مقاله مروری

مجله انفورماتیک سلامت و زیست پزشکی
مرکز تحقیقات انفورماتیک پزشکی
دوره دوم، شماره سوم. ص۱۹٤-۱۸٤، ۱۳۹٤

مطالعه تطبیقی سه استاندارد امنیت داده در نظام سلامت

حمید مقدسی[۱]، محمد مهدی قائمی[۲]*

• **دریافت مقاله:** ۹۴/۴/۲۵ • **پذیرش مقاله:** ۹۴/۶/۳۰

مقدمه: سیستم‌های اطلاعاتی الکترونیک، سهولت دسترسی و انتقال داده‌های ناشی از آن، اهمیت رعایت استانداردهای امنیت و حریم داده‌ها در این سیستم‌ها را دو چندان کرده است.

روش: در این مطالعه مروی ابتدا ترکیبات مختلف کلیدواژه‌ها مورد جستجو قرار گرفتند. از مقالات به دست آمده، تاریخچه استانداردهای مورد استفاده در داده‌های حوزه سلامت، لزوم استفاده از این استانداردها و میزان کاربرد استانداردها در سطح دنیا مطالعه گردید. سپس پرکاربردترین و معتبرترین استانداردها انتخاب شدند و پس از مطالعه متن کامل استانداردهای انتخابی، خصوصیات مورد نظر هر استاندارد استخراج و چک لیست خصوصیات جزئی به دست آمد که با کمک آن سه استاندارد انتخابی با یکدیگر مقایسه و نقاط ضعف و قوت هر یک مورد بحث و بررسی قرار گرفت.

نتایج: خصوصیات استانداردهای مورد بررسی در ۸ گروه و ۲۲ زیر گروه دسته‌بندی شدند. ISO-27799:2008 به همه ویژگی‌های گروه رمزنگاری توجه کرده است. HIPAA به رمزگذاری در ذخیره‌سازی و کلید نامتقارن و PCI-DSS به رمزگذاری در ذخیره‌سازی، الگوریتم‌های Hash و کلید نامتقارن توجه داشته است. امنیت سیستم عامل را HIPAA به کار برده بودند. به امنیت رادیو شناسه، DNS و تلفن همراه، فقط PCI-DSS اشاره و امنیت شبکه‌های بی‌سیم را ISO-27799:2008 و PCI-DSS منظور کرده بودند.

نتیجه‌گیری: با توجه به شرایط، می‌توان از استانداردی که در زمینه موردنظر مناسب‌تر است استفاده کرد. برای سامانه‌ای که بر روی تلفن همراه PDAها استفاده می‌شود PCI-DSS و زمانی که شبکه بی‌سیم داریم ISO-27799:2008 یا PCI-DSS توصیه می‌شود و یا برای امنیت سیستم عامل HIPAA مناسب می‌باشد. استاندارد ترکیبی که ویژگی‌های هر سه استاندارد مورد بررسی را دارا باشد به عنوان امن‌ترین روش، مدنظر است.

کلید واژه‌ها: امنیت داده‌های سلامت، استاندارد، سیستم اطلاعات سلامت

•ارجاع: مقدسی حمید، قائمی محمد مهدی. مطالعه تطبیقی سه استاندارد امنیت داده در نظام سلامت. مجله انفورماتیک سلامت و زیست پزشکی ۱۳۹۴؛ ۲(۳): ۱۹۴-۱۸۴.

۱. دکترای مدیریت اطلاعات سلامت، دانشیار ، دانشکده پیراپزشکی، دانشگاه علوم پزشکی شهید بهشتی، تهران، ایران.

۲. دانشجوی دکتری انفورماتیک پزشکی، دانشکده پیراپزشکی، دانشگاه علوم پزشکی شهید بهشتی، تهران، ایران.

*** نویسنده مسؤول:** کرمان ، بلوار شهید صدوقی، نرسیده به پل راه‌آهن، جمعیت هلال احمر استان کرمان

•شماره تماس: ۰۹۱۹۴۱۸۳۰۰۱ • **Email:** Dr.MGhaemi@gmail.com

مقدمه

سیستم‌های اطلاعات مراقبت بهداشتی یک عامل مهم در بهبود کیفیت مراقبت و کاهش هزینه‌ها می‌باشند. این سیستم‌ها به عنوان زیرساختی برای تصمیم‌گیری هستند و در مدیریت هزینه‌ها، بهبود کیفیت مراقبت و گسترش تحقیقات نقش مهمی دارند [۵-۱]. اطلاعات، مانند خون برای سیستم ارائه مراقبت بهداشتی حیاتی است و پزشکان، پرستاران و سایر ارائه دهندگان مراقبت بهداشتی برای درمان نیازمند آن هستند [۶،۷]. امروزه اطلاعات بهداشتی به دلیل استفاده در بهداشت عمومی، تحقیقات زیست‌پزشکی، مراقبت از بیمار، بازپرداخت مالی به ارائه دهندگان خدمت یا بیمار، ارزیابی کیفیت خدمات بهداشتی، برنامه‌ریزی خدمات و ایمنی بیمار از اهمیت ویژه‌ای برخوردار شده و داده‌های پرونده پزشکی برای افراد زیادی از جمله بیمار، سیستم مراقبت بهداشتی، ارائه دهندگان خدمات بهداشتی، مربیان، محققان و سازمان‌های بیمه ارزشمند شده است [۱۲-۶]. بیماران در کشورهای مختلف حقوق متفاوتی دارند ولی این حق همه بیماران است که اطلاعات مربوط به سلامت، تاریخچه بیماری، تشخیص احتمالی یا اقدام درمانی، آزمایشات تشخیصی، ویزیت متخصص و درمان‌های جراحی یا طبی آن‌ها محرمانه باقی بماند [۲۵-۱۲]. از طرفی هزینه‌های مراقبت بهداشتی و چگونگی پرداخت آن از مسائل مهم ملی است. در نتیجه افزایش شدید هزینه‌های مراقبت بهداشتی، محاسبه و تعیین این هزینه‌ها برای دولت به عنوان مسؤول اصلی ارائه مراقبت بهداشتی و شرکت‌های بیمه‌گر به منظور بازپرداخت هزینه‌ها بسیار مهم شده است. این شرکت‌ها می‌خواهند فقط برای خدماتی هزینه پرداخت نمایند که واقعاً به بیمار ارائه شده و برای بیمار ضروری بوده است. داده‌ها به عنوان منبع تجزیه و تحلیل هزینه‌های قابل پرداخت برای خدمات ارائه شده می‌باشند و پرداخت کنندگان شخص ثالث هزینه‌های مذکور را برپایه این داده‌ها تجزیه و تحلیل می‌نمایند [۶،۷،۲۶]. استفاده از داده‌های بهداشتی در پرداخت شرکت‌های بیمه، خطر تقلب و سوء استفاده را به همراه دارد که یکی از دلایل عمده افزایش روبه رشد هزینه‌های مراقبت‌های بهداشتی در دهه‌های اخیر است [۳۳-۲۷]. هزینه واقعی سالانه ناشی از تقلب و سوء استفاده در سیستم مراقبت بهداشتی نامشخص است ولی تخمین زده می‌شود که سیستم مراقبت بهداشتی، سالانه ۳ تا ۱۰ درصد هزینه اضافه بابت تقلب بپردازد [۳۷-۳۴].

