشی از اصول سه گانه محرمانگی، یکپارچگی و قابلیت دسترسی(۱۶)، یک اصل مهم در اخلاق و فعالیت‌های موثر پزشکی است، که توجه به محرمانه‌سازی اطلاعات بیمار در آن باید حفظ شود. این مسئله، موضوع محرمانگی و حریم خصوصی بیمار را تضمین می‌کند(۷) و از اولویت بالایی برخورداراست (۳).

محرمانگی حق مسلم و اختیار تام در خصوص کنترل نحوه جمع‌آوری، استفاده و بهره‌گیری از اطلاعات سلامت منحصر به فرد اشخاص است که بعد محرمانه بودن اطلاعات بهداشتی را شامل می‌شود (۳). گستره محرمانگی بسیار وسیع است و فرم‌های کتبی یا رایانه‌ای و اطلاعات شفاهی بیمار را در بر می‌گیرد (۱۷).

تعریف سطوح دسترسی به اطلاعات، تدوین مصوباتی در مورد چگونگی افشا آن‌ها و این‌که چه اطلاعاتی، تا چه اندازه‌ای، در چه زمانی و در چه مکانی باید در اختیار چه‌کسی و با چه سطح اختیاراتی گذاشته شود، همگی از جمله مسائلی هستند که مدیران کلیه

بیمارستان‌ها و مراکز بهداشتی درمانی را در سطح خرد و کلان با چالش‌هایی روبرو ساخته‌است (۳).

در مطالعه‌ی صدوقی و همکارانش در ارتباط با مقایسه‌ی سطوح دسترسی و محرمانگی مدارک پزشکی در کشورهای منتخب و ایران این گونه بیان شده است که وضعیت مدارک پزشکی، محرمانه سازی و سطوح دسترسی به آن در ایران، بسیار دور از استانداردهای جهانی است و سازمانی که متولی مدیریت بحث محرمانگی مدارک پزشکی در ایران باشد وجود ندارد. همچنین عدم تطابق عملکرد بخش مدارک پزشکی بیمارستان های ایران با فعالیت‌های استاندارد تعریف شده در کشورهای پیشرفته و روش‌های نامطلوب انجام کار، موجب انحراف فعالیت-های این بخش از اهداف اصلی خود می‌شود(۳)

حال با توجه به این چالش‌ها و با در نظر گرفتن نقش‌های بخش مدیریت اطلاعات سلامت در پایش و ارائه قوانین جهت تسهیل اقدامات محرمانه‌سازی، امنیت و افشا اطلاعات(۷)؛ ارائه قوانین جامع و کنترل های دسترسی باید در محیط‌های اطلاعات سلامت به قدر کافی فراهم شود(۱۵) بنابراین برای حفظ محرمانگی اطلاعات بیمار، تصویب قوانین حفاظت از داده‌ها لازم است (۱۸).

عرب و همکارانش در مطالعه‌ای پیشنهاد کردند که جهت حفظ محرمانگی و محدود نمودن سطوح دسترسی به اطلاعات بیماران، اقداماتی همچون؛ تصویب قوانین و ضوابط روشن و مشخصی پیرامون نحوه‌ی دسترسی به اطلاعات پرونده‌ی پزشکی بیمار توسط مراجع عالی در کشور صورت بگیرد(۱۹).

در این مطالعه قصد داریم وضعیت محرمانگی پرونده‌ی پزشکی را در بیماستان‌هایی از شهر اهواز که دارای قابلیت اسکن هستند مورد بررسی قرار دهیم تا مدل اولیه اطلاعاتی در جهت حفظ محرمانگی اطلاعات و ارتقای آن ارائه دهیم. در بیمارستان‌های مورد مطالعه از دو مدل یکپارچگی اطلاعات و سه نوع نرم افزار جهت اسکن استفاده می نمایند. برخی از این نرم افزارها با سیستم اطلاعات بیمارستانی لینک و یکپارچه می باشند و برخی مستقل از سیستم اطلاعات بیمارستان عمل می‌کنند که به منظور جلوگیری از کپی غیرقانونی از قفل سخت افزاری بهره می برند.

