شاخص‌های محرمانگی اطلاعات بیمار*

روح اله شیخ ابومسعودی[1]، نیلوفر امینی[2]، نازیلا اسماعیلی[2]

مقاله پژوهشی

چکیده

مقدمه: امروزه سازمان‌های مراقبت بهداشتی اطلاعات بیماران را در قالب پرونده‌های کاغذی و الکترونیکی جمع‌آوری می‌کنند. به طور کلی مالکیت فیزیکی پرونده پزشکی در اختیار بیمارستان است، اما بیمار مالک منطقی اطلاعات داخل پرونده می‌باشد، بنابراین دسترسی هر فرد دیگر به پرونده بیمار به اجازه بیمار نیاز دارد. هدف از این مطالعه شناسایی شاخص‌های محرمانگی اطلاعات بیماران در دو بیمارستان شهدای لنجان شهرستان زرین شهر و بیمارستان محمد رسول الله (ص) شهرستان مبارکه، در استان اصفهان، بود.

روش بررسی: پژوهش حاضر از دسته کاربردی است که به صورت کیفی (Qualitative) انجام شد. جامعه پژوهش دو بیمارستان بزرگ استان اصفهان، بیمارستان محمد رسول الله (ص) مبارکه و بیمارستان شهدای لنجان زرین شهر، در سال ۱۳۹۲ خورشیدی بود. چک لیستی معتبر و جهانی، منتشر شده از جانب انجمن پزشکی بریتیش کلمبیای کانادا، به عنوان ابزار گردآوری داده‌ها انتخاب گردید که ۲۵ سؤال در ۶ حیطه را شامل می‌شود. روایی این چک لیست پس از ترجمه توسط محققین و اعمال اصلاحات مورد نیاز بر روی آن از جانب اساتید مربوطه تأیید گردید. داده‌های مورد نیاز از طریق مصاحبه و مشاهده و توسط پژوهشگران گردآوری گردید. سپس اطلاعات مورد نیاز استخراج و فرآیند تحلیل و مقایسه به صورت کیفی انجام گرفت.

یافته‌ها: اصول محرمانگی در رابطه با چاپ، انتقال، ذخیره‌سازی و افشای اطلاعات پرونده بیماران در هر دو بیمارستان، به طور کلی رعایت می‌شود. سیاست گذاری هر دو بیمارستان در ارتباط با شاخص‌های حفظ محرمانگی در حیطه کارکنان ضعیف می‌باشد. در هیچ کدام از دو بیمارستان اطلاعیه‌ای مبنی بر آگاهی بیمار نسبت به حریم خصوصی بیمار و شیوه دسترسی به اطلاعاتش وجود ندارد. مسؤولین Information Technology بیمارستان‌ها به کمک مسؤولین بخش‌ها و با توجه به حیطه کاری هر فرد سطوح دسترسی کاربران را مشخص کرده و شناسه کاربری مناسب را به هر فرد اختصاص می‌دهند که رمز عبور توسط هر کاربر قابل تغییر می‌باشد. هر دو بیمارستان از فرآیندها و کنترل‌های فنی استفاده نمی‌کنند. در هر دو بیمارستان کنترل مناسبی به منظور تأمین امنیت در شبکه محلی و جلوگیری از ورود افراد غیر مجاز وجود ندارد.

نتیجه‌گیری: با توجه به اهمیت رعایت شاخص‌های محرمانگی در رابطه با اطلاعات بیماران لازم است اقدامات و فرآیندهای جدیدی درهر دو بیمارستان اعمال شود. هر دو بیمارستان مورد بررسی در زمینه‌های مورد مطالعه دارای نقاط ضعف و قوت می‌باشند. بنابراین رعایت نکات ضروری در رابطه با حفظ امنیت و محرمانگی اطلاعات بیماران الزامی است.

واژه‌های کلیدی: محرمانگی؛ امنیت؛ سیستم‌های اطلاعات بیمارستان.

دریافت مقاله: ۹۳/۴/۳۱ اصلاح نهایی: ۹۳/۹/۲۹ پذیرش مقاله: ۹۳/۱۰/۱۵

ارجاع: شیخ‌ابومسعودی روح اله، امینی نیلوفر، اسماعیلی نازیلا. **شاخص‌های محرمانگی اطلاعات بیمار.** مدیریت اطلاعات سلامت ۱۳۹۴؛ ۱۲(۴): ۳۹۳-۴۰۴.

*- این مقاله حاصل تحقیق مستقل بدون حمایت مالی سازمانی است.

۱- مربی، فوق لیسانس صنایع، دانشگاه علوم پزشکی اصفهان، اصفهان، ایران (نویسنده مسؤول) Email: Abumasoudi@live.com

۲- کارشناس، فناوری اطلاعات سلامت، دانشگاه علوم پزشکی اصفهان، اصفهان، ایران

مقدمه

در جامعه اطلاعاتی امروز، حجم زیادی از داده‌های شخصی جمع آوری، ذخیره و پردازش می‌گردند (۱). داده‌های پردازش شده که به شکل معنادار و مفیدی تعیین و تبیین شده‌اند، اطلاعات نامیده می‌شوند (۲). اطلاعات همچون سایر دارایی‌های سازمان و بلکه بسیار مهم‌تر از برخی از آنان محسوب شده و جزئی از سرمایه‌های سازمانی به شمار می‌رود (۳).

در عصر ما که به عصر اطلاعات موسوم است، در ایجاد ارزش افزوده هیچ عاملی قادر به رقابت با اطلاعات نیست (۴). در باب ارزش و اهمیت اطلاعات در جهان کنونی همین بس که نیمی از ارزش افزوده‌ای که در ژاپن و ایالت متحده حاصل می‌شود منشا اطلاعاتی دارد (۴). این درحالی است که سرعت و فعالیت‌های دسترسی به اطلاعات، به وسیله تکنولوژی اطلاعات و ارتباطات ارتقاء یافته است (۵).

بسیاری از این اطلاعات ماهیت حساسی دارند (مانند داده‌های پزشکی) و برای منفعت جامعه استفاده می‌شوند، اما می‌توانند توسط مردم بدخواه مورد سوء استفاده قرار بگیرند (۱). بنابراین، مسائل امنیت داده‌ها در هر پروژه‌ای که نیازمند ذخیره سازی یا دستکاری اطلاعات شخصی حساس باشد، به وجود می‌آید (۶).