کاربرد کامپیوتر در مراقبت بهداشتی افزایش یافته و نرم افزارهای کامپیوتری در زمینه‌های مالی، اداری و بالینی توسعه یافته است [۶]. امروزه تصور ارائه مراقبت بهداشتی بدون دسترسی به فناوری اطلاعات و ارتباطات ICT (Information and Communication Technology) بسیار مشکل است. ICT تقریباً در همه قسمت‌های حوزه سلامت اثر گذاشته است و با ایجاد تغییر در شیوه جمع آوری، ذخیره سازی، به اشتراک‌گذاری و استفاده از اطلاعات [۴۰-۳۸] منجر به توسعه سریع خدمات سلامت الکترونیک و موبایل در این حوزه شده است. به دلیل سهولت انتقال اطلاعات در سیستم‌های کامپیوتری و امکان تهیه نسخه چاپی متعدد و البته افزایش نیاز به استفاده از داده‌های پزشکی در مقاصد غیر درمانی، موضوع امنیت داده‌ها اهمیت ویژه‌ای یافته است [۶] و باعث گردیده امنیت و قابلیت اعتماد داده‌های الکترونیکی بیماران تبدیل به مسأله‌ای نگران کننده شود و لزوم اقدامات حفاظتی در برابر تهدیدات خارجی مثل سرقت و تهدیدات داخلی مثل دسترسی نامناسب اعضاء را هشدار دهد [۴۳،۱۹،۲۲-۴۱]. رشد استفاده از تکنولوژی در بخش مراقبت بهداشتی، مستلزم تجدیدنظر در رویه‌های امنیتی داده‌ها می‌باشد تا اداره صحیح تهدیدات اطلاعات بهداشتی در این سیستم‌ها بهتر صورت گیرد. به دلیل این که سازمان‌های مراقبت بهداشتی، جمع‌آوری، پردازش و ذخیره بیشتر اطلاعات بهداشتی را به شکل رایانه‌ای انجام می‌دهند و به منظور انتقال این اطلاعات به سایرین از سیستم‌های ارتباط از راه دور به شکل خصوصی و عمومی استفاده می‌کنند باید از وجود مکانیسم‌های کافی حفاظت از اطلاعات، مطمئن بود [۴۴]. هدف از سیاست‌های افشای داخلی و خارجی اطلاعات دستیابی به چارچوب و استانداردی برای اطمینان از در دسترس بودن اطلاعات سلامت برای کاربران نهایی به شکل مطمئن، پایدار و تحت کنترل است [۴۶،۴۷].

سازمان‌ها و گروه‌های مختلف محلی و بین المللی در زمینه تولید سیاست‌ها و استانداردهای مطرح در خصوص امنیت و حریم داده‌ها فعالیت کرده‌اند و از این میان گروهی از این استانداردها در سیستم‌های اطلاعات سلامت به کار رفته و در سطوح ملی و بین المللی مورد استفاده قرار گرفته‌اند. این مطالعه به بررسی مهمترین استانداردهای در دسترس که در زمینه امنیت و حریم داده‌ها در حوزه سلامت به کار می‌روند پرداخته و خصوصیات مدنظر آن‌ها را با یکدیگر مقایسه و نقاط ضعف و قوت هریک را بیان داشته است.

با توجه به اهمیت امنیت داده‌های حوزه سلامت، سازمان‌ها و انجمن‌هایی در سراسر دنیا در راستای ایجاد استاندارد در این

حوزه شروع به فعالیت و معرفی راهنماها و استانداردهایی کردند که در مطالعه حاضر در مورد آن‌ها بحث خواهد شد.

سازمان بین المللی استاندارد ISO (International Organization for Standardization) که در سال ۱۹۴۷ شروع به فعالیت کرد، متشکل از گروه‌های کاری متعددی است که در حوزه‌های مختلف راهنماها و استانداردهایی منتشر می‌سازد. گروه کاری TC215 (Technical Committee 215) این سازمان در زمینه اطلاعات سلامت فعالیت می‌کند که در سال ۲۰۰۴ یک راهنما به منظور الزامات حفاظت از داده‌ها منتشر کرد. این استاندارد انتقال اطلاعات سلامت را در سطح ملی تسهیل می‌کند که مشتمل بر هر دو جنبه حفاظت و امنیت می‌باشد [۴۹-۴۷]. راهنماها و استانداردهای تولید شده توسط این کمیته در جنبه‌های مختلف مرتبط با داده: شامل ذخیره سازی، انتقال، شناسه صادر کننده، نگهداری از راه دور سیستم‌های اطلاعات پزشکی و امنیت دسترسی کاربران به اطلاعات می‌باشد. فهرست (۱) استانداردهای منتشرشده در خصوص محرمانگی و امنیت داده‌ها توسط این سازمان را نشان می‌دهد.

فهرست ۱: استانداردهای منتشر شده ISO/TC251 در خصوص محرمانگی و امنیت اطلاعات [۵۰،۵۱]

عنوان استاندارد	موضوع
ISO 22857:2004	راهنمای حفاظت داده به منظور تسهیل جریان اطلاعات سلامت شخصی
ISO 20302:2006	کارت‌های سلامت: سیستم‌های شمارنده و رویه‌های ثبتی برای تعیین شناسه صادرکننده
ISO 17090-1:2008	زیرساخت کلید عمومی خلاصه‌ای از خدمات صدور گواهی دیجیتال
ISO 27799:2008	مدیریت امنیت در سلامت با استفاده از استاندارد ISO/IEC 27002
ISO/TR 11633-1:2009	مدیریت امنیت اطلاعات برای نگهداری از راه دور وسایل و سیستم‌های اطلاعات پزشکی
ISO/TR 11633-2:2009	مدیریت امنیت اطلاعات برای نگهداری از راه دور وسایل و سیستم‌های اطلاعات پزشکی
ISO/TS 13606-4:2009	ارتباطات پرونده‌های الکترونیک سلامت - قسمت۴ – امنیت
ISO/TS 21547:2010	نیازمندی‌های امنیتی ذخیره سازی پرونده الکترونیک سلامت
ISO/TR 21548:2010	نیازمندی‌های امنیتی ذخیره سازی پرونده الکترونیک سلامت
IEC/TR 80001-2-2:2012	راهنمای نیازهای امنیتی ارتباطات وسایل پزشکی

