حقوق اطلاعاتی بیمار: راهکارهایی برای امنیت اطلاعات در محیط الکترونیکی

مهتاب کرمی[1]
رضا صفدری
احمد سلطانی

چکیده

پرونده الکترونیک سلامت یکی از مهم‌ترین دستاوردهای سلامت الکترونیک برای رسیدن به مراقبت بیمار محور می‌باشد. در مراقبت بیمار محور هدف قابل دسترس‌بودن تمام اطلاعات بیمار برای درمانگران به منظور بهترین تصمیم‌گیری برای بیمار است. ایجاد محیطی برای به اشتراک‌گذاری اطلاعات و الکترونیکی‌شدن اطلاعات بهداشتی باعث گردید حفظ امنیت اطلاعات سلامت و حریم شخصی بیماران به موضوعی داغ و چالش‌برانگیز تبدیل گردد. لذا در این راستا مراکز بهداشتی - درمانی لازم است اقدام به ایجاد راهکارهای امنیتی برای حفظ حقوق اطلاعاتی بیماران نمایند. در این مقاله مروری، درباره چگونگی تدوین برنامه امنیتی برای حفظ اطلاعات و سیستم‌های اطلاعات سلامت در کنار ارتقای کیفیت مراقبت برای رسیدن به سه هدف اصلی مربوط به امنیت شامل محرمانگی، صحت و دقت و موجودبودن حول سه محور اصلی محافظت‌های مدیریتی، فیزیکی و تکنیکی بحث می‌گردد.

واژگان کلیدی

امنیت، حقوق اطلاعاتی بیمار، محیط الکترونیکی

---

۱. دانشجوی دکترای مدیریت اطلاعات بهداشتی، دانشگاه علوم پزشکی تهران، تهران، ایران. (نویسنده مسؤول)
Email: karami_m@razi.tums.ac.ir

مقدمه

سلامت الکترونیک به ابزاری قوی برای بیماران و درمانگران تبدیل شده است. در این حوزه پرونده الکترونیک سلامت، به طور قابل توجهی برای داشتن سیستم اطلاعاتی جامع به منظور ارائه مراقبتی بیمار محور مفید است. (تیجرو و همکاران، ۲۰۱۱ م.) هدف پرونده الکترونیک سلامت، فراهم‌کردن مدارک مستند از مراقبت‌های گذشته، حال و آینده بیمار است که درمانگران را حمایت می‌کند. این مستندسازی، ابزاری ارتباطی بین درمانگران مختلف را فراهم می‌نماید. (وندرلیند و همکاران، ۲۰۰۹ م.)

هنگامی که پرونده سلامت به شکل الکترونیکی درآمد این ظرفیت را پیدا کرد که در همه‌جا قابل دسترس باشد بدین منظور ضروری است اطلاعات از منابع مختلف پزشکی جمع‌آوری گردند. این ویژگی قابلیت دسترسی و پیشرفت در تکنولوژی‌های اطلاعات و ارتباطات به وضعیتی منجر شد که اطلاعات بیماران با تهدیدهای جدید امنیتی و حریم شخصی مواجه گردد. (تیجرو و همکاران، ۲۰۱۱ م.) طبق مطالعات گذشته از الزامات ایجاد پرونده الکترونیک سلامت امنیت می‌باشد و تدوین یک برنامه امنیتی برای مراکز بهداشتی ــ درمانی شامل شناسایی تهدیدهای بالقوه و فرایندهای اجرایی برای حذف تهدیدها یا کم‌کردن تأثیر آن‌ها در ایجاد صدمه ضروری به نظر می‌رسد. لذا توجه به این مقوله بسیار حائز اهمیت می‌باشد. برنامه امنیتی مراکز باید حول سه محور محافظت‌های مدیریتی، محافظت‌های فیزیکی و محافظت‌های تکنیکی تدوین گردد که هریک از این محورها می‌تواند به زیرگروه‌هایی تقسیم گردد. در این مقاله ابتدا به تعریف مفاهیم در این زمینه و سپس تعیین راهکارهایی برای حفظ حقوق اطلاعاتی بیمار با توجه به سه محور مذکور به تفصیل پرداخته می‌شود.

روش

مطالعه حاضر یک پژوهش مروری و کتابخانه‌ایست که با هدف شناخت اقدامات امنیتی رایجی که برای کاهش خطرهای بالقوه برای اطلاعات بهداشتی می‌تواند بکار گرفته شود، انجام شده است. برای بررسی متون از پایگاه‌های اطلاعاتی معتبر و همچنین کتاب‌هایی در حوزه انفورماتیک به عنوان منابع اولیه استفاده گردید.