بدون شک پرونده پزشکی یکی از مهم‌ترین مدارک و حاوی حساس‌ترین اطلاعات پزشکی و بهداشتی درمانی افراد می‌باشد (۴). اطلاعات موجود در پرونده پزشکی، باعث تداوم مراقبت بیمار توسط ارائه کننده مراقبت می‌شود و موارد قانونی و اخلاقی مهمی از قبیل: سطوح دسترسی شخص ثالث، نگهداری مناسب، امحا پرونده و افشا اطلاعات، آن را احاطه کرده است (۳). یک اصل مهم در اخلاق و فعالیت‌های مؤثر پزشکی، احترام به محرمانه سازی اطلاعات بیمار می‌باشد. این مسئله، محرمانگی حریم خصوصی بیمار را تضمین می‌کند (۳). انتظار می‌رود که محرمانگی و خصوصی بودن اطلاعات سلامت به هنگام استفاده حفظ شود و حفظ این اطمینان در هیچ حوزه‌ای حیاتی‌تر از بخش سلامت نیست (۷). در نتیجه حفظ محرمانگی اطلاعات مندرج و اسناد و مدارک موجود در پرونده ی پزشکی از اولویت بالایی برخوردار است (۴) و متخصصین بالینی و محققان نیازمند تأمین محرمانگی اطلاعات حساس بیمار خواهند بود (۱).

محرمانگی عبارتست از حق مسلم و اختیار تام در خصوص کنترل نحوه جمع‌آوری، استفاده و بهره‌گیری از اطلاعات سلامت منحصر به فرد اشخاص که بعد محرمانه بودن اطلاعات بهداشتی را شامل می‌شود (۴). گستره محرمانگی بسیار وسیع است و نه تنها شامل اوراق کتبی یا کامپیوتری می‌شود، بلکه اطلاعات شفاهی را نیز در بر می‌گیرد (۸).

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 چه کسی 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 ساخته‌اند (۴). بنابراین برای حفظ محرمانگی و امنیت اطلاعات بیمار، تصویب قوانین حفاظت از داده‌ها لازم است (۷).

قوانین جامع و کنترل‌های دسترسی باید در محیط‌های اطلاعات سلامت به قدر کافی فراهم شده باشند (۶). به طور کلی افشای اطلاعات جزء مسؤولیت‌های بخش مدیریت اطلاعات بهداشتی می‌باشد اما اشخاص دیگری نیز در آن مشارکت دارند (۸). یکی از مهم‌ترین نقش‌های بخش مدیریت اطلاعات بهداشتی، پایش و ارائه قوانین، استانداردهای حرفه‌ای، اقدامات تسهیل کننده محرمانه سازی، امنیت و افشا اطلاعات می‌باشد (۳). مردم اطلاعات بسیار حساسی را برای فراهم‌کنندگان مراقبت بهداشتی فاش می‌کنند که در صورت استفاده نامناسب، می‌تواند منجر به تبعاتی برای مشتریان سلامت شود (۷). دسترسی غیر مجاز و افشای اطلاعات سلامت می‌تواند منجر به تبعیض شغلی و بیمه‌ای و همچنین سایر ضررهای شخصی شود (۶). بنابراین در صورتی که معیاری برای ارزیابی و بهبود و حفظ محرمانگی تعریف نشود، این اطلاعات به میزان وسیعی منتشر و مشکلات عدیده حقوقی، اجتماعی و اقتصادی به دنبال خواهد داشت (۴).

صدوقی و همکارانش در پژوهش خود با عنوان «مقایسه سطوح دسترسی و محرمانگی مدارک پزشکی در کشورهای منتخب و ایران» اینگونه بیان کردند که وضعیت مدارک پزشکی، محرمانه سازی و سطوح دسترسی به آن در ایران با استانداردهای جهانی فاصله زیادی دارد. همچنین عدم تطابق عملکرد بخش مدارک پزشکی بیمارستان‌های ایران با فعالیت‌های استاندارد تعریف شده در کشورهای پیشرفته و نامطلوب بودن روش‌های انجام کار، باعث انحراف مسیر فعالیت‌های این بخش از اهداف اصلی خود شده است (۴). فرزندی پور و همکارانش در پژوهشی با عنوان «مطالعه‌ی تطبیقی اصول محرمانگی اطلاعات بیماران در پرونده‌ی الکترونیک سلامت در کشورهای منتخب» دریافتند که دو کشور استرالیا و کانادا در خصوص دسترسی خود فرد به اطلاعات پرونده‌ی الکترونیک سلامت محدودیت‌هایی ایجاد کرده‌اند و کشور انگلستان دسترسی فرد به اطلاعات را بر پایه‌ی نیاز به دانستن، به طور کلی مجاز شمرده است. آن‌ها همچنین بیان کردند که اصول محرمانگی اطلاعات پرونده الکترونیک سلامت در دو کشور استرالیا و کانادا از جامعیت بیشتری برخوردار است، این درحالی است که کشور ایران فاقد اصلی در این زمینه می‌باشد (۷). حاجوی و همکارانش در پژوهشی بر مبنای راهنمای سازمان بهداشت جهانی، به مقایسه میزان رعایت اصول محرمانگی در موارد قانونی، پرداختند. نتایج این پژوهش در زمینه میزان رعایت محرمانگی و افشای اطلاعات بیمار در بیمارستان‌های آموزشی وابسته به دانشگاه علوم پزشکی ایران، تهران و شهید بهشتی به ترتیب ۶۱/۶۰ و ۵۸ درصد می‌باشد (۳). Claerhout و DeMoor در مطالعه‌ای استفاده از تکنولوژی‌های بهبود حریم خصوصی به منظور حفاظت از حریم خصوصی داده‌های بالینی و ژنومی را بررسی نمودند. رویکردهای عملیاتی در این مقاله بر اساس دو مدل pseudonymisation بوده و نتایج نشان می‌دهد که تکنیک‌های پیشرفته این دو مدل می‌تواند حفاظت بهینه از حریم خصوصی اشخاص را فراهم نماید، در حالی که هنوز جمع آوری گروه بندی داده‌ها در مکان‌ها و دوره‌های زمانی متفاوت مجاز می‌باشد (۱).Denley و همکارانش در پژوهش خود رویکرد وسیعی به منظور مدیریت حریم خصوصی بیمار در سیستم اطلاعات بالینی در بخش مراقبت ثانویه توصیف نمودند. آن‌ها بیان کردند که در رویکرد سنتی، دسترسی به اطلاعات همه بیماران برای کارکنان بیمارستان فراهم می‌شود که این کار قابل قبول نمی‌باشد (۹). Anderson در پژوهش خود با عنوان «مدل سیاست امنیتی برای سیستم های اطلاعات بالینی» معتقد است که سردرگمی بسیاری در مورد اینکه چرا و چگونه باید اطلاعات حفاظت شوند، وجود دارد. زیرا هیچ مدل سیاست امنیتی قابل مقایسه که توضیح روشن و مختصری از نقش‌های دسترسی برای سیستم‌های اطلاعاتی را بیان کند، وجود ندارد (۱۰).