روش بررسی

پژوهش حاضر مطالعه‌ی توصیفی_مقطعی است که به بررسی وضعیت محرمانگی اطلاعات پرونده‌ی پزشکی در مرحله‌ی اسکن و پس از آن پرداخته است تا بتواند مدل اطلاعاتی اولیه مناسب جهت حفظ محرمانگی اطلاعات در آرشیو پرونده‌ی الکترونیک پزشکی در سطح کشور ارائه دهد. این مطالعه در سال ۱۳۹۷ انجام گردید. جامعه‌ی مورد مطالعه شامل ۱۱ بیمارستان دانشگاهی، خصوصی و یک بیمارستان وابسته به کمیته امداد امام خمینی(ره) شهر اهواز بود که فرایند اسکن پرونده‌های پزشکی سرپایی و بستری را انجام داده بودند و پرونده‌های جاری را نیز اسکن می-نمودند و به دلیل بررسی کل جامعه، نمونه‌گیری انجام نشد. ابزار مورد استفاده چک لیست پژوهشگر ساخته شامل ۳۱ سوال با پاسخ بله و خیر و همچنین قسمت ملاحظات جهت درج توضیحات تکمیلی به منظور کسب اطلاعات دقیق‌تر بود. این چک لیست در ۶ بخش با محتوای بررسی نحوه اختصاص رمز عبور به کاربران بیمارستانی، دسترسی به اطلاعات، وضعیت رمزگذاری اطلاعات اسکن شده، پیشگیری از عوامل مخرب بر اطلاعات، پشتیبانی از اطلاعات اسکن شده و مدیریت امنیت اطلاعات تدوین شد.

روایی چک لیست توسط دو نفر متخصص موضوع مربوطه، شامل یک نفر کارشناسی ارشد آموزش مدارک پزشکی، و یک نفر دکتری تخصصی انفورماتیک پزشکی با برگزاری جلسات متعددی تایید شده است و تیم تحقیقات را به منظور داشتن درک یکسان از مفاهیم پرسش ها و اخذ پاسخ مطمئن توجیه نمودند.

جمع‌آوری داده‌ها به روش مشاهده_مصاحبه توسط پژوهشگران انجام شد. در اکثر موارد چک لیست هر بیمارستان به صورت ترکیبی تکمیل شد به این معنا که هر

بخش از پرسش ها توسط مسئول ذیربط پاسخ داده شد؛ همچنین اطلاعات هویتی هر فرد مصاحبه شونده، اطلاعات شناسایی بیمارستان و اطلاعات نرم افزارهای مورد استفاده در ابتدای چک لیست ثبت شد. در پایان، داده‌ها با یک روش ترکیبی تجمیع شد تا از هر بیمارستان برآیند کامل به دست آید و از طریق نسخه‌ی اکسل ۲۰۱۶ مورد آنالیز توصیفی قرار گرفتند و فراوانی در قالب جداول محاسبه گردید. در پایان با جمع بندی اطلاعات به دست آمده، پیش نویس الگوی امنیتی حفظ و نگهداری اطلاعات پزشکی پرونده های بیماران تهیه گردید. پس از نظرسنجی و تعیین دیدگاه متخصصین امنیت اطلاعات، مدل اطلاعاتی اولیه در سطح استان تهیه گردید تا متعاقب آن، مدل اطلاعاتی نهایی و در نهایت، الگوی ملی تهیه شود و بیمارستان‌ها بتوانند از آن در قالبی استاندارد استفاده نمایند.

یافته ها

یافته‌های مطالعاتی در یازده بیمارستان شهر اهواز نشان داد که بیش از نیمی از افراد شرکت کننده در مطالعه مونث بودند که در دو حیطه مدارک پزشکی و فناوری اطلاعات تخصص و فعالیت داشتند. حداکثر تعداد شرکت کنندگان در رده‌ی سنی سی تا چهل و تعداد کمی در رده سنی بالای پنجاه سال بود.

در بخش شاخص‌های مربوط به تاییدیه ورود اطلاعات (نحوه اختصاص نام کاربری و رمز عبور به کاربران) اکثریت بیمارستان‌های تحت مطالعه در مورد معرفی کاربران به واحد فناوری اطلاعات قبل از اشتغال در واحد، اختصاص نام کاربری و رمز عبور منحصر به فرد عملکرد مشابه و یکسانی داشتند و رعایت این موارد، برای هر کاربر انجام می‌شد. در بخش فوق آموزش آشنایی کاربران با ویژگی‌های محرمانگی نرم افزار سیستم اطلاعاتی بیمارستان به‌طور کامل مراعات می شد. تنها در یک بیمارستان آیتم مربوط به تعهدنامه کتبی عدم در اختیار قرار دادن نام کاربری و رمز عبور یک کاربر به سایر کاربران رعایت می‌شد. در مطالعه انجام شده تنها در هفت بیمارستان رمز عبور کاربران به صورت دوره‌ای تغییر می-کرد.