مفاهیم امنیت

در بحث حقوق اطلاعاتی بیمار با مفاهیم زیر روبرو هستیم:

ـ امنیت[۱]: شامل اقدامات، تکنیک‌ها و فناوری‌های بکاررفته برای محافظت از اطلاعات و همچنین مسؤولیت‌پذیری است یعنی این‌که حق افراد برای انتقاد یا پذیرش درباره این‌که چرا بعضی چیزها اتفاق افتاده است.

ـ حریم شخصی[۲]: به معنای حق افراد نسبت به محافظت از اطلاعات سلامت است در این راستا که با دیگران به مشارکت گذاشته نشوند و کنترل نسبت به اطلاعاتی که قرار است افشاء شوند. به عبارتی دیگر، ادعای افراد، گروه‌ها یا موسسات است در مورد تعیین این‌که چه هنگام، چگونه و چه مقدار از اطلاعاتشان در اختیار دیگران قرار گرفته شود.

ـ محرمانگی[۳]: فرایندی است که تضمین می‌کند اطلاعات فقط برای افراد مجاز قابل دسترس می‌باشد. محرمانگی از طریق کنترل دسترسی و تکنیک‌های رمزگزاری حاصل می‌گردد.

ـ صحت و دقت[۴]: تضمین می‌کند که اطلاعات دقیق است و به روش‌های غیر مجاز تغییر نمی‌کند، یعنی داده‌ها هنگام دریافت دقیقا همانند داده‌ها هنگام ارسال می‌باشند. این ویژگی تأثیر بسزایی در ایمنی بیمار دارد.

ـ موجودبودن[۵]: امکان قابل استفاده و در دسترس‌بودن اطلاعات بر حسب تقاضای یک نهاد یا فرد مجاز است. این ویژگی در اثربخشی ارائه مراقبت تأثیر بسزایی دارد.

ـ تایید صلاحیت[۶]: فرایند تایید شناسایی کاربر می‌باشد.

ـ مجازبودن[۷]: فرایند ایجاد حق دسترسی برای کاربر است.

ـ عدم انکار[۸]: تضمین این‌که هر تراکنشی که اتفاق می‌افتد قابل اثبات باشد، یعنی هم فرستنده و هم گیرنده بر تبادل صورت گرفته توافق نمایند. (تیجرو و همکاران، ۲۰۱۱ م.؛ وندرلیند و همکاران، ۲۰۰۹م.؛ فرناندز-المان و همکاران، ۲۰۱۳ م.؛ وگر و همکاران، ۲۰۰۵م.؛ چن و همکاران، ۲۰۱۲ م.؛ کلاگ، ۲۰۰۴ م.؛ یو و همکاران، ۲۰۱۳ م.)

راهکارهای امنیتی

الف ـ محافظت های مدیریتی

محافظت‌های مدیریتی شامل آنالیز و مدیریت خطر، مسؤولیت امنیت سیستم و ارزیابی سیستم امنیت می‌باشد:

۱ـ آنالیز خطر: برنامه‌ایی امنیتی شامل شناسایی تهدیدهای بالقوه و فرایندهای اجرایی برای حذف تهدیدها یا کم‌کردن اثر آن‌ها در ایجاد صدمه است که این فرایند به ترتیب ذیل می‌باشد:

ـ تعریف مرز: در این مرحله باید محدوده سازمان به طور مفصل با تعیین همه اطلاعات سلامت مخصوص بیمار، سیستم‌های اطلاعات سلامت و استفاده کنندگان

از سیستم‌ها و اطلاعات مشخص گردد.

ـ تعیین تهدیدها: با تهیه لیستی از تهدیدهای بالقوه برای سیستم‌های سلامت شامل تهدیدهای انسانی، تهدیدهای ناشی از محیط و طبیعت و تهدیدهای ناشی از عملکرد بد فناوری صورت می‌گیرد.

ـ تعیین میزان آسیب‌پذیری: با استفاده از بسته‌های نرم‌افزاری، مصاحبه، ممیزی و استخدام مشاورین خارجی، عیب و نقص در رویه‌ها و طراحی سیستم تعیین می‌گردد.

ـ آنالیز کنترل امنیت: شامل اعمال کنترل‌های پیشگیرانه و کنترل‌های شناسایی‌کننده نقص‌های بالقوه و در حال وقوع می‌باشد.