Li و همکارانش در پژوهشی به بررسی دستگاه‌های جیبی در جهت افزایش امنیت و راحتی شهروندان سالمند پرداختند. آن‌ها بیان کردند که این کارت در حفظ حریم خصوصی بیماران سالمند موثر بوده و سالمندان می‌توانند از این کارت برای ذخیره شماره شناسایی شخصی خود استفاده کنند (۱۱). Gobuty به دنبال نتایج حاصل از مطالعه‌ای در سال۲۰۰۲ میلادی، به بررسی سازماندهی اجرای حریم خصوصی و امنیت در تکنولوژی تصویربرداری پزشکی، پرداخت. او معتقد است از نظر کمیته امنیت و حفظ حریم خصوصی، ارائه دهندگان مراقبت سلامت نیازمند اجرای قوانین به منظور حفاظت از محرمانگی داده‌های قابل شناسایی بیمار هستند. نتایج در این مقاله نشان دهنده آن است که تخصیص منطقی قوانین اساسی امنیت می‌تواند به فراهم کنندگان در تأمین الزامات قانونی خود تحت نظر HIPPA(Health Insurance Portability and Accountability Act) در ایالات متحده و سایر مقررات مشابه در سطح بین المللی کمک نماید (۱۲).

پژوهشی در سال ۲۰۱۲ میلادی با عنوان «دیدگاه استرالیایی‌ها در مورد حفاظت از حریم خصوصی اطلاعات سلامت شان در پایگاه داده‌های آماری»، حمایت ویژه مردم از تحقیقات پزشکی (۹۳ درصد) و نگرانی در رابطه با حریم خصوصی اطلاعات سلامت (۶۶ درصد) را نشان می‌دهد. در پایان محققان بهبود حفاظت از حریم خصوصی اطلاعات

شخصی را از طریق معرفی اقدامات امنیتی اضافی در انتشار داده‌ها پیشنهاد نموده‌اند (۱۳).

در این مطالعه شاخص‌های محرمانگی در بخش مدیریت اطلاعات بهداشتی دو بیمارستان استان اصفهان مورد بررسی قرار گرفته و نتایج در جهت ارتقای سطح محرمانگی ارائه گردیده است.

روش بررسی

پژوهش حاضر از دسته ی مطالعات کاربردی است که کاملا به صورت کیفی (Qualitative) می‌باشد. جامعه پژوهش، دو بیمارستان بزرگ استان اصفهان، بیمارستان محمد رسول الله (ص) مبارکه و بیمارستان شهدای لنجان زرین شهر، در سال ۱۳۹۲ خورشیدی بود. به دلیل تأیید بخش مدیریت فناوری و اطلاعات دانشگاه علوم پزشکی اصفهان در خصوص کامل بودن سیستم های اطلاعاتی، این دو بیمارستان به عنوان جامعه ی پژوهش انتخاب گردید.

با توجه به اینکه تاکنون هیچ پژوهشی در زمینه میزان رعایت محرمانگی در داخل کشور انجام نشده است، با جست و جو در پایگاه های مقالات خارجی، چک لیست معتبر و جهانی منتشر شده از جانب انجمن پزشکی بریتیش کلمبیای کانادا، به منظور گردآوری داده‌ها در این پژوهش مورد استفاده قرار گرفت. این چک لیست شامل ۲۵ سؤال در ۶ حیطه سیاست‌ها و دستورالعمل‌های بالینی، کارکنان، بیماران، پرونده الکترونیکی بیمار و سیستم اطلاعاتی، سخت‌افزارها و شبکه‌های محلی و بی‌سیم می‌باشد. روایی این چک لیست پس از ترجمه توسط محققین و اعمال اصلاحات مورد نیاز بر روی آن از جانب اساتید مربوطه تأیید گردید. همچنین با توجه به استاندارد بودن چک لیست، پایایی آن تأیید شده می‌باشد.

ممیزی فرآیندی است سیستماتیک، مستقل و مستند که بمنظور بدست آوردن شواهد ممیزی و ارزیابی هدفمندآنها انجام می شود تامشخص شود که معیارهای ممیزی تاچه اندازه برآورده شده اند. به این منظور پژوهشگران پس از دریافت مجوزهای لازم و هماهنگی با بخش های مربوطه ی بیمارستان ها اقدام به جمع آوری اطلاعات نمودند. داده های مورد نیاز از طریق مصاحبه و مشاهده و توسط پژوهشگران گردآوری گردید، که افراد مورد مصاحبه ۱۸ نفر از مدیران بخش مدارک پزشکی، کارشناسان IT و سایر افراد مرتبط به سیستم‌های اطلاعاتی بیمارستان‌ها بودند. پس از گردآوری داده‌ها، اطلاعات مورد نیاز استخراج و فرآیند تحلیل و مقایسه به صورت کیفی صورت گرفت. لازم به ذکر است که به لحاظ اهمیت موضوع، داده‌های گردآوری شده نزد پژوهشگران محفوظ مانده و صرفا «جهت دستیابی به اهداف پژوهش حاضر» از آن ها استفاده شده است.

یافته‌ها

یافته‌های حاصل به تفکیک بیمارستان و بر اساس ۶ حیطه اصلی در چک لیست به شرح زیر می‌باشد:

بیمارستان محمدرسول الله(ص) مبارکه

سیاست‌ها و دستورالعمل‌های بالینی

مباحث مربوط به رعایت محرمانگی در حیطه سیاست‌ها و دستورالعمل‌های بالینی، به خوبی رعایت می‌شود. این حیطه شامل مولفه‌های چاپ، انتقال، ذخیره سازی اطلاعات بیمار و افشای اطلاعات پرونده‌های بیماران می‌باشد که در جهت رعایت آن‌ها، هر کاربر دارای شناسه کاربری و رمز عبور مجزا بوده و از دسترسی افراد ناشناس جلوگیری می‌شود.

تاکنون بیمارستان با حوادث امنیتی و تحقیقات نفوذی مانند هکرها برخوردی نداشته است و امکان دسترسی غیر مجاز به اطلاعات داخل مجموعه ی بیمارستان و سیستم اطلاعاتی آن (HIS: Health Information System) وجود ندارد. در رابطه با فرآیندهای اجرایی به منظور مرتب سازی پرونده های کاغذی بیماران، پرونده های راکد کاغذی طبق استاندارد موجود تفکیک شده و آماده امحا می‌شوند و وسایل الکترونیکی قدیمی، مانند کامپیوترهای قدیمی، که شامل داده‌های محرمانه است، نزد مسئول IT، بایگانی می‌گردد.

