فصلنامه پژوهش‌های حفاظتی ـ امنیتی دانشگاه جامع امام حسین(علیه‌السلام)
سال دوم، شماره‌ی ۲ (تابستان ۱۳۹۲): صص ۱۲۷ – ۱۳۷

امنیت داده‌ها در سیستم‌های اطلاعات سلامت

حمید مقدسی[۱]
شیرین عیانی[۲]

تاریخ دریافت: ۱۳۹۲/۰۸/۱۱
تاریخ پذیرش: ۱۳۹۲/۰۹/۲۰

چکیده

سازمان‌های مراقبت بهداشتی تولیدکننده داده‌های سلامت بر بستر سیستم‌های اطلاعاتی می‌باشند. حفظ ماهیت اصلی و ذات این داده‌ها در یک محیط امن به منظور ارائه خدمات مناسب و با کیفیت به بیماران از وظایف سیستم اطلاعاتی می‌باشد. بررسی خصوصیات و ویژگی‌های داده‌های سلامت که ضرورت امنیت این داده‌ها را الزامی می‌نماید و نیز معرفی کوشش‌هایی که به صورت ایجاد استانداردهای امنیت داده در سیستم‌های اطلاعاتی انجام شده، هدف اصلی این مطالعه می‌باشد. یافته‌های این مطالعه در مورد اهمیت داده‌های سلامت حاکی از آن است، سه عامل که خود دلایل ضرورت امنیت داده‌ها در حوزه سلامت محسوب می‌شوند، عبارتند از: محرمانگی، ریسک سوء استفاده‌های مالی، تحقیقات زیست پزشکی و علوم رفتاری.

از سویی دیگر با توجه به اهمیت داده‌های سلامت و ضرورت تأمین امنیت آنها بسیاری از سازمان‌ها به تدوین استانداردهای ملی و بین‌المللی از قبیل: ASTM، CPRI، AAMC، NAIC، ISO ۲۷۰۰۰ و HIPPA مبادرت ورزیده‌اند. قابل ذکر است که پیدایش علوم جدید و اکتشافات گوناگون می‌تواند به تولید انواع تازه‌ای از داده‌های سلامت منجر شود، بنابراین شناسائی داده‌های سلامت و خصوصیات آنها به منظور انتخاب راهبرد امنیتی مناسب، گامی مهم در طراحی موثر سیستم‌های اطلاعات سلامت می‌باشد.

کلید واژه‌ها: *استانداردهای امنیتی حوزه سلامت، امنیت داده‌ها، سیستم‌های اطلاعات سلامت، داده‌های سلامت*

۱- دانشیار انفورماتیک پزشکی و مدیریت اطلاعات سلامت دانشکده پیراپزشکی، دانشگاه علوم پزشکی شهید بهشتی
moghaddasi@sbmu.ac.ir
۲- دانشجوی دکتری انفورماتیک پزشکی شعبه بین‌الملل دانشگاه شهید بهشتی، نویسنده مسئول ayani-sh@sbmu.ac.ir