در دسامبر ۲۰۰۴ پنج شرکت بزرگ فعال در زمینه کارت‌های اعتباری، سیاست‌های خود را با هم یکی نموده و استاندارد PCI-DSS را تولید کردند. این استاندارد برای افزایش کنترل بر داده‌های صاحب کارت و کاهش تقلب و افشای اطلاعات کارت اعتباری به وجود آمده است. انجمن استانداردهای امنیت PCI یک انجمن عمومی است که در سال ۲۰۰۶ شروع به کار کرد و مسؤولیت آن توسعه، مدیریت، آموزش و اطلاع‌رسانی در مورد استانداردهای امنیت PCI است که مشتمل است بر: استانداردهای امنیت داده (PCI-DSS)، امنیت داده‌های درخواست پرداخت و امنیت تبادل PIN (Payment Application Data Security Standard) [۲۷،۵۲،۵۳]. استاندارد منتشره از سوی این انجمن بر شش پایه اصلی: ایجاد شبکه امن، حفاظت از اطلاعات کارتخوان‌ها، برقراری برنامه مدیریت آسیب پذیری، کنترل دسترسی، نظارت و آزمایش شبکه و سیاست‌گذاری امنیت اطلاعات استوار شده است [۵۴].

در سال ۱۹۹۶ قانون قابلیت جابه‌جایی و پاسخگویی بیمه سلامت HIPAA (Health Insurance Portability and Accountability) توسط وزارت بهداشت و خدمات انسانی آمریکا DHHS (Department of Health and Human Services) تصویب شد. این قانون به منظور کاهش هزینه‌ها و بار اجرایی مراقبت بهداشتی با پذیرش انتقال الکترونیک تراکنش‌های اداری و مالی به شکل استاندارد می‌باشد که منجر به حاکمیت محرمانگی اطلاعات بهداشتی بر ارائه دهندگان خدمت گردید. HIPAA اولین قانون، راهنما و استاندارد جامع دولت فدرال در زمینه امنیت و محرمانگی در پشتیبانی از استانداردسازی تبادل داده می‌باشد [۱۰،۵۵] و جزئیات زیادی از امنیت را تحت پوشش قرار می‌دهد که عبارت است از: امنیت اداری، فیزیکی، فنی، نیازهای سازمانی، سیاست-

گذاری‌ها و رویه‌ها و مستندسازی که هر کدام به طور جزء به جزء نیز تشریح شده‌اند [۵۶].

علاوه بر سه استاندارد مذکور، سازمان‌ها و انجمن‌های دیگری نیز در سطح جهانی یا ملی دست به تولید استانداردها و راهنماهایی در زمینه امنیت و محرمانگی اطلاعات حوزه سلامت زده‌اند که به دلیل عدم دسترسی رایگان به مستندات آن سازمان‌ها فقط به معرفی آن‌ها اکتفا می‌شود.

در اروپا در سال ۱۹۹۷ کمیته استانداردسازی اروپا برای امنیت و محرمانگی انفورماتیک پزشکی (CENTC251) پیش نویسی در مورد رمزنگاری اطلاعات سلامت در شبکه‌ها ارایه کرد. این استاندارد منسوب به سازمان استانداردسازی سوئد HSS (Swedish Healthcare Standardization Organization) می‌باشد که توسط کار گروه شش این کمیته CENTC251/WG6(TC (Technical Committee 251 is responsible for Medical Informatics) پیشنهاد شد [۳۹،۴۰]. فهرست (۲) استانداردهای منتشرشده در خصوص محرمانگی و امنیت داده‌ها توسط این کار گروه را نشان می‌دهد:

فهرست ۲: استانداردهای منتشر شده CEN/TC251 در خصوص محرمانگی و امنیت اطلاعات [۵۷]

عنوان استاندارد	موضوع
CR 13694:1999	استانداردهای کیفیت نرم افزار مرتبط با ایمنی و امنیت برای مراقبت سلامت
CR 14301:2002	چارچوب حفاظت از امنیت ارتباطات مراقبت سلامت
CR 14302:2002	چارچوب نیازهای امنیتی دستگاه‌های متناوب متصل شونده
EN 14484:2003	انتقال بین المللی داده‌های سلامت شخصی تحت الزام حفاظت اطلاعات اروپا – سیاست امنیت سطح بالا
EN 12251:2004	شناسایی امن کاربر برای مدیریت مراقبت سلامت و امنیت تأیید و تصدیق هویت از طریق کلمه عبور
CEN/TR 15300:2006	چارچوبی برای مدل سازی قانونی سیاست‌های امنیت مراقبت سلامت
EN 13606-4:2007	ارتباطات پرونده الکترونیک سلامت – جزء ۴ – امنیت
EN ISO 27799:2008	مدیریت امنیت اطلاعات در سلامت با استفاده از ISO/IEC 27002 (ISO 27799:2008)

در سال ۱۹۹۸ تحت هدایت انجمن مدیریت و سیستم‌های اطلاعات مراقبت بهداشتی HIMSS (Healthcare Information Management & Systems Society) و انجمن رادیولوژی شمال آمریکا RSNA (Radiological Society of North America) مؤسسه یکپارچه سازی مراقبت سلامت IHE (Integrating the Healthcare Enterprise) با هدف بهبود و اصلاح روش سیستم‌های کامپیوتری در به اشتراک گذاری اطلاعات بسیار مهم مراقبت بهداشتی تأسیس گردید. IHE شامل: پزشکان متخصص و عمومی، مدیران، سازمان‌های استاندارد، افراد ماهر در زمینه فناوری اطلاعات و فروشندگان می‌باشد. کمیته فنی زیرساخت اطلاعات IHE شمای یکپارچگی امنیت و محرمانگی را توسعه می‌دهد [۵۸].