کارکنان

کارکنان در ماه‌های اول استخدام نسبت به چگونگی حفظ حریم خصوصی و محرمانگی اطلاعات سلامت، توجیه می‌شوند.

مسئول IT بیمارستان از اهمیت این موضوع کاملا آگاه بوده و حتی اقدامات آموزشی در زمینه رعایت محرمانگی را در نظر گرفته است. با این حال توافق نامه‌ای که کارکنان را ملزم به حفظ محرمانگی اطلاعات سلامت نماید، در بیمارستان وجود ندارد.

بیماران

در زمینه آگاهی بیمار نسبت به حریم خصوصی و شیوه‌های دسترسی به اطلاعات، هیچ اطلاعیه‌ای در بیمارستان وجود ندارد و تنها در سالن‌ها و بخش‌های بالینی، یک منشور اخلاقی در رابطه با آیین‌نامه‌های واگذاری اطلاعات پرونده، به صورت خلاصه و موردی مشاهده می‌شود. لازم به ذکر است، روندهای از پیش تعیین شده‌ای در راستای پاسخ‌گویی به درخواست بیمار جهت دسترسی به اطلاعات شخصی، اصلاحات و شکایات، وجود دارد.

پرونده الکترونیکی بیمار و سیستم اطلاعاتی

در میان کارکنان بیمارستان مورد پژوهش، شخصی با سمت مدیر سیستم اطلاعاتی وجود ندارد و مشکلات ایجاد شده در این سیستم توسط مسؤول IT بیمارستان مرتفع می گردد. دیگر وظایف مسؤول IT شامل اضافه کردن کاربر جدید به مجموعه، تغییرات سطح دسترسی کاربر و غیر فعال کردن حساب کاربران قدیمی می‌باشد. شناسه کاربری کاربران توسط مدیر IT مشخص گردیده و رمز عبور هر کاربر، به منظور دسترسی به سیستم اطلاعاتی، توسط خود فرد تعیین شده و فاقد امنیت بالا می‌باشد. تعیین سطوح دسترسی توسط مسئول IT و با کمک مدیر هر بخش انجام می‌شود و اطلاعات بیماران برای هر یک از کاربران سیستم با توجه به حیطه کاری آن‌ها، قابل دسترس می‌باشد.

نتایج ثبت شده توسط هر فرد در سیستم، از طریق نرم‌افزارهای مدیریت سرور مشخص می‌باشد. با کمک فرآیند Log گیری مواردی همچون اطلاعات ثبت شده، تغییرات انجام شده و زمان دسترسی هر فرد به سیستم، مشخص می‌شود. همچنین قابلیت ردگیری افراد از طرف دانشگاه علوم پزشکی اصفهان، در صورت نیاز، وجود دارد. برنامه و دستورالعمل ممیزی برای انتخاب فردی که امور عادی و دوره‌ای محرمانگی و امنیت سیستم‌های اطلاعاتی را به صورت مداوم مورد پایش قرار دهد، وجود ندارد. به طور کلی سرپرست هر بخش، مسؤول پایش امور عادی و دوره‌ای محرمانگی و امنیت سیستم های اطلاعاتی می‌باشد.

سخت افزارها

استفاده از فکس و ایمیل برای کلیه بخش‌های بیمارستان ممنوع بوده و تنها در واحد آمار بیمارستان برای گزارشات آماری استفاده از ایمیل مجاز می‌باشد. برای جلوگیری از دسترسی غیر مجاز به اطلاعات، دستگاه‌های جانبی مانند پرینتر به صورت محدود و تنها برای پرینت نتایج گزارشات تعبیه شده است. این دستگاه‌ها در محل‌های امن و دور از دسترسی افراد عادی قرار گرفته‌اند. لازم به ذکر است که پرینترها شبکه هستند.

برای جلوگیری از رویت اطلاعات توسط افراد غیر مجاز، مانیتور کامپیوترها پشت به افراد مراجعه کننده قرار گرفته، به گونه‌ای که فقط کارکنان هر ایستگاه کاری قابلیت رویت صفحه نمایش را دارند. لازم به ذکر است در یکی از بخش‌های بازدید شده این مهم در نظر گرفته نشده بود. به منظور دسترسی به اطلاعات از خارج از کامپیوتر، دستگاه‌ها مجهز به دی وی دی خوان و درگاه USB می‌باشند. اطلاعات ذخیره شده در سیستم‌های بیمارستان مانند فایل‌های Word، Excel و ... فاقد رمز بوده و به راحتی قابل دسترسی می‌باشند.

فرآیندها و کنترل‌های فنی (همچون سیستم‌های هوشمند قفل کردن کامپیوتر که در صورت عدم استفاده کاربر عمل می‌کند و کاربر بعد از مراجعه با وارد کردن رمز عبور مجددا می‌تواند به سیستم دسترسی داشته باشد) برای جلوگیری از مشاهده صفحه نمایش، زمانی که کاربر محل کار خود را ترک کرده وجود ندارد.

سیستم‌های بیمارستان مجهز به آنتی ویروس Kaspersky ، تحت شبکه دانشگاه علوم پزشکی اصفهان بوده و در حال حاضر توسط سرور مرکزی، آخرین فایل‌های بروز رسانی را

دریافت می‌نماید. همچنین به دلیل ناسازگاری برخی از نرم‌افزارهای نصب شده بر روی سیستم‌های بیمارستان، دیوار آتش غیر فعال است.

شبکه محلی و بی‌سیم

بیمارستان فاقد شبکه بی‌سیم می‌باشد. در راستای تأمین امنیت در شبکه محلی (LAN: Local Area Network) سیمی و جلوگیری از ورود افراد غیر مجاز، کنترل‌های مناسبی وجود ندارد. اما با توجه به محدود بودن تعداد کامپیوترها در هر بخش، همیشه تعدادی از پرسنل در هر ایستگاه کاری حضور داشته و از ورود افراد غیرمجاز جلوگیری می‌نمایند. همچنین کاربران برای اتصال به اینترنت از VPN (Virtual Private Network) استفاده می‌کنند که در اختیار افراد خاص و محدود قرار می‌گیرد.