بر اساس یافته‌های موجود تمامی بیمارستان‌های تحت مطالعه، دسترسی به اطلاعات اسکن شده برای هر کاربر، سطح دسترسی تعریف شده بر اساس ماهیت شغلی و مسئولیت هر کاربر معیار تعیین سطح دسترسی قرارگرفته بود. امکان ابطال حق دسترسی در زمان مورد نیاز (نظیر مرخصی، ماموریت آموزشی و دوره بازنشستگی) در تمامی بیمارستان‌ها رعایت می‌شد. سایر یافته‌ها در این بخش حاکی از آن است که اکثریت بیمارستان‌های مورد مطالعه، استفاده از سیستم Log را جهت ردگیری دسترسی به اطلاعات تایید نموده اند. این در حالی است که در هفت بیمارستان، بازبینی دوره‌ای و منظم از سیستم Log صورت می‌گرفت.

وضعیت رمزگذاری اطلاعات اسکن شده به گونه‌ای بود که تنها سه بیمارستان از بیمارستان‌های تحت مطالعه، رعایت می‌نمودند.

به منظور پیشگیری از عوامل مخرب بر اطلاعات، تمامی بیمارستان‌ها از نرم افزارهای امنیت شبکه برای اقدامات حفاظتی نظیر آنتی ویروس‌ها و فایروال‌ها استفاده می‌کردند که بروزرسانی این نرم‌افزارها به صورت دوره‌ای و منظم انجام می‌شد.

در سه بیمارستان، امکان ویرایش فرم‌های اسکن شده و اتصال حافظه‌های جانبی به رایانه‌های حاوی اطلاعات سلامت افراد وجود داشت. همین تعداد بیمارستان از سخت افزارهای سالم جهت جلوگیری از آلوده شدن آن‌ها نسبت به بدافزارها استفاده نمی‌کردند.

در بخش پشتیبانی از داده‌های اسکن شده، کلیه بیمارستان‌ها در ارتباط با تهیه‌ی نسخه پشتیبان عملکرد مشابهی داشتند در حالی که شش بیمارستان این اطلاعات ذخیره شده را در محلی خارج از اتاق سرور نیز نگهداری می نمودند.

در بخش مدیریت امنیت اطلاعات اکثریت بیمارستان‌ها استفاده از مکانیسم‌های حفاظتی مناسب برای

ایمنی اطلاعات بیماران خاص (مانند بیماران مبتلا به ایدز یا بیماران روانی) را رعایت ننموده و ساز و کار مشخصی برای موارد بیماری‌ها خاص در اختیار نداشتند. یافته‌ها نشانگر آن است که در هشت بیمارستان از بیمارستان‌های تحت مطالعه فردی را به عنوان مسئول پاسخگویی و رعایت مقررات مربوط به سطوح دسترسی و محرمانگی پرونده‌ی پزشکی تعیین شده است. در هفت بیمارستان آیتم‌های عدم اتصال شبکه‌ی حاوی سیستم اطلاعاتی به اینترنت و یکپارچه بودن آرشیو الکترونیکی پرونده‌ی پزشکی با سیستم اطلاعات بیمارستان رعایت گردیده این درحالی است که در نه بیمارستان مورد مطالعه آیین نامه یکپارچه سازی اطلاعات اسکن شده با سیستم اطلاعات بیمارستان وجود نداشت. در اکثریت بیمارستان‌های مورد مطالعه جهت اطمینان از نوع علکرد (صحت اسکن) رعایت نظارت بر انجام تست‌هایی بصورت تصادفی صورت می-گرفت. تهیه‌ی آیین‌نامه‌ی واگذاری و به کارگیری اطلاعات اسکن شده به کاربران داخلی و خارجی به ترتیب در شش وهفت بیمارستان وجود داشته است. در هشت بیمارستان مورد مطالعه تعهد نامه‌ای در مورد نحوه‌ی واگذاری اطلاعات اسکن شده‌ی بیمارستان درخصوص افشای غیر مجاز اطلاعات اسکن شده وجود نداشت. در ارتباط با تهیه‌ی آیین‌نامه و برنامه اجرایی مدیریت بحران امنیتی در مواقع اضطراری در راستای مدیریت بحران تعداد بیمارستان‌ها در حداقل تعداد خود (پنج بیمارستان) و تهیه-ی آیین‌نامه‌ی مدیریت ریسک (خطر) امنیتی در شش بیمارستان صورت می‌گرفته است.