انجمن آزمایش و مواد آمریکا ASTM (American Society for Testing and Materials) در سال ۱۸۹۸ تأسیس شد و ابتدا در حوزه صنعت راه آهن شروع به ارائه استاندارد کرد. در سال ۲۰۰۱ پسوند بین المللی گرفت تا نشان‌دهنده جهانی بودن استانداردهای منتشره شده آن باشد [۵۹]. کمیته E31 این انجمن از سال ۱۹۷۰ بر روی گسترش استانداردهای انفورماتیک مراقبت سلامت شامل: معماری، محتوا، ذخیره سازی، امنیت، محرمانگی، کارایی و ارتباطات اطلاعات به کار رفته در مراقبت سلامت و تصمیم سازی مراقبت سلامت فعالیت می‌کند [۶۰،۶۱] و زیر کمیته‌های E31.17، E31.20، E31.25 در مورد مدیریت داده مراقبت سلامت، قابلیت اعتماد و محرمانگی به فعالیت می‌پردازد [۵۵،۶۲،۶۳]. فهرست(۳) استانداردهای منتشرشده در خصوص محرمانگی و امنیت داده‌ها توسط این کمیته را نشان می‌دهد:

فهرست ۳: استانداردهای ASTM E31 درخصوص محرمانگی و امنیت اطلاعات [۶۳،۶۴]

عنوان استاندارد	موضوع
E1762-95(2003)	راهنمای استاندارد برای تأیید الکترونیک اطلاعات مراقبت سلامت
E1985-98(2003)	راهنمای استاندارد برای تصدیق و مجوز کاربر
E1986-98(2005)	راهنمای استاندارد برای اولویت دسترسی به اطلاعات سلامت
E1869-04	راهنمای استاندارد برای اصول محرمانگی، حریم خصوصی، دسترسی و امنیت داده برای مراقبت سلامت شامل پرونده‌های الکترونیک سلامت
E1988-98	راهنمای استاندارد برای آموزش افرادی که به اطلاعات سلامت دسترسی دارند
E2174-01	تعیین استاندارد برای ممیزی و افشای گزارشات استفاده از سیستم‌های اطلاعات
E1869	راهنما برای اصول قابلیت اعتماد، محرمانگی، دسترسی و امنیت داده برای اطلاعات سلامت شامل پرونده کامپیوتری بیمار
E1987	راهنمای استاندارد برای حقوق افراد درمورد اطلاعات سلامت
PS115-99	تعیین استاندارد موقت برای ممیزی و افشای گزارشات استفاده از سیستم‌های اطلاعات
E1902	راهنمای استاندارد برای مدیریت قابلیت اعتماد و امنیت املاء، ترجمه و پرونده‌های سلامت ترجمه شده
PS100-97	تعیین استاندارد موقت برای تصدیق اطلاعات مراقبت سلامت با استفاده از امضای دیجیتال
PS101-97	تعیین استاندارد موقت برای یک چارچوب امنیت فنی برای انتقال و ذخیره اطلاعات سلامت
PS102-97	تعیین استاندارد موقت برای امنیت اینترنت و اینترانت
E2017-99	راهنمای استاندارد برای اصلاح اطلاعات سلامت

هیأت استانداردهای فناوری اطلاعات سلامت HITSP (Health Information Technology Standards Panel) یک هماهنگ کننده ملی است که کار آن ایجاد مشارکت و همکاری بین قسمت‌های خصوصی و عمومی در جهت هماهنگ سازی استانداردهای موجود به منظور گسترش قابلیت تعامل نرم‌افزارهای کاربردی مراقبت بهداشتی است تا اطلاعات را در سطح محلی، منطقه‌ای یا ملی در شبکه اطلاعات سلامت آمریکا تبادل کنند.

در ژاپن و شرق آسیا انجمن سیستم‌های اطلاعات سلامت ژاپن JAHIS (Japanese Association of Healthcare Information Systems) از سال ۱۹۹۴با عضویت ۱۷۴ شرکت شروع به کار کرد و در حال حاضر ۲۴۳ عضو دارد که در زمینه سیستم‌های اطلاعاتی بهداشتی، مراقبت پزشکی و خدمات رفاه اجتماعی فعالیت می‌کند. کمیته کیفیت و امنیت این انجمن با هدف دستیابی به راهنماهایی در مورد کیفیت و امنیت سیستم‌های اطلاعات پزشکی شروع به فعالیت کرد که منجر به رسیدن به استاندارد امنیت نرم‌افزار ISO/IEC و IEC آزمایشی برای امنیت اساسی سیستم‌های الکترونیک قابل برنامه‌ریزی گردید. همچنین استانداردی را با نام کامل - MDS A 001 0017 برای ضبط تصاویر پزشکی با رعایت اصول امنیت، سازگاری و تکثیرپذیری تولید کرد [۶۵].

روش

در این مطالعه مروری ابتدا با استفاده از موتور جستجوی گوگل ترکیبات مختلف کلیدواژه‌های Health, Data, Security, Standard Information System, Medicine مورد جستجو قرار گرفت. از مقالات به دست آمده، تاریخچه استانداردهای مورد استفاده در داده‌های حوزه سلامت و لزوم استفاده از این استانداردها و میزان کاربرد استانداردها در سطح دنیا مطالعه گردید. سپس با توجه به تعدد استانداردها، پرکاربردترین و معتبرترین آن‌ها انتخاب شدند. در مرحله بعد، متن کامل استانداردهای انتخابی تهیه شد و مورد مطالعه و بررسی قرار گرفت و خصوصیات موردنظر هر استاندارد استخراج گردید. اجتماع این خصوصیات تبدیل به چک لیست خصوصیات جزئی گردید که به منظور تسهیل مقایسه و بررسی، خصوصیات هم‌خانواده در دسته بندی کلی در یک گروه قرار گرفتند. در نهایت با کمک چک لیست حاصله سه استاندارد انتخابی با یکدیگر مقایسه و نقاط ضعف و قوت هر یک مورد بحث و بررسی قرار گرفت.

نتایج

براساس مطالعات انجام شده در مورد استانداردهای ISO 27799:2008 و HIPAA وPCI-DSS پس از استخراج ویژگی‌های مربوط به استانداردهای امنیت داده‌ها این ویژگی‌ها به ۸ گروه کلی تقسیم شدند که مجموعاً دارای ۲۲ زیرگروه می‌باشند [۵۴،۶۶،۶۷]. این گروه‌ها عبارت بودند از:

۱) اطلاعات
۲) آموزش
۳) دسترسی
۴) رمزنگاری

۵) سرور شبکه
۶) سیستم عامل
۷) شبکه
۸) تلفن همراه (Mobile)

و ۲۲ زیر گروه نیز عبارتند از:

۱،۱) ارزیابی امنیت اطلاعات
۲،۱) آموزش درحوزه امنیت
۳،۱) کنترل دسترسی فیزیکی
۳،۲) پیشگیری از نفوذ نرم افزارهای مخرب
۳،۳) شناسایی افراد با استفاده از شناسه‌های بیومتریک
۴،۱) فناوری های رمزگذاری درذخیره سازی
۴،۲) استفاده از الگوریتم‌های Hash در برنامه‌های کاربردی
۴،۳) امضای دیجیتال
۴،۴) رمزگذاری با استفاده از کلید نامتقارن (کلید عمومی و کلید خصوصی)
۵،۱) امنیت سرور
۵،۲) مدیریت گزارش‌های امنیتی (log)
۶،۱) امنیت سیستم عامل
۷،۱) تنظیمات امنیت شبکه
۷،۲) به کارگیری SSL (Secure Sockets Layer)
۷،۳) به کارگیری VPN (Virtual Private Network)
۷،۴) امنیت در استفاده از فناوری رادیو شناسه (RFID)
۷،۵) امنیت شبکه‌های بی سیم IEEE 802.11i
۷،۶) امنیت در ارائه سرویس تحت وب
۷،۷) امنیتDNS (Domain Name System)
۷،۸) به کارگیری پست الکترونیک
۷،۹) استفاده از دیواره آتش (Firewall) و تنظیمات آن
۸،۱) امنیت تلفن همراه

سپس استانداردهای انتخابی باتوجه به چک لیست تهیه شده‌ای که شامل کلیه موارد فوق الذکر بود، مورد بررسی قرار گرفتند و اطلاعات لحاظ شدن موارد مذکور در مورد هرسه استاندارد، در چک لیست وارد گردید.