بیمارستان شهدای لنجان زرین شهر

سیاست‌ها و دستورالعمل‌های بالینی

اصول محرمانگی در زمینه چاپ، انتقال، ذخیره‌سازی و افشای اطلاعات پرونده‌های بیماران در سیستم مدیریت اطلاعات، در نظر گرفته شده است. به منظور جلوگیری از دسترسی افراد غیر مجاز و رعایت محرمانگی در این حیطه‌ها، به هر کاربر شناسه کاربری و رمز عبور مجزا تعلق گرفته است. تاکنون بیمارستان با حوادث امنیتی و تحقیقات نفوذی مانند هکرها برخورد نداشته است و امکان دسترسی غیر مجاز به اطلاعات داخل مجموعه بیمارستان و سیستم اطلاعاتی آن (HIS) نیز وجود ندارد. تاکنون هیچ یک از پرونده کاغذی بیمارستان امحا نشده است و همگی در بخش مدارک پزشکی بیمارستان نگهداری می‌شوند. کلیه اطلاعات الکترونیکی بیماران بر روی سرور ذخیره و اطلاعات محرمانه‌ای روی کامپیوترهای بخش‌ها وجود ندارد. تنها در بخش‌های محدودی با توجه به سیاست‌های هر بخش، اطلاعات در قالب نرم افزارهایی مانند Word و Excel بر روی هارد کامپیوتر ذخیره می‌گردد.

کارکنان

در رابطه با چگونگی حفظ حریم خصوصی و محرمانگی اطلاعات سلامت توسط کارکنان، در ماه‌های اول استخدام توضیحات کلی به افراد داده می‌شود. مسؤول بخش IT و مدارک پزشکی بیمارستان بر این عقیده‌اند که نیازی به آموزش سالیانه کارکنان در ارتباط با چگونگی حفاظت از شناسه کاربری و رمز عبور، حلقه‌های دسترسی به اطلاعات محرمانه و اختیارات دسترسی نیست، زیرا که سیستم اطلاعاتی بیمارستان ثابت و بدون تغییر می‌باشند. همچنین هیچ توافق نامه‌ای مبنی بر رعایت محرمانگی اطلاعات سلامت بیمار که کارکنان را ملزم به رعایت آن گرداند، وجود ندارد.

بیماران

در رابطه با آگاهی بیمار نسبت به حریم خصوصی و شیوه‌های دسترسی به اطلاعات، هیچ اطلاعیه‌ای در بیمارستان وجود ندارد و تنها در سالن‌ها و بخش‌های بالینی، یک منشور اخلاقی در رابطه با آیین نامه‌های واگذاری اطلاعات پرونده، به صورت خلاصه و موردی مشاهده می‌شود. با این حال، روندهای از پیش تعیین شده‌ای در راستای پاسخ گویی به درخواست بیمار جهت دسترسی به اطلاعات شخصی، اصلاحات و شکایات، تعریف شده است.

پرونده الکترونیکی بیمار و سیستم اطلاعاتی

در میان کارکنان بیمارستان شخصی با سمت مدیر سیستم اطلاعاتی وجود ندارد و مسؤول IT پاسخگوی مشکلات ایجاد شده در سیستم‌ها می‌باشد. از وظایف دیگر مسئول IT بیمارستان می‌توان به اضافه کردن کاربر جدید به مجموعه، تغییرات سطح دسترسی کاربران و غیر فعال کردن حساب کاربران قدیمی، اشاره نمود. شناسه کاربری کاربران توسط مدیر IT مشخص گردیده و رمز عبور هر کاربر جهت دسترسی به سیستم اطلاعاتی توسط خود فرد تعیین شده و فاقد امنیت بالا می باشد. دسترسی هر کاربر به اطلاعات بیماران با توجه به حیطه کاری او می باشد که توسط مسؤول IT و با کمک مدیر هر بخش مشخص می‌گردد.

نتایج ثبت شده توسط هر فرد از طریق نرم‌افزارهای مدیریت سرور مشخص می‌گردد. فرآیند Log گیری در بیمارستان انجام شده و مواردی همچون اطلاعات ثبت شده، تغییرات

انجام شده و زمان دسترسی هر فرد را مشخص می‌کند. قابلیت ردگیری استفاده کنندگان از سیستم اطلاعاتی توسط دانشگاه وجود دارد، که نیازمند انجام هماهنگی لازم با بیمارستان می‌باشد. برنامه و دستورالعمل ممیزی برای انتخاب فردی که امور عادی و دوره‌ای محرمانگی و امنیت سیستم‌های اطلاعاتی را به صورت مداوم مورد پایش قرار دهد، وجود ندارد و سرپرست هر بخش، مسؤول پایش امور عادی و دوره‌ای محرمانگی و امنیت سیستم‌های اطلاعاتی می‌باشد.

سخت افزارها

در سیاست‌های کاری بیمارستان استفاده از فکس و ایمیل برای کلیه بخش‌های بیمارستان ممنوع گردیده است. دستگاه‌های جانبی مانند پرینتر برای جلوگیری از دسترسی غیر مجاز به اطلاعات، به صورت محدود و تنها به منظور پرینت نتایج گزارشات تعبیه شده‌اند. با این حال در چند بخش نیز از پرینترهای معمولی استفاده شده که با یکدیگر شبکه هستند.

در تعدادی از بخش‌ها مانیتورها در زیر هر پیش‌خوان به صورت مورب قرار گرفته‌اند و بدین ترتیب امکان مشاهده اطلاعات توسط افراد غیرمجاز وجود دارد. به منظور دسترسی به اطلاعات از خارج از کامپیوتر، دستگاه‌ها مجهز به سی دی خوان بوده، اما درگاه USB غیر فعال می‌باشد. اطلاعات ذخیره شده در سیستم‌های بیمارستان مانند فایل‌های Word، Excel و ... فاقد رمز بوده و به راحتی قابل دسترسی می‌باشند. فرآیندها و کنترل‌های فنی (همچون سیستم‌های هوشمند قفل کردن کامپیوتر که در صورت عدم استفاده کاربر عمل می‌کند و کاربر بعد از مراجعه با وارد کردن رمز عبور مجددا می‌تواند به سیستم دسترسی داشته باشد) در جهت جلوگیری از مشاهده صفحه نمایش، زمانی که کاربر محل را ترک کرده وجود ندارد. سیستم‌های بیمارستان مجهز به آنتی ویروس Kaspersky بوده و توسط سرور مرکزی آخرین فایل‌های بروز رسانی را دریافت می‌دارد. دیوار آتش بر روی همه کامپیوترهای بیمارستان فعال گردیده است.