ـ تعیین احتمال خطر: شامل تعیین درجه ریسک برای هر قسمت از سیستم اطلاعات سلامت است.

ـ آنالیز اثر ناشی از خطر: در این مرحله اثرات نقص‌های امنیتی بر روی محرمانگی، درستی و قابلیت دسترسی تعیین می‌گردد.

ـ تعیین خطر: در این مرحله تمام اطلاعات جمع‌آوری‌شده برای تعیین سطح واقعی خطر بر اساس مواردی از قبیل احتمال تهدیدی خاص برای واردکردن آسیبی خاص وجود دارد، میزانی که تهدیدات به طور موفقیت‌آمیزی اعمال شوند و میزان کفایت کنترل‌های امنیتی اعمال شده مورد بررسی قرار می‌گیرد.

ـ توصیه‌های کنترل امنیت: شامل گردآوری گزارشی خلاصه در مورد یافته‌های آنالیز و توصیه‌هایی برای بهبود کنترل امنیت است.

۲ـ مسؤولیت امنیت سیستم: هر مرکز بهداشتی - درمانی باید فردی را به عنوان مسؤول نظارت بر برنامه‌های امنیت اطلاعات در نظر گیرد. این فرد تحت عنوان مدیر کل امنیت باید گزارش خود را به مدیر کل اطلاعات یا مدیر دیگری

در سازمان ارائه کند.

۳ـ ارزیابی سیستم امنیت: تلاش‌های زیادی جهت ایجاد استاندارد مشخص و جهانی برای امنیت فناوری اطلاعات صورت گرفته است. مثلا یکی از منابع این استانداردها معیارهای ارزیابی سیستم کامپیوتری مطمئن، منتشرشده توسط وزارت دفاع آمریکا است و دیگری استاندارد ISO15408 می‌باشد که طبق آن‌ها می‌توان سیستم امنیت سازمان را ارزیابی نمود. (وگر و همکاران، ۲۰۰۹ م.؛ ابدلهاک و همکاران، ۲۰۰۸ م.)

ب ـ محافظت‌های فیزیکی

محافظت‌های فیزیکی به صورت موارد ذکرشده در ذیل ارائه می‌گردد:

۱ـ تعیین مسؤولیت: هر کارمند باید مسؤول قسمتی از امنیت سیستم باشد. مثلا در بخش پرستاری، مدیر بخش مسؤول است در برابر این‌که همه کارمندان درباره اهمیت و استفاده از معیارهای امنیت آموزش دیده باشند. نکته مهم دیگر این‌که مدیر شبکه، شخصی را برای واگذاری رمزهای عبور اولیه و حذف دسترسی کارمندان بازنشسته یا انتقالی، در نظر گیرد.

۲ـ کنترل رسانه‌ها: سیاست‌ها و اقداماتی است که دریافت و حذف سخت‌افزار، نرم‌افزار و رسانه‌های کامپیوتری در داخل و خارج از سازمان و همچنین نحوه ذخیره داده‌ها را کنترل می‌نماید. روش امحاء یا حالت نهایی رسانه‌های الکترونیکی نیز جنبه دیگری از کنترل رسانه‌ها است بدین صورت که باید هنگامی که سازمان، کامپیوترهای قدیمی خود را برمی‌چیند یا تجهیزاتی را جزء مواد زائد قرار می‌دهد، سیاست‌هایی برای از بین‌بردن اطلاعات بیمار در نظر گرفته شود.

۳ـ کنترل فیزیکی: به صورت استفاده از قفل و کلید می‌باشد که در این روش ممکن است ضمن ایجاد دسترسی به اطلاعات بیمار برای درمانگران محدود گردد. روش دیگر می‌تواند سیستم کنترل موجودی باشد که شامل علامت‌گذاری یا برچسب‌زدن به هر قطعه از تجهیزات با یک شماره واحد است سپس هر قطعه به یک مکان و یک شخص مسؤول واگذار می‌شود و هنگامی که تجهیزات جا به جا، خراب یا کنار گذاشته می‌شوند باید در این سیستم ثبت شوند. نصب ابزارهای ضد سرقت به شکل استفاده از زنجیرها برای بستن کامپیوترها به میز و نصب هشداردهنده‌ها می‌تواند نوع دیگری از کنترل فیزیکی باشد.