نتایج بررسی سه استاندارد ISO 27799:2008، HIPAA، PCI-DSS، در جدول (۱) آمده است.

جدول ۱: نتایج بررسی سه استاندارد ISO 27799:2008، HIPAA، PCI-DSS

ردیف	گروه	زیرگروه(ویژگی)	HIPAA	ISO 27799:2008	PCI-DSS
۱	اطلاعات	ارزیابی امنیت اطلاعات	✓	✓	✓
۲	آموزش	آموزش در حوزه امنیت	✓	✓	✓
۳	دسترسی	کنترل دسترسی فیزیکی	✓	✓	✓
۴	دسترسی	پیشگیری از نفوذ نرم افزارهای مخرب	✓	✓	✓
۵	دسترسی	شناسایی افراد با استفاده از شناسه های بیومتریک	✓	✓	✓
۶	رمزنگاری	فناوری های رمزگذاری در ذخیره سازی	✓	✓	✓
۷	رمزنگاری	استفاده از الگوریتم‌های Hash در برنامه های کاربردی	–	✓	✓
۸	رمزنگاری	امضای دیجیتال	–	✓	–
۹	رمزنگاری	رمزگذاری با استفاده از کلید نامتقارن (کلیدعمومی و کلید خصوصی)	✓	✓	✓
۱۰	سرورشبکه	امنیت سرور	✓	✓	✓
۱۱	سرورشبکه	مدیریت گزارش های (log) امنیتی	✓	✓	✓
۱۲	سیستم عامل	امنیت سیستم عامل	✓	–	–
۱۳	شبکه	تنظیمات امنیت شبکه	✓	✓	✓
۱۴	شبکه	به کارگیری SSL	✓	✓	✓
۱۵	شبکه	به کارگیری VPN	✓	✓	✓
۱۶	شبکه	امنیت در استفاده از فناوری رادیو شناسه (RFID)	–	–	✓
۱۷	شبکه	امنیت شبکه های بی‌سیم IEEE 802.11i	–	✓	✓
۱۸	شبکه	امنیت در ارائه سرویس تحت وب	✓	✓	✓
۱۹	شبکه	امنیت DNS	–	–	✓
۲۰	شبکه	به کارگیری پست الکترونیک	✓	✓	✓
۲۱	شبکه	استفاده از دیواره آتش (Firewall) و تنظیمات آن	✓	✓	✓
۲۲	همراه	امنیت تلفن همراه	–	–	✓

در گروه امنیت اطلاعات، ویژگی ارزیابی امنیت اطلاعات مطرح گردید که در هر سه استاندارد مورد توجه قرار گرفته بود. هرسه استاندارد به گروه آموزش که زیرگروه آموزش در حوزه امنیت را در برداشت و بر آموزش نیروی انسانی تأکید دارد نیز توجه داشتند. در گروه دسترسی، سه ویژگی کنترل دسترسی فیزیکی، پیشگیری از نفوذ نرم افزارهای مخرب و شناسایی افراد با استفاده از شناسه‌های بیومتریک قرار داشتند که هر سه این استانداردها، همه ویژگی این گروه را مدنظر داشتند. در گروه رمز

نگاری، چهار ویژگی که عبارت بودند از: فناوری‌های رمزگذاری در ذخیره سازی، استفاده از الگوریتم‌های Hash در برنامه‌های کاربردی، امضای دیجیتال و رمزگذاری با استفاده از کلید نامتقارن (کلید عمومی و کلید خصوصی) که ISO 27799:2008 به هر چهار مورد توجه داشته ولی HIPAA فقط به دو مورد فناوری‌های رمزگذاری در ذخیره سازی و رمزگذاری با استفاده از کلید نامتقارن (کلید عمومی و کلید خصوصی) توجه داشته و PCI-DSS، به سه مورد فناوری‌های رمزگذاری در ذخیره سازی، استفاده از الگوریتم‌های Hash در برنامه‌های کاربردی و رمزگذاری با استفاده از کلید نامتقارن (کلید عمومی و کلید خصوصی) را مورد توجه قرار داده است. در گروه سرور شبکه، دو ویژگی امنیت سرور و مدیریت گزارش‌های (log) امنیتی بودند که هر سه استاندارد آن‌ها را مدنظر قرار داده بودند. در گروه سیستم عامل، تنها ویژگی امنیت سیستم عامل بررسی شد که فقط HIPAA این مورد را منظور کرده بود. در گروه شبکه، ۹ ویژگی مورد بررسی قرار گرفت که عبارت بودند از: تنظیمات امنیت شبکه، به‌کارگیری SSL، به کارگیری VPN، امنیت در استفاده از فناوری رادیوشناسه (RFID)، امنیت شبکه‌های بی‌سیم IEEE 802.11i، امنیت در ارائه سرویس تحت وب، امنیت DNS، به کارگیری پست الکترونیک و استفاده از دیواره آتش (Firewall) و تنظیمات آن. از این موارد، به ویژگی امنیت در استفاده از فناوری رادیو شناسه (RFID) و امنیت DNS نیز فقط استاندارد PCI-DSS اشاره کرده بود و دو استاندارد دیگر آن را در نظر نگرفته بودند و امنیت شبکه‌های بی‌سیم IEEE 802.11i را نیز دو استاندارد ISO 27799:2008 و PCI-DSS منظور کرده بودند، این در حالی است که HIPAA اشاره‌ای به آن نکرده بود. در گروه همراه دو ویژگی امنیت تلفن همراه دیده می‌شد که PCI-DSS ویژگی امنیت تلفن همراه را در نظر گرفته بود در حالی که HIPAA و ISO 27799:2008 آن را در نظر نگرفته بودند.