بحث

این مطالعه نشان داد کارکنان تمامی بیمارستان ها قبل از شروع به کار با قوانین مربوط به محرمانگی نرم افزار سیستم اطلاعاتی آشنا می‌شوند که این مطلب همسو با پژوهش زاهدی‌فر می‌باشد که بیان داشت در تمامی واحدهای مورد مطالعه پرسنل مدارک پزشکی قبل از شروع به کار با وظایف و مسئولیت‌های خود در ارتباط با رازداری و محرمانگی اطلاعات بیماران آشنا می‌شدند(۲۰). در پژوهشی نیز عنوان شده که نیازهای سازمان خدمات درمانی در قبال مسئولیت محرمانگی با سایر مشاغل تفاوت دارد و شاغلین مدیریت اطلاعات بهداشتی بنابر خاصیت آموزش‌ها و تجاربی که دارند بسیاری از مهارت ها را دارا می‌باشند. آموزش کاربران آن‌ها را از اهمیت حفظ محرمانگی آگاه می‌کند و باعث می‌شود که کاربران مسئولیت پذیری بیشتری در حین کار با اطلاعات اسکن شده از خود نشان دهند(۲۱). در همه‌ی بیمارستان‌های مورد مطالعه شناسه کاربری و رمز عبور مجزا برای همه‌ی کاربران در نظر گرفته می‌شد که در این راستا شیخ ابومسعودی و همکاران نیز بیان داشتند که هر کاربر دارای شناسه کاربری و رمز عبور مجزا بوده و از دسترسی افراد ناشناس جلوگیری می‌شود.

طبق نتایج این پژوهش، در تمامی بیمارستان‌های مورد مطالعه برای هر کاربر بر اساس ماهیت شغلی و مسئولیت کاربر حق دسترسی تعیین می‌شود که این نتایج با نتایج پژوهش شیخ ابومسعودی و همکاران مطابقت دارد. آنها نیز در این زمینه به این نتیجه رسیدند که سطح دسترسی کاربران با توجه به حیطه‌ی کاری آنها می‌باشد. همخوانی سطح دسترسی با ماهیت شغلی موجب جلوگیری از افشای اطلاعات برای افراد فاقد صلاحیت می‌شود (۲۲).

با توجه به اینکه بیشتر بیمارستان ها اطلاعات اسکن شده را رمزگذاری نمی‌کردند، عدم رمزگذاری اطلاعات اسکن شده می تواند سوء استفاده‌ی افراد غیرمجاز از اطلاعات پزشکی را موجب شود. بنابراین وجود الزامی جهت رمزگذاری اطلاعات می‌تواند تضمینی برای محرمانگی باشد تا در صورت دسترسی افراد غیرمجاز قادر به رمزگشایی و خواندن آن ها نباشند.

در این مطالعه تمامی بیمارستان ها در حیطه ی پیشگیری از عوامل مخرب از نرم افزار های امنیت شبکه استفاده می‌کردند و این نرم افزارها را به صورت دوره‌ای به روز رسانی می‌نمودند. شیخ ابومسعودی و همکاران در پژوهشی به این نتیجه رسیدند که بنا به اهمیت بالای

اطلاعات بیماران لازم است سیاست گذاری‌های لازمی همچون استفاده از دیواره‌ی آتش می‌تواند شبکه را در برابر ترافیک ناخواسته و هم چنین نفوذ دیگران به کامپیوترها حفاظت کند و استفاده از کنترل های فنی به منظور قفل صفحه نمایش در زمانیکه کاربر محل خود را ترک کرده و یا با سیستم کار نمی‌کند (۲۲). یکی از نتایج پژوهش در این زمینه استفاده از قفل سخت افزاری به منظور جلوگیری از کپی غیرقانونی و عدم اتصال حافظه های جانبی به رایانه های حاوی اطلاعات سلامت افراد بود که مطابق با آن ابومسعودی و همکاران نیز در پژوهشی بیان داشتند که جهت جلوگیری از کپی برداری اطلاعات سیستم ها باید درگاه های اتصال حافظه های قابل حمل غیرفعال باشد. به طور کلی پیشگیری از عوامل مخرب در همه زمینه ها باعث تضمین ایمنی اطلاعات می شود(۲۲).