مقدمه

نیاز به مستندسازی مراقبت بیماران که از پیچیدگی‌ها و ظرافت‌های خاصی برخوردار است، عامل مهمی در استقرار سیستم‌های اطلاعات سلامت در اکثر سازمان‌های مراقبت بهداشتی به شمار می‌رود (Bates & Gawande, ۲۰۰۳). سیستم‌های اطلاعاتی که در مراکز بهداشتی، نقش پشتیبان ارائه خدمات را بر عهده دارند (Pagarkar, ۲۰۰۴) به دلیل مزایائی از قبیل کاهش خطاهای پزشکی، تداوم بخشیدن به مراقبت و ارتقاء سلامت بیماران و پژوهش دارای اهمیت فراوان هستند (Moghaddasi, ۲۰۰۸). سیستم‌های اطلاعات سلامت که بر بستر تکنولوژی ارتباطی[۱] به تبادلات سریع داده‌ها می‌پردازند از توانمندی‌های چشمگیر و اهمیت ویژه‌ای برخوردارند (Gans, Kralewski, Hammons, & Dowd, ۲۰۰۵) و (Simba, ۲۰۰۴). در صورتی که این گونه سیستم‌ها به خوبی طراحی شده باشند، امکان مدیریت و برنامه‌ریزی موفق خدمات سلامت و بحران را فراهم آورده (TanJent, ۲۰۰۵) و هزینه‌های جاری درمان را کاهش می‌دهند (Black et al., ۲۰۱۱). انجام این امور از طریق سیستم اطلاعاتی به خوبی طراحی شده با رفع نیاز گروه‌های کاری مختلف داخل و یا خارج سازمانی و به اشتراک‌گذاری داده‌های با کیفیت محقق می‌شود (W. Liu & Park, ۲۰۱۲) و (Blobel & Roger-France, ۲۰۰۱). از زاویه دید دیگر بروز هرگونه اغتشاش در ذات داده‌های سلامت نمایانگر عدم کارای سیستم اطلاعاتی است (Alemán, Señor, Lozoya, & Toval, ۲۰۱۳).

نگرانی از توزیع داده‌های بی‌کیفیت از طریق سیستم‌های اطلاعات سلامت به دلیل اثرات مخرب و ناگوار آن بر سلامتی و جان بیماران بسیار جدی است (Espinosa, ۱۹۹۸). در این زمینه متخصصین انفورماتیک پزشکی می‌کوشند تا با تهیه زیر ساخت مناسب در سیستم‌های اطلاعاتی، فضای امن و قابل اعتمادی برای حفاظت از داده‌ها فراهم آورند به گونه‌ای که هر گونه تزاحم، شناسائی و رفع گردد (Mark Diehl, ۲۰۰۸) و (Sabnis & Charles, ۲۰۱۲).

هدف این مطالعه، بررسی خصوصیات و ویژگی‌های داده‌های سلامت است که ضرورت امنیت این داده‌ها را الزامی می‌نماید و نیز معرفی کوشش‌هایی که به صورت ایجاد استانداردهای امنیت داده در سیستم‌های اطلاعاتی انجام شده، می‌باشد.

سابقه

یافته‌های حاصل از کالبد شکافی داده‌های سلامت نشان می‌دهد که بخشی از این داده‌ها مربوط به فرآیند مراقبت از بیمار هستند که خود شامل اطلاعات هویتی بیمار و داده‌های تشخیص و درمان می‌باشند.

۱. ICT

حفظ محرمانگی داده‌های هویتی و اسرار بیماران آنچنان از اهمیت ویژه‌ای برخوردار است که از حدود دو هزار سال پیش تا کنون با ادای قسم بقراط توسط پزشکان مورد توجه قرار دارد (Barber, ۱۹۹۸).

مبادله اطلاعات میان پزشک و بیمار در یک فضای محرمانه به گونه‌ای که بیمار بتواند با آرامش خاطر، خصوصی‌ترین اطلاعات شخصی خود را با پزشک مطرح کند، رمز موفقیت در مسیر تشخیص و کنترل بیماری می‌باشد (Holloway, ۲۰۰۴) و (Mermelstein & Wallack, ۲۰۰۸). حفظ محرمانگی اطلاعات بیماران، محافظ پزشک و سیستم‌های اطلاعاتی در مقابل دعاوی حقوقی و منطبق بر اصول اخلاق پزشکی و پژوهش است (Mermelstein & Wallack, ۲۰۰۸).