۴ـ امنیت ایستگاه‌های کاری: بدین صورت که در محلی امن قرار گیرند یا همواره دیده‌بانی شوند. صفحه نمایش به نحوی قرار گیرد که اطلاعات در آن برای همه قابل مشاهده نباشد و مهم‌تر این‌که سیاست‌هایی واضح برای استفاده از ایستگاه‌های کاری مشترک وضع گردد. (وگر و همکاران، ۲۰۰۵ و ۲۰۰۹ م.؛ الوف، ۱۹۹۹ م.؛ جلینی، ۲۰۰۹ م.)

ج ـ محافظت‌های فنی

۱ـ کنترل دسترسی: بدین معنا که فقط افرادی که نیاز به دانستن دارند باید به اطلاعات سلامت و هویت بیمار دسترسی داشته باشند. کنترل دسترسی به داده‌های سلامت ممکن است به یکی از روش‌های دسترسی مبتنی بر کاربر، دسترسی مبتنی بر نقش و دسترسی مبتنی بر زمینه باشد. (تیجرو و همکاران، ۲۰۱۱ م.؛ وندرلیند و همکاران، ۲۰۰۹ م.؛ فرناندز-المان و همکاران، ۲۰۱۳ م.؛ وگر و همکاران، ۲۰۰۵ م.؛ ابدلهاک و همکاران، ۲۰۰۸ م.؛ شورتلیف، ۲۰۰۱ م.)

۲ـ روش‌های تایید صلاحیت: برای تایید صلاحیت از یکی یا چندین روش زیر استفاده می‌گردد.

ـ سیستم رمز عبور: رایج‌ترین روش برای کنترل دسترسی در سیستم اطلاعات سلامت ترکیبی از نام کاربری و کلمه عبور است. در این حالت کلمه عبور امن‌تر از نام کاربری است.

ـ سیستم شناسایی بیومتریک: روش شناسایی بیومتریک به یکی از صورت‌های ثبت صدا، اثر انگشت، اسکن شبکیه، اسکن کل بدن و غیره می‌باشد.

ـ تایید شماره تلفن: این روش هنگامی استفاده می‌گردد که پرسنل سازمان بخواهند از خانه به اطلاعات دسترسی داشته باشند. عملکرد آن بدین صورت است که وقتی مودمی به سیستم متصل می‌گردد این برنامه ابتدا شماره تلفن را بررسی اگر شماره تایید شد اجازه دسترسی را صادر می‌نماید. (وگر و همکاران، ۲۰۰۵ و ۲۰۰۹ م.؛ جلینی، ۲۰۰۹ م.؛ رودریگوس، ۲۰۱۰ م.)

ـ توکن[۹]: وسایلی هستند مانند کلید کارت‌ها که داخل درها یا کامپیوترها وارد می‌شوند. در این سیستم، شناسایی بر پایه مالکیت توکن است. عیب توکن‌ها این است که ممکن است گم شوند یا در جایی نامناسب قرار گیرند. هنگامی که توکن‌ها با کلمه عبور استفاده می‌شوند ضروی است که کلمه عبور روی توکن یا جایی نزدیک آن نوشته نشود. (وگر و همکاران، ۲۰۰۵ م.؛ ابدلهاک و همکاران، ۲۰۰۸ م.؛ تان، ۲۰۰۹ م.؛ مک وی، ۲۰۰۸ م.)

۲ـ بررسی اثرات بجا مانده[۱۰]: روشی است که نشان می‌دهد چه کسی به سیستم دسترسی داشته و چه کارهایی در طول زمان دسترسی انجام شده است. همچنین این قابلیت را برای مدیران شبکه به وجود می‌آورد که استفاده از منبع شبکه را مشاهده کنند. (تان، ۲۰۰۹ م.؛ هریستیدیس، ۲۰۱۰ م.)

۳ـ رمزگذاری داده‌ها[۱۱]: برای تضمین ایمنی انتقال داده‌ها از یک مکان به مکان دیگر در شبکه در برابر استراق سمع یا مخدوش‌شدن می‌رود. شکل‌هایی از رمزگذاری که امروزه در حوزه سلامت بکار می‌روند عبارتند از:

ـ زیرساختار کلید عمومی[۱۲]: در این سیستم دو کلید عمومی و خصوصی وجود دارد. معمولا داده‌ها با کلید عمومی رمزگذاری و با کلید خصوصی رمزگشایی می‌شوند.