شبکه محلی و بی سیم

با توجه به اینکه شبکه بیمارستان سیمی می‌باشد، به منظور تأمین امنیت در شبکه محلی (LAN) و جلوگیری از ورود افراد غیر مجاز، کنترل‌های مناسبی وجود ندارد. اما با توجه به محدود بودن تعداد کامپیوترها در هر بخش، همیشه تعدادی از پرسنل در هر ایستگاه کاری حضور داشته و از ورود این افراد جلوگیری می‌نمایند. همچنین کاربران به منظور اتصال به اینترنت از VPN استفاده می‌کنند که در اختیار افراد خاص و محدود قرار می‌گیرد.

بحث

نتایج مطالعه Gobuty نشان دهنده آن است که از نظر کمیته امنیت و حفظ حریم خصوصی، ارائه دهندگان مراقبت سلامت نیازمند اجرای قوانین به منظور حفاظت از محرمانگی داده‌های قابل شناسایی بیمار هستند. این داده‌ها ممکن است در مرحله ایجاد، ذخیره و حتی انتقال به صورت الکترونیکی باشد (۱۲). حاجوی و همکارانش نیز در نتایج خود اعلام می‌کند که در کلیه بیمارستان‌ها افراد خارج از بیمارستان یا مرکز بهداشتی اجازه دسترسی (۱۰۰ درصد) به مدارک پزشکی را ندارند (۳). با توجه به هدف اصلی این پژوهش که ممیزی شاخص‌های محرمانگی در بخش مدیریت اطلاعاتی این دو بیمارستان و همچنین میزان تطابق بخش‌های مختلف با این شاخص‌ها می‌باشد، نتایج حاکی از آن است که اصول محرمانگی در رابطه با چاپ، انتقال، ذخیره‌سازی و افشای اطلاعات پرونده بیماران در هر دو بیمارستان، به طور کلی رعایت می‌شود. در این راستا جهت احراز هویت کارکنان از شناسه کاربری و رمز عبور مختص هر فرد استفاده شده که دسترسی به سیستم را محدود می‌کند. لازم به ذکر است هیچ کدام از دو بیمارستان تاکنون با حوادث امنیتی و تحقیقات نفوذی مانند هکرها برخورد نداشته‌اند.

در بیمارستان مبارکه برنامه‌ریزی‌هایی در راستای امحای پرونده‌های کاغذی و نگهداری از وسایل الکترونیکی قدیمی که شامل اطلاعات محرمانه می‌باشد، انجام شده است. اما در رابطه با بیمارستان زرین شهر، تاکنون اقدامی در راستای

امحای پرونده‌های کاغذی انجام نشده است و کلیه اطلاعات الکترونیکی بر روی سرورها ذخیره می‌گردد.

نتایج مطالعه صدوقی و همکارانش بر روی کشورهای کانادا، استرالیا، آمریکا و انگلستان، نشان می‌دهد که کادر بیمارستان اعم از مدیر اجرایی مرکز، مترون، مدیر امور مالی، مشاور اطلاعات بهداشتی، مدیر خدمات اطلاعات بهداشت، کارکنان پذیرش و مدارک پزشکی، کادر پرستاری و حتی بهیاران به اطلاعات و مدارک پزشکی بیماران دسترسی دارند. آنچه مسلم است این است که باید بین نیاز به حفظ جنبه محرمانه اسناد و مدارک پزشکی و نیاز به دسترسی سریع به این اطلاعات تعادل مناسبی برقرار شود (۴). در مطالعه حاضر سیاست‌گذاری هر دو بیمارستان در ارتباط با رعایت محرمانگی در حیطه کارکنان ضعیف می‌باشد. هیچ توافق نامه‌ای که کارکنان را ملزم به حفظ محرمانگی اطلاعات سلامت نماید، در بیمارستان‌ها وجود ندارد. همچنین برگزاری برنامه‌های آموزشی در این حوزه تنها توسط مسؤولین بیمارستان شهرستان مبارکه در نظر گرفته شده و مسؤولین بیمارستان شهرستان زرین شهر نیازی به برگزاری این دوره‌ها نمی‌بینند.

بررسی‌ها نشان دهنده آن است که بیمار باید از حق دسترسی به مدارک پزشکی و اصلاح اشتباهات مندرج در آن‌ها برخوردار باشد (۴). دو کشور استرالیا و کانادا در خصوص دسترسی خود فرد به اطلاعات پرونده‌ی الکترونیک سلامت محدودیت‌هایی ایجاد کرده‌اند و کشور انگلستان دسترسی فرد به اطلاعات را بر پایه‌ی نیاز به دانستن، به طور کلی مجاز شمرده است (۷). در این مطالعه در هیچ کدام از دو بیمارستان اطلاعیه‌ای مبنی بر آگاهی بیمار نسبت به حریم خصوصی بیمار و شیوه دسترسی به اطلاعاتش وجود ندارد، که این امر موجب عدم آگاهی بیماران از حقوق خود می‌شود.

نتایج مطالعه حاضر نشان دهنده آن است که مدیریت واحدی بر روی سیستم اطلاعات سلامت هر دو بیمارستان در نظر گرفته نشده است و مشکلات سیستم‌ها، توسط مسئولین IT بیمارستان‌ها پیگیری و برطرف می‌شود. مسؤولین IT بیمارستان‌ها به کمک مسئولین بخش‌ها و با توجه به حیطه کاری هر فرد سطوح دسترسی کاربران را مشخص کرده و شناسه کاربری مناسب را به هر فرد اختصاص می‌دهند که رمز عبور توسط هر کاربر قابل تغییر می‌باشد. فرآیند Log گیری در هر دو بیمارستان انجام می‌شود.

صدوقی و همکارانش بیان می‌کند که در کلیه کشورهای مورد مطالعه شخصی به عنوان مسئول حفظ محرمانگی اطلاعات بیماران وجود دارد که پاسخگوی مواردی چون صحت و تکمیل اطلاعات و پاسخ به سؤالات بیمار می‌باشد (۴). در این مطالعه هر دو بیمارستان فاقد برنامه و دستورالعمل ممیزی به منظور انتخاب فردی که امور عادی و دوره‌ای محرمانگی و امنیت سیستم‌های اطلاعاتی را به صورت مداوم مورد پایش قرار دهد، می‌باشند.