محرمانگی اطلاعات که از مهم‌ترین حقوق بیمار به حساب می‌آید، هیئت مدیره سازمان مراقبت بهداشتی و بیمه‌گرها را ملزم به تنظیم سیاست‌های داخلی و خارجی افشای[۱] اطلاعات نموده است (Wiant, ۲۰۰۵). تبیین این سیاست‌ها به تعیین گروه‌های مجاز (اعم از کاربران داخلی و خارجی) و سطوح دسترسی آنان به اطلاعات منتج می‌گردد (Moghaddasi, ۲۰۰۸). ایجاد ساختارهای متنوعی از داده‌های سلامت و عرضه آن به افراد مجاز و نیز جلوگیری از دسترسی افراد غیر مجاز به داده‌ها از بزرگترین چالش‌های روز علم انفورماتیک پزشکی به شمار می‌رود (Wiant, ۲۰۰۵). از سوی دیگر امروزه امنیت مالی بهداشت و درمان بیماران از طریق شرکت‌های بیمه و با حمایت اکثر دولت‌ها در جهان تضمین می‌شود. بار مالی این خدمات بر دوش دولت‌ها به قدری سنگین است که بیمه شوندگان نیز در اجرای این مهم با پرداخت حق بیمه به دولت یاری می‌رسانند. مسلماً در چنین شرایطی سوء استفاده‌های مالی و تقلباتی همچون بهره‌برداری افراد بیمه نشده از حق بیمه شدگان، بار مضاعفی بر دوش دولت‌ها و بیمه‌شدگان می‌باشد (Blobel, ۲۰۰۷) و (Barrett, ۲۰۰۴). بهره‌برداری بیشتر از سهم بیمه بیماران که به وسیله ارائه اطلاعات مالی غیر واقعی از طرف کادر درمانی به شرکت‌های بیمه انجام می‌شود نیز یک گونه قابل ملاحظه از سوء استفاده‌های مالی است که از اعتماد شرکت‌های بیمه به منظور پرداخت همان سهم اندک نیز می‌کاهد (Fernandez, ۲۰۰۴). در چنین شرایطی لازم است بیماران با فراهم نمودن ادله منطقی و ارائه داده‌های صحیح (مربوط به مراقبت و درمان و پرداخت‌ها) در برابر شرکت‌های بیمه حفاظت شوند (Moghaddasi, ۲۰۰۸). در حقیقت شرکت‌های بیمه، یکی از مهم‌ترین استفاده کنندگان داده‌های سلامت می‌باشند و از این جهت نقش سیستم‌های اطلاعاتی قابل اعتماد و امن که داده‌های مورد نیاز را در کمال صحت به این سازمان‌ها ارائه کند، مبرهن است (Blobel & Roger-France, ۲۰۰۱).

به نظر می‌رسد که تنظیم و اجرای قوانین به منظور پوشش دهی بیمه‌ای بر مبنای نسل جدید سیستم‌های الکترونیک که مبتنی بر ارتباطات از راه دور می‌باشند یکی از چالش‌های پیش رو در طراحی

۱. policy Internal and external disclosure

سیستم‌های اطلاعات سلامت باشند (Espinosa, ۱۹۹۸). بنابراین داده‌های سلامت به لحاظ مالی از اهمیت ویژه‌ای برخوردارند.

یکی از دلایل اهمیت داده‌های سلامت، مربوط به نتایج حاصل از روش‌ها و تکنولوژی‌های درمانی جدید که از طرق مختلفی مانند سلولی، مولکولی، ژنتیکی، داروئی و نانو تکنولوژی‌ها انجام می‌شوند، می‌باشد. این داده‌ها می‌توانند امنیت ملی و بین‌المللی مردم را دستخوش مخاطره نمایند لذا بایستی محرمانه بمانند. در حقیقت این روش‌های درمانی جدید به مانند یک تیغ دو لبه دارای فواید و مضرات بسیاری هستند (Bainbridge, ۲۰۰۲). از فواید آن می‌توان به درمان‌های قطعی بیماری‌ها مزمن و لاعلاج، شبیه‌سازی اعضای بدن انسان و سرعت در بهبودی بیماران اشاره کرد (Altmann, ۲۰۰۴). از سوی دیگر طراحی و ساخت سلاح‌های بیولوژیک، میکرو روبوت ها و میکرو سنسورهای جنگی و یا ایجاد موجودات شبیه‌سازی شده از موارد استفاده خطرناک این روش‌های مدرن درمانی جدید محسوب می‌شوند. یکی از خطرات جدی این روش‌ها کنترل تکنولوژی‌های نانوی قابل کاشت در بدن انسان می‌باشد (Macoubrie, ۲۰۰۴). هر یک از موارد مذکور می‌تواند حیات انسان و سایر موجودات زنده بر روی کره زمین را از بین برده و یا از سیر طبیعی آن منحرف نماید (Altmann, ۲۰۰۴). به صورت مشابه، داده‌های مرتبط با علوم رفتاری و شناختی[۱] به منظور درمان بیماران، ساخت تجهیزات پزشکی، سلاح‌ها و تجهیزات جنگی به کار می‌روند و از جمله سرمایه‌های دانشی و تحقیقاتی جوامع محسوب می‌شوند (Halff, ۱۹۸۶). مطالعات نشانگر آن است که کارائی این روش‌ها و تکنیک‌های درمانی، تائید شده و مورد توجه عموم هستند، لذا به منظور توسعه و ادامه کاربری، نیازمند تهیه زیر ساخت‌های امنیتی به منظور جلوگیری از بهره برداری‌های خطرناک و غیر ضروری می‌باشند (Macoubrie, ۲۰۰۴). در این راستا بسیاری از محققین در تلاشند تا با تهیه قوانین و مقررات ملی و بین‌المللی، الزامات و محدودیت‌های مورد نیاز به منظور حفاظت از این‌گونه داده‌ها را فراهم آورند (Altmann, ۲۰۰۴).