بحث و نتیجه‌گیری

با توجه به ویژگی‌های استانداردهای PCI-DSS، HIPAA و ISO 27799:2008 که در جدول ۱ گفته شد به نظر می‌رسد که سه استاندارد مقایسه شده، در زمینه رعایت ضروریات حوزه امنیت در گروه‌های اطلاعات، آموزش، دسترسی و سرور شبکه در یک سطح قرار دادند و هر سه استاندارد بیشترین تمرکز را در این چهار گروه خصوصیت قرارداده‌اند اما تفاوت‌هایی نیز با یکدیگر دارند [۵۴،۶۶،۶۷].

ISO 27799:2008 در زمینه رمزنگاری، قوی‌تر از PCI-DSS و HIPAA بوده و با توجه بیشتر در به کار گیری امضای دیجیتال به منظور افزایش قدرت رمزنگاری داده‌ها برتر از دو استاندارد دیگر شده است. در این زمینه، PCI-DSS از HIPAA استاندارد مناسب‌تری دارد زیرا در برنامه‌های کاربردی، استفاده از الگوریتم Hash را در نظر گرفته است و از این‌رو HIPAA با در نظر نگرفتن الگوریتم Hash و امضای دیجیتال در زمینه رمزنگاری داده‌ها ضعف عمده‌ای دارد. در زمینه نکات ایمنی در مورد سیستم عامل، HIPAA برتر از دو استاندارد دیگر است و ISO 27799:2008 و PCI-DSS در این زمینه نکات مهمی را در نظر نگرفته‌اند. در زمینه شبکه، استاندارد PCI-DSS قوی‌تر از سایرین بوده زیرا با درنظر گرفتن امنیت در استفاده از فناوری رادیوشناسه و همچنین امنیت DNS بیش از استانداردهای HIPAA و ISO27799:2008 در مورد امنیت شبکه مورد اطمینان می‌باشد و ISO 27799:2008 که امنیت در استفاده از فناوری رادیو شناسه و همچنین امنیت DNS را مدنظر قرار نداده اگرچه به امنیت شبکه‌های بی‌سیم توجه نموده است از HIPAA استاندارد مناسب‌تری است و از طرف دیگر HIPAA که هیچ یک از موارد امنیت در استفاده از فناوری رادیو شناسه و امنیت DNS و امنیت شبکه‌های بی‌سیم را مورد توجه قرار نداده ضعیف‌ترین استاندارد در حوزه امنیت شبکه می‌باشد. در زمینه تلفن همراه و دستیار دیجیتال شخصی نیز فقط استاندارد PCI-DSS موضوع امنیت تلفن همراه را در نظر گرفته و ISO 27799:2008 و HIPAA به این مورد توجه نکرده‌اند. تمایز این سه استاندارد به این صورت است که HIPAA بر سیستم عامل، ISO 27799:2008 بر رمزنگاری و PCI-DSS بر امنیت تلفن همراه تمرکز دارد. [۵۴،۶۷]. در زمینه شبکه، PCI-DSS قدرت مناسبی چه در زمینه شبکه–های بی‌سیم و چه در زمینه شبکه‌های کابلی دارا می‌باشد.

با توجه به این که در بررسی حاضر، از گروه بندی در نظر گرفته شده یا استانداردها جهت مقایسه بین آن‌ها استفاده شده، فقط می‌توانستیم وجود یا عدم وجود یک خصوصیت را در استاندارد ها با یکدیگر مقایسه کنیم. در صورتی که اگر شاخص‌هایی به صورت مستقل و علمی وجود داشت، این مقایسه به شکل کامل‌تری و با در نظر گرفتن میزان قدرت استانداردها در هر زمینه مورد بررسی انجام می‌پذیرفت و نتایج مناسب‌تری به دست می‌آمد.

با توجه به این که برتری کلی به هیچ یک از سه استاندارد فوق الذکر نمی‌توان داد لذا با توجه به زیرساخت محل اجرای پروژه، موقعیت و مکان مورد استفاده می‌توان از استانداردی که در آن زمینه قوی‌تر است استفاده کرد. مثلاً اگر می‌خواهیم برای سامانه‌ای که قرار است برروی تلفن همراه استفاده شود از یکی از این سه استاندارد استفاده شود، PCI-DSS توصیه می‌شود که در استانداردش به امنیت در زمینه تلفن همراه نیز توجه خاص داشته است و یا مثلاً در صورتی که زیرساخت شبکه، بی سیم است بهتر است از ISO 27799:2008 یا PCI-DSS استفاده شود. چنانچه سیستم عاملی روی سخت افزارهایمان نصب است که امنیت آن برایمان سؤال برانگیز است، بهتر است از HIPAA کمک گرفته شود که درزمینه امنیت سیستم عامل به طور خاص استاندارد دارد. استفاده از استاندارد ترکیبی که ویژگی‌های هر سه استاندارد مورد بررسی را دارا می‌باشد بعنوان امن‌ترین روش و البته سخت‌ترین روش می‌تواند مدنظر قرار گیرد. به این ترتیب ضعف‌های استانداردها همپوشانی شده و امنیت حداکثری برای پروژه تضمین می‌گردد.