نتایج مطالعه‌ای در کشور استرالیا حاکی از آن است که بهبود حفاظت از حریم خصوصی اطلاعات شخصی از طریق معرفی اقدامات امنیتی اضافی در انتشار داده‌ها امکان پذیر می‌باشد (۱۳). در مطالعه حاضر هر دو بیمارستان از فرآیندها و کنترل‌های فنی به منظور قفل صفحه و عدم نمایش دسکتاپ در هر سیستم، زمانی که کاربر محل کار خود را ترک کرده و یا با سیستم کار نمی‌کند، استفاده نمی‌کنند. همچنین اطلاعات ذخیره شده در سیستم‌های هر دو بیمارستان مانند فایل‌های Word، Excel و ... فاقد رمز بوده و به راحتی قابل دسترسی می‌باشند.

نتایج تحقیقات Claerhout و DeMoor در راستای استفاده از تکنولوژی‌های بهبود حریم خصوصی نشان می‌دهد که تکنیک‌های پیشرفته دو مدل استفاده شده توسط آن‌ها می‌تواند حفاظت بهینه از حریم خصوصی اشخاص را فراهم نماید (۱). در این مطالعه سیستم‌های هر دو بیمارستان مجهز به به آنتی ویروس Kaspersky تحت شبکه دانشگاه علوم پزشکی اصفهان بوده و در حال حاضر توسط سرور مرکزی، آخرین فایل‌های بروز رسانی را دریافت می‌نماید. همچنین دستگاه‌های پرینت در هر دو بیمارستان شبکه بوده و تنها به منظور اهداف مشخص تعبیه شده‌اند. نحوه قرار گرفتن

مانیتورها به منظور جلوگیری از رویت اطلاعات توسط افراد غیرمجاز در بیمارستان شهرستان مبارکه بهتر از بیمارستان شهرستان زرین شهر رعایت شده است. اتصال حافظه‌های قابل حمل (فلش، هارداکسترنال و...) به منظور کپی برداری از اطلاعات با توجه به غیر فعال بودن پورت (USBUniversal Serial Bus) در بیمارستان شهرستان زرین شهر امکان‌پذیر نمی‌باشد، اما این موضوع در بیمارستان شهرستان مبارکه رعایت نشده است. همچنین دیوار آتش در بیمارستان شهرستان مبارکه غیر فعال بوده و بیمارستان شهرستان زرین شهر این قابلیت را بر روی همه کامپیوترها فعال نموده است. در مطالعه حاضر در هر دو بیمارستان کنترل مناسبی به منظور تأمین امنیت در شبکه محلی (LAN: Network Local Area) و جلوگیری از ورود افراد غیر مجاز وجود ندارد و اتصال به اینترنت از طریق (VPN Network Virtual Private) و تنها برای افراد خاص و محدود می‌باشد. در مراحل اجرای این پژوهش می‌توان محدودیت‌هایی همچون: عدم هماهنگی واحدهای مختلف با ممیزان، عدم اجازه حراست برای دسترسی به کل مستندات مربوطه، عدم آشنایی پرسنل بیمارستان‌ها با کلیدواژه‌های مهم امنیت و محرمانگی و همچنین محدودیت‌های اولیه در ارتباط با کلیت انجام این طرح در این دو بیمارستان را مدنظر قرار داد.

نتیجه‌گیری

با توجه به کلیه نکات ذکر شده در بخش یافته‌ها و مقایسه عملکرد دو بیمارستان در رابطه با شاخص‌های حفظ محرمانگی اطلاعات بیمار می‌توان بیان کرد که هر دو بیمارستان در زمینه‌های بررسی شده دارای نقاط ضعف و قوت می‌باشند و باید نکات ضروری در رابطه با حفظ امنیت و محرمانگی اطلاعات بیماران را مدنظر قرار دهند. در ادامه برخی از نکات با توجه به شاخص‌های مورد نظر در زمینه حفظ محرمانگی اطلاعات بیماران در راستای بهبود عملکرد این دو بیمارستان ارائه شده است:

– به دلیل اهمیت حفاظت از اطلاعات بیمار بهتر است در شیوه دسترسی به پرینت اطلاعات، امنیت بیشتری اعمال گردد. این امنیت می‌تواند به شکل اعمال محدودیت بوده، به گونه‌ای که تنها مدیر بخش قادر به چاپ اطلاعات بیمار باشد.

– با توجه به افزایش حملات سایبری و نفوذ هکرها نادیده گرفتن مسائل امنیتی می‌تواند منجر به حوادث جبران ناپذیری گردد. با در نظر گرفتن این موضوع بیمارستان‌ها نیازمند سیاست گذاری بیشتری در این زمینه می‌باشند.

– سیاست‌های لازم در جهت امحای پرونده کاغذی باید تدوین و بکار گفته شوند.

– اطلاعات نگهداری شده توسط مسؤول IT بهتر است درون گاوصندوق و در مکان مناسب، دور از دید افراد قرار گیرد.

– برنامه‌ریزی مناسب در ارتباط با رعایت محرمانگی در حیطه کارکنان.

– آموزش‌های اولیه هنگام استخدام در ارتباط با اهمیت حریم خصوصی و رعایت محرمانگی اطلاعات بیمار کافی نیست. با توجه به ضرورت حفظ حریم خصوصی بیماران، آموزش دوره‌ای افراد اهمیت فراوانی داشته و سیاست‌گذاری جامع‌تری را می‌طلبد.

– حفظ حریم خصوصی فقط محدود به پرونده‌های کاغذی نبوده و شامل سیستم‌های اطلاعاتی نیز می‌باشد. لذا با در نظر گرفتن توافق نامه‌ای مبنی بر رعایت محرمانگی اطلاعات سلامت، می‌توان کارکنان را از عواقب عدم توجه به این موضوع آگاه کرده و ملزم به رعایت آن نمود.

– تهیه اطلاعیه‌های جامع در مورد شیوه‌های دسترسی بیماران به اطلاعات شان می‌تواند آگاهی بیماران را نسبت به حقوق قانونی شان بالا برد.

– برگزاری جلسات آموزشی در مورد روش های بالا بردن امنیت سرور، در جهت بهبود و ارتقای دید کاربران نسبت به انتخاب رمز عبور و حفاظت از اطلاعات بیمار.

– قرار گرفتن صفحه نمایش رایانه‌ها به گونه‌ای که افراد غیرمجاز قادر به رویت آن نباشند. این اقدام در راستای حفظ امنیت و رعایت محرمانگی اطلاعات بیماران است.

– جهت جلوگیری از کپی برداری اطلاعات سیستم‌ها، باید

درگاه‌های USB برای اتصال حافظه‌های قابل حمل (فلاش، هارد اکسترنال و ...) غیرفعال باشد.

– دیوار آتش، شبکه را در برابر ترافیک ناخواسته و همچنین نفوذ دیگران به کامپیوترها حفاظت می‌کند. بنابراین بکارگیری آن یک امر حیاتی است.