با توجه به اهمیت داده‌های سلامت و ضرورت تأمین امنیت آنها بسیاری از سازمان‌ها به تدوین استانداردهای ملی و بین‌المللی مبادرت ورزیده‌اند. متعاقباً برخی از این استانداردها: AAMC, CPRI, ISO ۲۷۰۰۰, HIPPA, ASTM, NAIC مورد بررسی قرار گرفته‌اند.

- **استاندارد ASTM و استاندارد CPRI**

استاندارد امنیتی ASTM از طریق کمیته‌های انجمن مواد و آزمون امریکا (مانند کمیته فنی E۳۱) به منظور حفظ امنیت داده‌ها در سیستم‌های الکترونیک تهیه و تنظیم گردیده است (Part, ۱۹۸۶) و از سوئی

۱. Cognitive Science

استاندارد امنیتی CPRI توسط موسسه پرونده الکترونیک پزشکی در راستای حفاظت از پرونده الکترونیکی بیمار تنظیم شده است (Cooper, ۲۰۰۷). این دو استاندارد بر حفاظت از اطلاعات دریافت کننده خدمات من الجمله بیماران تمرکز شایانی دارند و امنیت اطلاعات کادر درمانی را نیز تحت پوشش قرار می‌دهند. از سوئی بر حفظ حریم خصوصی و محرمانگی تاکید داشته و به منظور برقراری امنیت در پرونده الکترونیک سلامت بیماران طراحی گردیده‌اند (Jan Lovorn, ۲۰۱۰).

- **استاندارد AAMC**

استاندارد AAMC که توسط انجمن کالج‌های پزشکی آمریکا به منظور حفظ امنیت داده‌های پزشکی تبیین شده است، به منظور حفاظت از داده‌های زیست پزشکی، علوم رفتاری، تحقیقات سلامت و اپیدمیولوژیکی شکل گرفته و در سیستم‌های اطلاعاتی سازمان‌های تولید کننده این گونه داده‌ها کاربرد دارد (AAMC, ۲۰۱۲).

- **استاندارد NAIC**

استاندارد NAIC توسط اتحادیه ملی نمایندگان بیمه در راستای حفاظت از حقوق مشتریان تهیه گردیده است و در راستای حفاظت از داده‌های مالی و بیمه‌ای بیماران مورد استفاده قرار می‌گیرد. تهیه کنندگان این استاندارد مدعی‌اند که حریم خصوصی شکست ناپذیری را برای کلیه بیمه‌گرها و بیمه شدگان فراهم آورده‌اند (NAIC, ۲۰۱۳).