ـ حریم شخصی خوب[۱۳]: در این روش از کلید عمومی و امضای دیجیتالی استفاده می‌شود و گیرنده و فرستنده هر دو باید در ایستگاه کاری خود پی.جی.پی یکسان داشته باشند. (وگر و همکاران، ۲۰۰۵ م.؛ الوف، ۱۹۹۹ م.؛ جلینی، ۲۰۰۹ م.؛ هریستیدیس، ۲۰۱۰ م.؛ سیلی، ۱۹۹۱ م.)

۳ـ محافظت با دیواره آتش: یک سیستم یا ترکیبی از سیستم‌هاست که از یک سیاست کنترل دسترسی بین دو شبکه حمایت می‌کند. همچنین ممکن است برای توصیف نرم افزاری که از منابع کامپیوتری حمایت می‌کند یا ترکیبی از نرم‌افزار، سخت‌افزار و سیاست‌هایی که از این منابع حفاظت می‌کنند، اصطلاح دیواره آتش استفاده شود. رایج‌ترین محل برای دیواره آتش بین شبکه‌های داخلی سازمان و اینترنت است. با وجود این‌که دیواره‌های آتش سرتاسر سیستم‌های امنیت اطلاعات سلامت وجود دارند، آن‌ها نمی‌توانند از یک سیستم در برابر همه انواع حمله‌ها محافظت کنند مثلا دیواره آتش نمی تواند ویروس‌هایی را متوقف کند که می‌توانند در داخل اسناد پنهان شوند.

۴ـ چک‌کردن ویروس‌ها: کنترل ویروس‌ها بخش مهمی از برنامه امنیتی اطلاعات سلامت است. انواع رایج ویروس‌ها به شکل فایل آلوده، فایل‌های سیستمی آلوده و فایل‌های آلوده می‌باشد. کرم‌ها نیز نوع خاصی از ویروس می‌باشند که در کامپیوتر ذخیره و سپس تکثیر می‌شوند. کرم‌ها معمولاً از طریق ایمیل از کامپیوتری به کامپیوتر دیگر منتقل می‌شوند. (وگر و همکاران، ۲۰۰۵ م.؛ ابدلهاک و همکاران، ۲۰۰۸ م.؛ تان، ۲۰۰۹ م.؛ مک وی، ۲۰۰۸ م.)

نتیجه‌گیری

برنامه امنیتی سازمان مراقبت بهداشتی شامل شناسایی تهدیدات بالقوه و اجرای فرایندهایی برای رفع یا کاهش این تهدیدات برای رسیدن به اهدافی از قبیل محرمانگی، صحت و دقت و موجودبودن است، اما نباید فراموش گردد که در یک مرکز بهداشتی - درمانی امنیت علاوه بر اطلاعات برای حفاظت از سرمایه‌های فناوری اطلاعات سازمان از قبیل شبکه‌ها، سخت‌افزار، نرم‌افزار و برنامه‌های کاربردی تشکیل‌دهنده سیستم اطلاعات سلامت سازمان نیز بکار می‌رود، چراکه بکارگیری چنین سیستم‌هایی بسیار هزینه‌بر می‌باشد. اغلب، مراکز بهداشتی - درمانی برای داشتن برنامه امنیتی مؤثر با دو چالش اصلی روبرو هستند:

اولاً: ایجاد تعادل بین نیاز به امنیت و هزینه امنیت؛

ثانیاً: ایجاد تعادلی رضایت‌بخش بین امنیت سیستم اطلاعات سلامت و موجودیت داده‌ها و اطلاعات سلامت.

بنابراین با توجه به این‌که هدف اصلی نگهداری اطلاعات و پرونده‌های سلامت افزایش کیفیت مراقبت برای بیماران است. اگر اقدامات امنیتی سازمان خیلی شدید باشد دسترسی مناسب به اطلاعات لازم برای مراقبت بیمار سخت می‌شود. از طرفی دیگر هم اگر سازمان اجازه دسترسی نامحدود به اطلاعات بیمار را برای همه کارکنان خود فراهم نماید، به طور قطع حقوق بیماران از نظر حریم شخصی و محرمانگی خدشه‌دار خواهد شد و دارایی‌های فناوری اطلاعات سازمان نیز در معرض خطر قابل توجهی قرار خواهد گرفت. مراکز بهداشتی ــ درمانی باید برای تدوین و توسعه برنامه‌های امنیتی خود در چهار محدوده اصلی شامل مطابقت با استانداردها، قواعد و خط مشی‌های مربوط به اشتراک و دسترسی به اطلاعات، مدیریت ارتباطات و عملیات‌ها، کنترل دسترسی و امنیت منابع انسانی شامل

آگاهی و آموزش کاربران درباره مسائل امنیتی، طیف وسیعی از کاربران سیستم از درمانگران گرفته تا مشاورین قانونی و خبرگان تکنیکی را دخیل و همواره به اصل «حفظ حقوق بیمار همراه با دسترسی مناسب به اطلاعات بیمار» توجه نماید.