– استفاده از کنترل‌های فنی به منظور قفل صفحه و عدم نمایش دسکتاپ بر روی هر سیستم، در زمانی که کاربران محل کار خود را ترک کرده و یا با سیستم کار نمی‌کنند.

– تعبیه رمزهایی با امنیت بالا برای اطلاعات ذخیره شده در سیستم‌های بیمارستان مانند فایل‌های Word، Excel و ... در راستای ایجاد محدودیت‌های دسترسی.

پیشنهادها

۱. طراحی یک دستورالعمل اجرایی برای اطلاع‌رسانی به بیماران در مورد حریم خصوصی و شیوه‌های دسترسی به اطلاعات

۲. آموزش دوره کارکنان بیمارستان در زمینه رعایت محرمانگی اطلاعات بیمار.

۳. تنظیم توافق نامه رعایت محرمانگی و امضا آن توسط کارکنان در زمان استخدام.

۴. اختصاص رمز عبور به هر کاربر توسط مسؤول IT.

۵. در نظر گرفتن سمت مدیریت سیستم اطلاعات بیمارستان به منظور نظارت و حفظ هماهنگی سیستم‌ها.

۶. عدم استفاده از نرم‌افزارهای سیستم اطلاعات تحت ویندوز.

تشکر و قدردانی

بر خود لازم می‌دانیم که از تمام مدیران و پرسنل حوزه حراست و بخش IT دو بیمارستان محمد رسول الله (ص) مبارکه و شهدای لنجان زرین شهر که در این راه ما را یاری نمودند، تشکر و قدردانی نماییم.

References

1. Claerhout B, DeMoor GJE. 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.

2. Sadoughi F, Ghazisaeid M, Meraji M, Kimiafar K, Ramezanghorbani N. Health Information Management technology. Tehran: Jafari Publish, 2011. [In Persian]

3. Hajavi A, Khoshkam 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 ShahidBeheshti Medical Sciences Universities; 2007. Health Administration 2008; 11(33):7-16. [In Persian]

4. Sadoughi F, Khoshgam M, Behnam S. Acomparative investigation of the access levels and confidentiality of medical documents in Iran and selected countries. Journal of Health Administration 2007; 10 (28):49-56. [In Persian]

5. Pereira T, Santos H. A Conceptual Model Approach to Manage and Audit Information Systems Security. In Proceedings of the 9th European Conference on Information Warfare and Security: University of Macedonia and Strategy International Thessaloniki, Greece, 1-2 July 2010 (p. 360). Academic Conferences Limited. 2010.

6. Cushman R, Froomkin A.M, Cava A, Abril P, Goodman K.W. Ethical, legal and social issues for personal health records and applications. Journal of Biomedical Informatics 2010; 43(5): S51-5.

7. Farzandipour M, Sadoughi F, Ahmadi M, Karimi I. Security requirements and solutions in electronic health records: Lessons learned from a comparative study. Journal of medical systems 2010; 34(4):629-42. [In Persian]

8. Davis N, LaCour M. Introduction to health information technology. Saunders WB Co: Course Technology; 2001.

9. Denley I, Weston Smith S, Gardner M, O'Conor R. Privacy in clinical information systems in secondary careCommentary: Let's discuss wider social and professional issuesCommentary: Organisational and cultural aspects are also important. BMJ 1999; 318(7194):1328-31.

10. Anderson RJ, editor. A security policy model for clinical information systems. Procceding of Security and Privacy (IEEE Symposium); 06 -08 May 1996; Oakland, CA; 1996.

11. Lai JT, Hou TW. Pocket EZPIN device for healthcare IC cards to enhance the security and convenience of senior citizens. Computers in Biology and Medicine 2008; 38(4):411-15.

12. Gobuty DE. Organizing security and privacy enforcement in medical imaging technology. In International Congress Series2003; 1256: 319-29.

13. King T, Brankovic L, Gillard P. Perspectives of Australian adults about protecting the privacy of their health information in statistical databases. International Journal of Medical Informatics 2012; 81(4):279-89.

Indicators of Patient Information Confidentiality*

Rouhollah Sheikh Abumasoudi[1], Niloofar Amini[2], Nazila Esmaeili[2]

Original Article

Abstract

Introduction: In present times health care organizations gather patients' information electronically and on paper documents. The physical possession of the medical records is with the hospital but the patient is the logical possessor of the information in the record so any access to the record requires the patient's permission. The objective of this study was to identify the indicators of confidentiality in the hospitals, ShohadayeLenjan in Zarinashahr and Mohammad Rasoul Allah in Mobarake in Esfahan province.

Methods: This practical research was a qualitative study. Research community was the two largest hospitals in Isfahan province, Mohammad Rasoul Allah in Mobarake and ShohadayeLanjan in ZarinShahr in 2013. A valid and universal checklist published by British Columbia Medical Association has been chosen as the data collecting process which contains 25 items in 6 domains. The validity of checklist approved by related professors, after translating and performing corrections. The required data was collected through interview and observation by the researchers. The required data was extracted, analyzed and compared.

Results: Principles of confidentiality related to printing, transfer, storage and revelation of the patients' information in the records were on the whole followed by both the hospitals. Policies related to confidentiality indicators in employees' domain were weak. In the studied hospitals there weren't any notifications based on awareness of the patient towards him/her privacy and ways to access his/her information. Considering their work domain, the CIO (Chief Information Officer) and supervisors of the hospital, define users' level of access and allocate an authenticated account in which they can change their password. None of the hospitals used technical processes' and controls. In both the hospitals in order to ensure security in local network and preventing entrance of unauthenticated individuals the absence of suitable controls were visible.

Conclusion: Considering the importance of implementing confidentiality indicators in relationship with patients' information, it's necessary to apply new procedures and processes in both the hospitals. The two hospitals assessed in this study had strengths and weaknesses. Therefor considering the important points related to ensuring security and confidentiality of patients' information is necessary.

Keywords: Confidentiality, Security, Hospital Information Systems.

Received: 22 Jul, 2014 Accepted: 5 Jan, 2015

Citation: Sheikh Abumasoudi R, Amini N, Esmaeili N. **Indicators of Patient Information Confidentiality.** Health Inf Manage 2015; 12(4):404.

*- This article resulted from an independent research without finanacial support.

1- Lecturer, Industrial Engineering, Isfahan University of Medical Sciences, Iran (Corresponding Author) Email: Abumasoudi@live.com
2- BS, Health Information Technology (HIT), Isfahan University of Medical Sciences, Isfahan, Iran