- **استاندارد ISO ۲۷۰۰۰**

استاندارد ISO ۲۷۰۰۰ که به منظور حفظ امنیت داده‌ها در سیستم‌های اطلاعاتی از طریق گروه کاری چهارم سازمان جهانی‌سازی استاندارد معرفی شده است و به عنوان استاندارد جامع و رفرنس به منظور ایجاد بستر امنیتی در سیستم‌های الکترونیک سلامت مورد استفاده قرار می‌گیرد. قابلیت پوشش دهی آن به سیستم‌های اطلاعات داروخانه، تجویز داروئی و ابزار آلات و تجهیزات پزشکی نیز تعمیم می‌یابد (Constantine Gikas Catapult Technology Ltd., ۲۰۱۰).

- **استاندارد HIPPA**

استاندارد مهم مدیریتی و فنی HIPPA که در دولت فدرال امریکا تصویب و توسعه یافته است و ایمن‌سازی فضای تبادل اطلاعات پرونده پزشکی بیماران را بر عهده دارد (O'Brien & Yasnoff, ۱۹۹۹) در ابتدا به منظور حفظ اصول امنیتی مرتبط با داده‌های مورد نیاز شرکت‌های بیمه شکل گرفت (Dwyer III,

(Weaver, & Hughes, ۲۰۰۴). ولی امروزه با توسعه این استاندارد، بسیاری از کشورهای دنیا به عنوان رفرنس قوانین مربوط به حافظت داده‌های سلامت از آن بهره‌برداری می‌کنند (C.-H. Liu, Chung, Chen, & Wang, ۲۰۱۲). این استاندارد جامع و رفرنس به منظور ایجاد بستر امنیتی در سیستم‌های الکترونیک سلامت با تمرکز بر حفظ حریم خصوصی و محرمانگی اطلاعات و پیاده‌سازی سیاست‌های افشای آن شکل یافته است. از سوئی توجه به این نکته ضروری است که هنوز ویژگی مهم استاندارد HIPPA در راستای حفاظت از داده‌های مالی و بیمه‌ای بیماران مورد توجه استفاده کنندگان می‌باشد.

قابل ذکر است که استانداردهای امنیتی بسیار دیگری با کاربری‌های خاص در علم انفورماتیک پزشکی به منظور ساخت سیستم‌های اطلاعاتی مورد استفاده‌اند. فرضاً استاندارد PCI-DSSکه به منظور امنیت کارت‌های پرداخت و تائید امضای الکترونیکی تبیین گردیده است (Constantine Gikas Catapult Technology Ltd., ۲۰۱۰).

یافته‌ها

یافته‌های حاصل از مطالعه در مورد اهمیت داده‌های سلامت حاکی از آن است، سه عامل که خود دلایل ضرورت امنیت داده‌ها در حوزه سلامت محسوب می‌شوند به شرح زیر مطرح هستند:

ـ داده‌های سلامت و محرمانگی

عدم وجود سیستم‌های امنیتی به منظور حفظ محرمانگی داده‌های سلامت با بروز دعاوی و شکایات قانونی علیه سازمان و یا کادر درمانی همراه می‌باشد. قابل ذکر است که عدم کفایت سیاست‌ها و قوانین مورد نیاز (اعم از سیاست‌های افشای داخلی و خارجی) به ناتوانی و یا شکست کاربری هر گونه سیستم امنیتی مرتبط با محرمانگی منجر می‌شود (Fisher & Madge, ۱۹۹۶).

ـ داده‌های سلامت و ریسک سوء استفاده‌های مالی

دایره حفاظتی شکست ناپذیر به منظور پاسداری از داده‌های مالی بیماران در سیستم‌های اطلاعاتی، ضمن جلوگیری از بروز سوء استفاده‌های مالی از دولت‌ها و افزایش اعتماد شرکت‌های بیمه به منظور پرداخت حق بیمه بیماران، امکان تنظیم قوانین جدید در راستای بیمه کردن خدمات از راه دور پزشکی را فراهم می‌آورد (Espinosa, ۱۹۹۸).