پی‌نوشت‌ها

1. Security
2. Privacy
3. Confidentiality
4. Integrity
5. Availability
6. Aauthentication
7. Aauthorization
8. Non-repudiation
9. Token
10. Audit Trails
11. Data Encryption
12- Public Key Infrastructure (PKI)
13. Pretty Good Privacy (PGP)

فهرست منابع

Abdolhak, M. Grostick, S. Hanken, M. (2008). *Health information of a strategic resource*. USA: W. B Saunders company.

Caelli, W. Longley, D. Shain, M. (1991). *Information security handbook*. NewYork: Macmillan, Computers.

Chen, YY. Lu, JC. Jan, JK. (2012). A secure EHR system based on hybrid clouds. *J Med Syst*. 36 (5): 3375-84.

Eloff, S. (1999). Security in health-care information systems—current trends. *International Journal of Medical Informatics*. 54 (1): 39-54.

Fernández-Alemán, JL. Señor, IC. Lozoya, PÁ. Toval, A. (2013). Security and privacy in electronic health records: A systematic literature review. *J Biomed Inform*. 46 (3): 541-62

Gleni, S. Maple, C. Yue, Y. (2009). Security Issues of a Biometrics Health Care Information System: The Case of the NHS. Computing, Engineering and Information, . I. in CC '09. *International Conference*. Fullerton.

Hristidis, V. (2010). *Information Discovery on Electronic Health Records*. New York: Taylor and Francis Group.

Kluge, EH. (2004). Informed consent and the security of the electronic health record (EHR): some policy considerations. *Int J Med Inform*. 73 (3): 229-34.

MCway, D. (2008). *Today's health information management*. USA: Thomson (Delmar).

Rodrigues, J. (2010). *Health Information Systems: Concepts, Methodologies, Tools, and applications*. NewYork: Hershy.

Shortliffe, E. (2001). *Medical informatics: computer applications in health care and biomedicine*. 2ed. New York: Springer.

Tan, J. (2009). *Medical Informatic: concepts, methodology, tools and applications*. NewYork: Hershy.

Tejero, A. De la Torre, I. (2011). Advances and current state of the security and privacy in electronic health records: survey from a social perspective. *J Med Syst*. 36 (5): 3019-27.

Tejero, A. De la Torre, I. (2011). Advances and current state of the security and privacy in electronic health records: survey from a social perspective. *J Med Syst*. 36 (5): 3019-27.

Van der Linden, H. Kalra, D. Hasman, A. Talmon, J. (2009). Inter-organizational future proof EHR systems. A review of the security and privacy related issues. *Int J Med Inform*. 78 (3): 141-60.

Wager, K. Lee, FJ. Glaser, J. (2005). Managing healthcare Information system. *USA: John Wiley & Sons*.

Wager, K. Lee, FJ. Glaser, J. (2009). *Health Care Information Systems: A Practical Approach for Health Care Management*. USA: Jossey-Bass / Wiley.

Yoo, S. Kim, S. Lee, S. Lee, KH. Baek, R. Hwang, H. (2013). A study of user requests regarding the fully electronic health record system at Seoul National University Bundang Hospital: Challenges for future electronic health record systems. *Int J Med Inform*. 82 (5): 387-97.

یادداشت شناسه مؤلفان

مهتاب کرمی: دانشجوی دکترای مدیریت اطلاعات بهداشتی، دانشگاه علوم پزشکی تهران، تهران، ایران. (نویسنده مسؤول)

پست الکترونیک: Karami_m@razi.tums.ac.ir

رضا صفدری: دکترای مدیریت اطلاعات بهداشتی، دانشیار دانشگاه علوم پزشکی تهران، تهران، ایران.

احمد سلطانی: کارشناس ارشد مدارک پزشکی، دانشگاه علوم پزشکی تهران، تهران، ایران.

تاریخ دریافت مقاله: ۱۳۹۲/۴/۱۲

تاریخ پذیرش مقاله: ۱۳۹۲/۶/۱۷