براساس این پژوهش همه‌ی بیمارستان‌ها نسخ پشتیبانی از داده های اسکن شده را تهیه می کنند ولی تنها در شش بیمارستان این نسخ را در فضایی خارج از اتاق سرور نگهداری می کنند. بنابرین در صورت از بین رفتن اطلاعات امکان بازیابی دوباره انها وجود ندارد.

در حیطه مدیریت امنیت اطلاعات یافته های این پژوهش حاکی از آن است که هشت بیمارستان مورد مطالعه فردی را به عنوان مسئول پاسخگویی و رعایت مقررات مربوط به سطوح دسترسی تعیین می نمودند که همسوی با ان مطالعه ی بهنام و زاهدی فر نشان داد که در کشور پرسنل مدار پزشکی به عنوان حافظ محرمانگی اطلاعات بیماران محسوب شده و ضمن آشنایی آنان با رازداری و محرمانگی اطلاعات بیماران، پاسخگوی موضوعات محرمانگی اطلاعات و رعایت حفظ امنیت اطلاعات پرونده بیماران می باشند(۲۰, ۲۳).

لذا به منظور حفظ محرمانگی اطلاعات توصیه می شود بیمارستان ها به طراحی فرم تعهد نامه ی کتبی اقدام نموده و پیش از اشتغال مسئولین واحد فناوری اطلاعات، مدارک پزشکی و سایر کاربران به اخذ آن عمل نمایند. همچنین پژوهشگران علاقمند می توانند این مدل اطلاعاتی اولیه را در استان های سطح کشور بررسی نموده تا منجر به ارائه ی الگوی ملی گردد.

قدردانی

این مقاله برگرفته از طرح تحقیقاتی دانشجویی مصوب به شماره‌ی 97s27 توسط کمیته‌ی تحقیقات دانشجویی دانشگاه علوم پزشکی جندی شاپور اهواز می-باشد که بدینوسیله نویسندگان مقاله، مراتب سپاس و قدردانی را از مسئولین مربوطه اعلام می‌دارند.

منابع

1-Moghaddasi H, Sheikhtaheri A. Organizational chart of health information management department, presented a new pattern for hospital of Iran. Payesh. 2008;7(2):129-40.[In Persian].
2-Mashoufi M, Rostami K, Mardi A. Documentation of medical records by physicians in the hospitals under Ardabil University of Medical Sciences, 2001. Journal of Ardabil University of Medical Sciences. 2006;6(1):73-7.
3-Sadoughi F, Khoushkam M, Siavash B. A comparative investigation of the access levels and confidentiality of medical document in Iran and selected countries. Journal of Health administration. 2007;10(28):49-56.
4-Daniali A, Keshtkaran A. The management of medical records to the design. Shiraz University of Medical Sciences Publications. 2001.
5-Claerhout B ,DeMoor G. Privacy protection for clinical and genomic data: The use of privacy-enhancing techniques in medicine. International Journal of Medical Informatics. 2005;74(2-4):257-65.
6-Sadoughi F, Ghazisaeid M, Meraji M, Kimiafar K, Ramazanghorbani N. Health information management technology. Tehran: jafari publish; 2011.
7-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;11(33):7-16.
8-Kabirzadeh A, MohseniSaravi B, Asgari Z, BagherianFarahabadi E, BagherzadeLadari R. Rate of general health, job stress and factors in medical records workers. Health Information Management 2007;4.۲۲-۲۱۵:(۲)