ـ داده‌های سلامت و نتایج بسیار مهم تحقیقات زیست پزشکی و علوم رفتاری

در حال حاضر نگرانی از استفاده‌های غیر مجاز از این گونه داده‌ها که ریسک بروز حوادث وحشتناک و غیر مترقبه را افزایش می‌دهد از سرعت توسعه کاربری و پیشرفت این علوم می‌کاهد؛ لذا در صورت تنظیم قوانین و بسترسازی حفاظتی مناسب علی‌الخصوص در حوزه امنیت داده‌ها، امکان استفاده مفید از این علوم فراهم می‌گردد (Halff, ۱۹۸۶) و (Bainbridge, ۲۰۰۲). آنچه مسلم است نشانگر اهمیت این گونه داده‌های سلامت در ارتباط با امنیت و تحقیقات کشورها می‌باشد. از دیگر یافته‌های این مطالعه ابعاد و مختصات استانداردهای امنیت داده‌های حوزه سلامت است که جدول شماره (۱) این ابعاد و مختصات را نشان می‌دهد.

جدول ۱- ابعاد و مختصات استانداردهای امنیت داده‌های حوزه سلامت

ردیف	شاخص داده / نام استاندارد	محرمانگی	مالی	زیست پزشکی و علوم رفتاری
۱	ASTM	✓		
۲	CPRI	✓		
۳	AAMC			✓
۴	NAIC		✓	
۵	ISO ۲۷۰۰۰	✓		
۶	HIPPA	✓	✓	

بحث و نتیجه‌گیری

نتایج حاصل از این تحقیق سه عامل که خود دلایل ضرورت امنیت داده‌ها در حوزه سلامت می‌باشند را به وضوح مشخص نموده و بیانگر این واقعیت است که استانداردهای امنیت داده‌های حوزه سلامت برای حفاظت از یک و یا تعدادی از این عوامل تهیه گردیده‌اند (Buckovich, Rippen, & Rozen, ۱۹۹۹).

فرضاً تمرکز اصلی دو استاندارد ASTM و CPRIبر حفظ محرمانگی داده‌ها است (Cooper, ۲۰۰۷). در صورتی که استاندارد AAMC به منظور صیانت از داده زیست پزشکی و علوم رفتاری تبیین گردیده است (Xiao, Hu, Croitoru, Lewis, & Dasmahapatra, ۲۰۱۰). استاندارد NAIC صرفاً به منظور حفظ امنیت مالی داده‌ها کاربرد دارد (NAIC, ۲۰۱۳)؛ و استاندارد HIPPA به دو منظور حفاظت از داده‌های مالی و حفظ محرمانگی آنها قابل استفاده است. ضمناً استاندارد ISO ۲۷۰۰۰ با توجه به پوشش دهی قابل ملاحظه‌ای که بر حفظ امنیت داده‌ها دارد بر حفاظت از محرمانگی داده‌های سلامت تاکید بیشتری دارد. (Constantine Gikas Catapult Technology Ltd., ۲۰۱۰) با توجه به این که ضرورت طراحی یک مدل و یا

چارچوب امنیتی مستقل برای سیستم اطلاعاتی الزامی است و اجرای سیاست‌های چند لایه امنیتی قابل اخذ از استانداردهای مختلف در ساخت این مدل‌ها بسیار موفق عمل کرده‌اند (Smith & Eloff, ۱۹۹۹) می‌بایست به منظور انتخاب استانداردهای موثر، به شاخص‌های مختلف داده‌های سلامت و نیاز واقعی سازمان مراقبت بهداشتی توجه داشت. در حقیقت شناسائی وجه تمایز داده‌های سلامت در سازمان‌های مراقبت بهداشتی، امکان انتخاب بهینه‌ترین استاندارد امنیتی را مقدور می‌سازد چرا که حفظ کیفیت ویژگی‌های داده‌های سلامت از طریق استانداردهایی صورت می‌پذیرد که به منظور حفاظت از آن ویژگی خاص تبیین گردیده‌اند. قابل ذکر است که در صورتی که سازمانی بهداشتی درمانی تولید کننده ابعاد داده‌ای گوناگون و متفاوتی باشد، طراحی زیر ساخت امنیتی بر اساس تلفیقی از استانداردهای مرتبط با نوع داده‌های تولید شده جوابگو خواهد بود.