References

1. Fichman RG, Kohli R, Krishnan R. The role of information systems in healthcare: current research and future trends. Information Systems Research. 2011;22(3):419-28.
2. Bauer J, Polakoff P. The growing importance of data in healthcare. Executive Briefing & Exchange. 2007;3(2).
3. Appari A, Johnson ME. Information security and Privacy in healthcare: current state of research. International Journal of Internet and Enterprise Management. 2010;6(4):279-314.
4. Haux R. Health information systems - past, present, future. Int J Med Inform. 2006;75(3-4):268-81.
5. Council of Europe. Training strategies for health. Information Systems: Council of Europe Publishing; 1996.
6. Huffman EK. Health Information Management. Berwyn, IL: Physicians' Record Company;1994.
7. Abdelhak M, Grostick S, Hanken MA, Jacobs E. Health information: management of a strategic resource: 4th ed. Saunders/Elsevier; 2011.
8. Richards-Kortum R. Biomedical engineering for global health. USA: Cambridge University Press; 2010.
9. Engstrom P. Technology outpaces privacy protection. Thursday; 2008. [cited 2013 Sep 3]. Available from: http://www.curetoday.com/publications/cure/2008/summer2008/Technology-Outpaces-Privacy-Protection
10. Houghton J. Information technology and the revolution in healthcare. 2002. [cited 2013 Sep 2]. http://www.eldis.org/vfile/upload/1/document/1201/Information%20Technology%20and%20Revolution%20in%20Healthcare.pdf
11. Nesbitt A, Kemeny C, Broshy E, Wurster T. Managing for a wired health care industry. IN VIVO: The Business and Medicine Report; 1996.
12. Olukunle O. Assessing innovative ICT for health information system in African rural communities. eldis; 2009.
13. Cotturri G, Inglese SA, Moro G, Roffiaen C, Scattolon C. European charter of patients' rights. Rome: Active Citizenship Network; 2002.
14. Manson JE, Greenland P, LaCroix AZ, Stefanick ML, Mouton CP, Oberman A, et al. Walking compared with vigorous exercise for the prevention of cardiovascular events in women. The New England Journal of Medicine. 2002;347(10):716-25.
15. The Office for Civil Rights of the U.S. Department of Health and Human Services. Protecting Your Privacy and Security [cited 2013 Sep 3]. Available from: http://www.healthit.gov/sites/default/files/pdf/health-information-privacy-and-security.pdf.
16. Your health information privacy: The Office for Civil Rights of the U.S. Department of Health and Human Services; 2013 [cited 2013 Sep 3]. Available from: http://www.hhs.gov/ocr/privacy/hipaa/understanding/consumers/consumer_rights.pdf.
17. Confidentiality and Privacy- Personal Health Information Toronto: College of Nurses of Ontario; 2009.
18. Protecting Your Privacy & Security Your Health Information Rights: The Office for Civil Rights of the U.S. Department of Health and Human Services; [cited 2013 Sep 3]. Available from: http://www.healthit.gov/patients-families/your-health-information-rights.
19. Hiller J, McMullen MS, Chumney WM, Baumer DL. Privacy and security in the implementation of health information technology (electronic health records): US and EU compared. BUJ Sci & Tech L. 2011;17:1.
20. Collst G, Duquenoy P, George C, Hedström K, Kimppa, K, Mordini E. ICT in medicine and health care: assessing social, ethical and legal issues. Social Informatics: An Information Society for all? In Remembrance of Rob Kling: US: Springer; 2006.
21. Rudowski R. Impact of Information and Communication Technologies (ICT) on Health Care. [cited 2013 Sep 3]. Available from: http://www.map.uniroma2.it/digital_evolution/papers/rudowski_paper.pdf: 2008.
22. Chetley A, Davies J, Trude B, McConnell H, Ramirez R. Improving health, connecting people: the role of ICTs in the health sector of developing countries. This paper is part of a study commissioned by the info Dev program Grant no; 2006.1-65.
23. Wilson I, Mahdavy E. ICT in Healthcare better care, sustainable costs: Orange and European policy; 2013. [cited 2013 Sep 3]. Available from:

http://www.orange.com/en/content/download/11116/241913/version/4/file/ICT+in+healtcare_Orange.pdf
24. World Health Organization (WHO). Patients' rights. [cited 2013]. Available from: http://www.who.int/genomics/public/patientrights/en/.
25. National Association of Citizens Advice Bureaux. NHS patients' rights. [cited 2013 Sep 3]. Available from: http://www.adviceguide.org.uk/england/healthcare_e/healthcare_nhs_healthcare_e/nhs_patients_rights.htm.
26. Wager KA, Lee FW, Glaser JP. Health care information systems: a practical approach for health care management. 3th ed. Wiley Jossey-Bass; 2103.
27. Fisher E. The Impact of Health Care Fraud on the United States Healthcare System. School of Public and Environmental Affairs. 2008; 2(4):1-4.
28. Staman J. Health Care Fraud and Abuse Laws Affecting Medicare and Medicaid: An Overview.: Congressional Research Service; 2010. [cited 2013 Sep 3]. Available from: https://www.fas.org/sgp/crs/misc/RS22743.pdf
29. AAOMS Committee on Healthcare & Advocacy. A Review of Healthcare Fraud and Abuse in America. 2011.
30. Kökoğlu F, Leventoğlu A, Erdemoglu AK. Dorsal Sural Nerve Conduction Studies in Patients with Early Diabetic Neuropathy and Its Relations with plasma adiponectin and hs-CRP Levels. Journal of Neurological Sciences (Turkish). 2009;26(4):404-15.
31. Schunkert H, Konig IR, Kathiresan S, Reilly MP, Assimes TL, Holm H, et al. Large-scale association analysis identifies 13 new susceptibility loci for coronary artery disease. Nat Genet. 2011;43(4):333-8.
32. StevensWS. Health Insurance: Current Issues and Background. USA: Nova Science; 2003.
33. Chaikind HR, Redhead S, HearneJ, Stone J, Like B, Franco C. The Health Insurance Portability and Accountability Act (HIPAA). Overview and Analyses: NewYork: Nova Science; 2004.
34. Rudman WJ, Eberhardt JS, Pierce W, Hart-Hester S. Healthcare fraud and abuse. Perspectives in health information management/AHIMA, American Health Information Management Association. Perspect Health Inf Manag. 2009; 6.
35. Lind KD (AARP Public Policy Institute) Attacking Waste, Fraud, and Abuse in Health Reform. Washington DC; 2011. [cited 2013 Sep 3]. http://assets.aarp.org/rgcenter/ppi/health-care/fs186-fraud.pdf
36. Goldman TR, King KM, Sparrow MK, Agres, T, Dentzer S. Health Policy Brief. [cited 2013 Sep 3]. Available from: 2012.http://healthaffairs.org/healthpolicybriefs/brief_pdfs/healthpolicybrief_72.pdf
37. American Health Information Management Association (AHIMA). A study of health care fraud and abuse: Implications for professionals managing health information; 2010. [cited 2013 Sep 3]. Available from: http://www.ahimafoundation.org/downloads/pdfs/Fraud%20and%20Abuse%20-%20final%2011-4-10.pdf
38. Rodrigues J. Health information systems: concepts, methodologies, tools and applications. 1th ed. USA: IGI Global; 2009.
39. Kabashiki IR. Bumps in the road to better health care: Xlibris Corporation; 2012.
40. Chetley A, Davies J, Trude B, McConnell H, Ramirez R, Shields T, et al. Improving Health, Connecting People: The Role of ICTs in the Health Sector of Developing Countries: InfoDev; 2006 [cited 2013 Sep 3] Available from: http://www.infodev.org/infodev-files/resource/InfodevDocuments_84.pdf
41. Tamas P, Voyiatzis AG, Anastasiadou D, Jovanovich Z. SWOT Analysis on the theme ICT for Health. Hungary: 2012. [cited 2013 Sep 3]. Available from: http://forsee.eu/documents/Montenegro_OC_FORSEE_SWOT_Analysis_eHealth_5p_v1_short_161.pdf
42. British Medical Association(BMA). Confidentiality and disclosure of health information tool kit. [cited 2013 Sep 3]. Available from: http://bma.org.uk/-/media/files/pdfs/practical%20advice%20at%20work/ethics/confidentialitytoolkit_full.pdf.
43. Kelly T. Public interest disclosure policy and procedure. MiddleSex University; 2008.
44. Clayton PD, Boebert W, Defriese G, Dowell S, Fennell M, Frawley K, et al. For the record: protecting electronic health information Washington DC: National Academy Press;1997.
45. Disclosure Policy Canada: Export Development Canada; 2010 [cited 2013 Sep 3]. Available from: http://www.edc.ca/EN/AboutUs/Disclosure/Documents/disclosure-policy.pdf.
46. Government of Western Australia Department of Health. Information Access and Disclosure Policy. [cited 2013 Sep 3]. Available from: http://www.health.wa.gov.au/CircularsNew/attachments/632.pdf.
47. The Government of the Hong Kong Special Administrative Region. An overview of information security standards Hong Kong: infosec; 2008. [cited 2013 Sep 3]. Available from: http://www.infosec.gov.hk/english/technical/files/overview.pdf.
48. Thomson SM. A standard-based security model for health information systems [dissertation]. Nelson: Mandela Metropolitan University; 2008.
49. Quinn J. HL7: Who, What & What's New. cited 2013 Sep 3]. Available from: https://www2.uef.fi/documents/1020024/1430597/JQ-2011-05-23_HL7_Finland__HL7_Who_What_and_What_s_New.pdf/527a359f-a337-4569-a29f-30af7564c5cf
50. California Department of Mental Health. EHR and PHR standards and requirements. [cited 2013 Sep 3]. Available from: http://www.countyofplumas.com/DocumentCenter/Home/View/3120
51. International Organization for Standardization. Health security; [cited 2013 Sep 3]. Available from:

http://www.iso.org/iso/home/search.htm?qt=health+security&published=on&active_tab=standards&sort_by=rel.
52. PCI Security Standards Council. PCI-DSS History; 2010. [cited 2013 Sep 3]. Available from: https://www.pcisecuritystandards.org/organization_info/index.php.
53. Wikipedia. Payment Card Industry Data Security Standard [cited 2013 Sep 3]. Available from: http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard.
54. PCI Security Standards Council. Payment Card Industry (PCI) Data Security Standard; 2010 [cited 2013 Sep 3]. Available from: https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf.
55. Waegemann CP. Confidentiality and Security for e-Health; 2003 [cited 2013 Sep 3]. Available from: https://www.itu.int/itudoc/itu-t/workshop/e-health/s5-05.pdf
56. HIPAA Administrative Simplification Statute and Rules Department of Health and Human Services Office for Civil Rights; 2006. [cited 2013 Sep 3]. Available from: http://www.hhs.gov/ocr/privacy/hipaa/administrative/privacyrule/adminsimpregtext.pdf
57. European Committee for Standardization. CEN/TC 251, Technical Bodies [cited 2013 Sep 3]. Available from: www.cen.eu/CEN/Sectors/TechnicalCommitteesWorkshops/CENTechnicalCommittees/Pages/Standards.aspx?param=6232&title=CEN/TC+251.
58. Witting K, Moehrke J. Health Information Exchange: Enabling Document Sharing Using IHE Profiles; 2012 [cited 2013 Sep 3]. http://www.ihe.net/Technical_Framework/upload/IHE_ITI_White-Paper_Enabling-doc-sharing-through-IHE-Profiles_Rev1-0_2012-01-24.pdf.
59. Wikipedia. ASTM International [cited 2013 Sep 3]. Available from: http://en.wikipedia.org/wiki/astm_international.
60. ASTM. ASTM International Technical Committee E31 on Healthcare Informatics. [cited 2013 Sep 3]. Available from: http://www.astm.org/COMMIT/SUBCOMMIT/E3125.htm.
61. Lovorn J. ASTM E31 Security Standards. National Committee on Vital and Health Statistics; 2013.
62. ASTM International Standards Worldwide. ASTM International Technical Committee E31 on Healthcare Informatics; 1970. [cited 2013 Sep 3]. Available from: http://www.astm.org/e31mail.htm.
63. ASTM. ASTM Healthcare Informatics Standard. 2003.[cited 2013 Sep 3]. Available from: http://www.astm.org/SNEWS/JULY_2003/hi_jul03.htm
64. Amatayakul M. Managing Information Privacy & Security in Healthcare Setting Standards in Healthcare Information. 2007.
65. Kanai T. Home-based Elderly People Support Information System. JAHIS News; 1996.
66. Gikas C. A General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards. Information Security Journal: A Global Perspective. 2010;19(3):132-41.
67. Health informatics - Information security management in health using ISO/IEC 27002 (ISO 27799:2008). British Standard Institution; 2008.

Review Article

Journal of Health and Biomedical Informatics
Medical Informatics Research Center
2015; 2(3): 184-194

A Comparative Study of Three Standards of Data Security in Health Systems

Hamid Moghadesi [1], Mehdi Ghaeme Mohammad[2]*

• **Received:** 16 Jul, 2015 • **Accepted:** 21 Sep, 2015

Introduction: The increasing influence of ICT on health and changing information systems to electrical form makes using the information, data transmission, and also preparation printouts of information so easy that the importance of internal and external disclosure policy, data security, and confidentiality standards in these systems have been doubled.

Method: At the first, in this review study research, all the combinations of key words were searched, then the history and importance of the health data security standards were studied. So the most prevalent and reliable standards were selected to perform the full text. For the next step the researchers extracted the properties which were used to be compared with the selected standards and finally the comparison was discussed.

Results: PCI-DSS, HIPAA, and ISO-27799:2008 properties were classified in 8 groups and 22 subgroups. ISO-27799:2008 was attended to all properties in Encryption group, but HIPAA was just attended to Encryption in storage, and asymmetric key, and PCI-DSS was considered on Encryption in storage, using Hash algorithm and use of asymmetric key. Operation system security was considered only in HIPAA. Only PCI-DSS standard considered RFID and DNS security and cell phone security, and PCI-DSS as well as ISO-27799:2008 considered wireless networks security.

Conclusion: One can use the standard that is stronger in context. So, it is recommended to use PCI-DSS for cell phones, and ISO-27799:2008 or PCI-DSS for wireless networks. It is better for security in operation systems to use HIPAA. Combined standard with all these three standards aspects can be used as the safest approach.

Key words: Local Cardiovascular Terms, Coding, Application, ICD

•**Citation:** Moghadesi H, Ghaeme MM. A Comparative Study of Three Standards of Data Security in Health Systems. Journal of Health and Biomedical Informatics 2015; 2(3): 184-194.

1. Ph.D. in Medical Informatics & Information Management, Associate Professor, Shahid Beheshti University of Medical Sciences, School of Paramedical, Tehran, Iran.
2. Ph.D. in Medical Informatics, Shahid Beheshti University of Medical Sciences, School of Paramedical, Tehran, Iran.
***Correspondence:** Red Crescent Society, Helal Ahmar St., Sadoughi blvd., Kerman, Iran
• **Tel:** 09194183001 • **Email:** Dr.MGhaemi@gmail.com