9-Davari doulatabadi N, Shahi M, Tavasoli farahi M. Effects of environmental factors on medical files kept in the hospitals affiliated to Hormozgan university of medical sciences, 2004. Medical journals of Hormozgan University 2006;10(3):279-8.
10-Farzandipour M, Sadoughi F, Ahmadi M, Karimi I. Designing a Confidentiality Principles Model of Electronic Health Record for Iran; 2007. 2008.
11-Zarei J. Compare electronic medical record filing with traditional approach in hospitals in selected cities and submit appropriate framework: MSc Thesis], Isfahan University of Medical Sciences; 2010.
12-Pereira T, Santos H, editors. A conceptual model approach to manage and audit information systems security. Proceedings of the 9th European Conference on Information Warfare and Security; 2010.
13-Paterson M, Iacovino L. Health privacy: the draft Australian national health privacy code and the shared longitudinal electronic health record. Health Information Management 2004;33(1):5-11.
14-Jo H, Kim S ,Won D. Advanced Information Security Management Evaluation System. KSII Transactions on Internet Information Systems. 2011;5(6):1192-213.
15-Cushman R, Froomkin AM, Cava A, Abril P, Goodman KW. Ethical, legal and social issues for personal health records and applications. 2010;43(5):S51-S5.
16-Barham C. Confidentiality and security of information. Anaesthesia Intensive Care Medicine. 2010;11(12):502-4.
17-Davis N, LaCour M. Introduction to health information technology: Saunders WB Co; 2001.
18-Farzandipour M, Ahmadi M, Sadoughi F, Karimi I. A comparative study on security requirements of electronic health records in the selected countries. Health Information Management. 2008;5(2):149.
19-Arab M, PourReza A, Eshraghian M, Khabiri R. A Survey on current status of patient information privacy in Tehran's hospital. Health Information Management. 2011;8(1):33-40.
20-Zahedifar R. An Investigation over the Observance of Patients' Rights in Medical Record Department in consumers' health information for research purposes,
consumers' health forum of Australi. 1998.
21-Callahan D. The new privacy officer's game plane. AHIMA.72(6):26-32.
22-SheikhAbumasoudi R, Amini N, Esmaeili N. Indicators of patient information confidentiality. Health Information Management. 2015;12(4):404.
23-Behnam S. A Comparative Study of Accessibility levels Confidentiality of Medical Records in Selected Countries Iran university of Medical Sciences2005.

The Study on Providing a Primary Information Model of Confidentiality of Electronic Archive of Medical Records in Hospital

Amirabbas Azizi[1], Sakineh Badvi[2], Sara Rashidi[2], Marzieh Bavir[2], Rojin Barati[2], Sahar Zandi[2], Hadis Ghasemi[2], Ahmad Azizi[3*]

1-Assistant Professor of Medical Informatics
2-BSc of Health Information Technology
3-MSc in Medical Record Education.

1,2,3-Department of Health Information Technology, School of Allied Medical Sciences, Ahvaz Jundishapur University of Medical Sciences, Ahvaz, Iran.

**Corresponding author:*
Ahmad Azizi; Department of Health Information Technology, School of Allied Medical Sciences, Ahvaz Jundishapur University of Medical Sciences, Ahvaz, Iran.
Tel:+989026001590
Email: azizimaster@gmail.com

Abstract

Background and Objective: In recent years, in order to solve problems related to the storage and retrieval of paper-based medical records, the hospitals scan those using imaging systems. New technology development allows unauthorized access to data therefore, data protection rules and principles are required to maintain the confidentiality of patients' information. In the present study, we investigated the confidentiality of electronic archive of medical records in hospitals in the city of Ahvaz and suggest a primary model for maintaining and enhancing data confidentiality.

Materials and Methods: This is a descriptive cross-sectional study that investigates the confidentiality of electronic archive of medical records in selected hospitals of Ahvaz in 2019. The study population includes 11 selected hospitals. The required data were gathered through a researcher-made checklist completed in person (by observing) at Medical Record Department and Information Technology Units. Frequency tables were provided by Excel software (Ver 2016).

Results: According to the study, despite various security criteria to protect the confidentiality of data, obtaining written letter of commitment for non-disclosure of the password and username had been ignored in all the centers under study except one.

Conclusion: Considering the sensitivity of health data, it is recommended that hospitals develop a written form as letter of commitment to improve confidentiality. They should require information technology and medical documents officials as well as all users to fill in the form before they can access any type of medical data.

Keywords: Confidentiality, Security, Privacy.

►*Please cite this paper as:*
Azizi AA, Badvi S, Rashidi S, Bavir M,Barati R, Zandi S, Ghasemi H, Azizi A. The Study on Providing a Primary Information Model of Confidentiality of Electronic Archive of Medical Records in Hospital. Jundishapur Sci Med J 2020; 19(6):515-522

Received: Oct 20, 2020 **Revised: April 17, 2020** **Accepted: Oct 11, 2020**