از سوئی قابل توجه است که دستیابی به علوم جدید و اکتشافات گوناگون باعث ایجاد تغییرات سریع در محیط زندگی نوع بشر گردیده است. قابل پیش بینی است که ظهور تکنولوژی‌ها و روش‌های درمانی نوین در سیستم‌های مراقبت بهداشتی به تولید گونه‌های جدیدی از داده‌های سلامت خواهند انجامید. در این راستا در مرحله نخست تبیین و تصویب قوانین مرتبط با داده‌های جدید به منظور حفظ امنیت داده‌ها و در مرحله دوم تهیه و تنظیم استانداردهای امنیتی مرتبط با شاخص‌های داده‌های جدید به منظور طراحی مدل‌های امنیتی، لازمه حفاظت از داده‌ها در محیطی امن خواهد بود (Buckovich et al., ۱۹۹۹). بنابراین در دنیای تکنولوژیک جدید شناسائی داده‌های سلامت و خصوصیات آنها که می‌توانند در محیط‌های گوناگون و یا توسط تجهیزات متنوع تولید شوند به منظور انتخاب راهبرد امنیتی مناسب، گام مهمی در طراحی موثر سیستم‌های اطلاعات سلامت می‌باشد.

کتابنامه

AAMC. (۲۰۱۲). Advisor Information System Reference Manual

Alemán, J. L. F., Señor, I. C., Lozoya, P. Á. O., & Toval, A. (۲۰۱۳). Security and privacy in electronic health records: a systematic literature review. Journal of biomedical informatics.

Altmann, J. (۲۰۰۴). Military uses of nanotechnology: perspectives and concerns. Security Dialogue, ۳۵(۱) , ۶۱-۷۹.

Bainbridge, W. S. (۲۰۰۲). Public attitudes toward nanotechnology. Journal of Nanoparticle Research, ۴(۶) , ۵۶۱-۵۷۰.

Barber, B. (۱۹۹۸). Patient data and security: an overview. International Journal of Medical Informatics, ۴۹(۱) , ۱۹-۳۰.

Barrett, S. (۲۰۰۴). Insurance fraud and abuse: A very serious problem. Retrieved January, ۱۸, ۲۰۰۵.

Bates, D. W., & Gawande, A. A. (۲۰۰۳). Improving safety with information technology. New England Journal of Medicine, ۳۴۸(۲۵) , ۲۵۲۶-۲۵۳۴.

Black, A. D., Car, J., Pagliari, C., Anandan, C., Cresswell, K., Bokun, T., Sheikh, A. (۲۰۱۱). The impact of eHealth on the quality and safety of health care: a systematic overview. PLoS medicine, ۸(۱) , e۱۰۰۰۳۸۷.

Blobel, B. (۲۰۰۷). Comparing approaches for advanced e-health security infrastructures. International Journal of Medical Informatics, ۷۶(۵-۶) , ۴۵۴.

Blobel, B., & Roger-France, F. (۲۰۰۱).A systematic approach for analysis and design of secure health information systems. International Journal of Medical Informatics, ۶۲(۱) , ۵۱.

Buckovich, S. A., Rippen, H. E., & Rozen, M. J. (۱۹۹۹). Driving Toward Guiding Principles A Goal for Privacy, Confidentiality, and Security of Health Information. Journal of the American Medical Informatics Association, ۶(۲) , ۱۲۲-۱۳۳.

Constantine Gikas Catapult Technology Ltd., B., Maryland, USA. (۲۰۱۰). A General Comparison of FISMA, HIPAA, ISO ۲۷۰۰۰ and PCI-DSS Standards. Information Security Journal, ۱۹(۳) , ۱۳۲-۱۴۱.

Cooper, T. (۲۰۰۷). Managing Information Privacy & Security in Healthcare CPRI Guidelines - Information Security PoliciesDwyer III, S. J., Weaver, A. C., & Hughes, K. K.. Health Insurance Portability and Accountability Act. (۲۰۰۴). Security Issues in the Digital Medical Enterprise.

Espinosa, A. L. (۱۹۹۸). Availability of health data: requirements and solutions. International Journal of Medical Informatics, ۴۹(۱) , ۹۷-۱۰۴.

Fernandez, B. (۲۰۰۴). Health insurance: a primer.

Fisher, F., & Madge, B. (۱۹۹۶). Data security and patient confidentiality: the manager's role. International journal of bio-medical computing, ۴۳(۱) , ۱۱۵-۱۱۹.

Gans, D., Kralewski, J., Hammons, T., & Dowd, B. (۲۰۰۵). Medical groups' adoption of health records and information systems. Health Affairs, ۲۴(۵) , ۱۳۲۳-۱۳۳۳. electronic

Halff, H. M. (۱۹۸۶). Cognitive Science and Military Training. American Psychologist, ۴۱(۱۰) , ۱۱۳۱-۱۱۳۹.

Holloway, F. (۲۰۰۴). Confidentiality: threats and limits. Psychiatry, ۳(۳) , ۱۱-۱۳.

Jan Lovorn, M. K. P. (۲۰۱۰). Astm E۳۱ Security Standards.

Liu, C.-H., Chung, Y.-F., Chen, T.-S., & Wang, S.-D. (۲۰۱۲). The enhancement of security in healthcare information systems. Journal of medical systems, ۳۶(۳) , ۱۶۷۳-۱۶۸۸.

Liu, W., & Park ,E. (۲۰۱۲). e-Healthcare Security Solution Framework. Paper presented at the Computer Communications and Networks (ICCCN), ۲۰۱۲ ۲۱st International Conference on.

Macoubrie, J. (۲۰۰۴). Public perceptions about nanotechnology: Risks, benefits and trust. Journal of Nanoparticle Research, ۶(۴) , ۳۹۵-۴۰۵ .

Mark Diehl, P. E., Gretchen Murphy,Arden Forrey,Mary Alice Hanken. (۲۰۰۸). The Health Information Domain, EHR and E-۳۱Standards .

Mermelstein, H. T., & Wallack, J. J. (۲۰۰۸). Confidentiality in the age of HIPAA: a challenge for psychosomatic medicine. Psychosomatics, ۴۹(۲) , ۹۷-۱۰۳ .

Moghaddasi, H. (۲۰۰۸). Health Data Processing. Tehran: word processor.

NAIC. (۲۰۱۳). AVS+ User’s Guide.

O'Brien, D. G., & Yasnoff, W. A. (۱۹۹۹). Privacy, confidentiality, and security in information systems of state health agencies. American journal of preventive medicine, ۱۶(۴) , ۳۵۱.

Pagarkar, M. H. (۲۰۰۴). Medical Informatics Final Paper.

Part, E. (۱۹۸۶). Form and Style for ASTM Standards: American Society for Testing and Materials, Philadelphia.

Sabnis, S., & Charles, D. (۲۰۱۲). Opportunities and Challenges: Security in eHealth. Bell Labs Technical Journal, ۱۷(۳) , ۱۰۵-۱۱۱.

Simba, D. O. (۲۰۰۴). Practice Points Application of ICT in strengthening health information systems in developing countries in the wake of globalisation. African Health Sciences, ۴(۳) , ۱۹۴-۱۹۸ .

Smith, E., & Eloff, J. (۱۹۹۹). Security in health-care information systems—current trends. International Journal of Medical Informatics, ۵۴(۱) , ۳۹-۵۴ .

TanJent, e ,.project team. (۲۰۰۵). Study on Economic Impact of eHealth:Developing an evidence-based context-adaptive method of evaluation for eHealth.

Wiant, T. L. (۲۰۰۵). Information security policy's impact on reporting security incidents. computers & security, ۲.۴۵۹-۴۴۸, (۶)۴

Xiao, L., Hu, B., Croitoru, M., Lewis, P., & Dasmahapatra, S. (۲۰۱۰). A knowledgeable security model for distributed health information systems. computers & security, ۲۹(۳) , ۳۳۱-۳۴۹.