# Designing a model for security requirements of electronic health records in Iran

M Farzandipour* M Ahmady** F Sadoughi*** I Karimi****

* Assistant professor of health information management, Kashan University of Medical Sciences, Kashan, Iran
**Associate professor of health information management, Iran University of Medical Sciences, Tehran, Iran
***Assistant professor of health information management, Iran University of Medical Sciences, Tehran, Iran
**** Associate professor of health economic, Iran University of Medical Sciences, Tehran, Iran

**Abstract**

**Background:** Flourishing capacity of information technologies for collecting, storage and transmission unheard of amount of information creates a great deal of concerns for patients. Patients are worried over the access of numerous people to their electronic health records.

**Objective**: To determine the security requirements of electronic health records for Iran.

**Methods:** This descriptive study was carried out in 2007. Security requirements of electronic health records gathered from comparative study performed in Australia, Canada and England countries followed by designing the initial model. The final model was prepared through gathering the information by questionnaire and the use of Delphi Technique. The values under 50 percent were eliminated from the model and those equal or higher than 75 percent added to the model.

**Findings:** The proposed model for Iran includes the requirements for organizing information, information classification, human resources, communication and operation management, and access control security.

**Conclusion:** A comprehensive model of electronic health records security requirements was designed for Iran. The approval of this model by authorities for protecting the electronic health information security is recommended.

**Keywords:** Electronic in Medical, Health, Information Security, Electronic Health Record, Security Model, Iran

**Corresponding Address:** 3rd Km. of Ravand-Kashan Highway, Kashan University of Medical Sciences, Kashan, Iran
**Email:** farzandipour_m@kaums.ac.ir
**Tell:** +98 9133624412
**Received:** 2008/01/20
**Accepted:** 2008/11/05

# طراحی الگوی الزامات ایمنی اطلاعات پرونده الکترونیک سلامت برای ایران

دکتر مهرداد فرزندی پور * دکتر مریم احمدی** دکتر فرحناز صدوقی*** دکتر ایرج کریمی****

* استادیار مدیریت اطلاعات بهداشتی- درمانی دانشگاه علوم پزشکی کاشان
** دانشیار مدیریت اطلاعات بهداشتی- درمانی دانشگاه علوم پزشکی ایران
*** استادیار مدیریت اطلاعات بهداشتی- درمانی دانشگاه علوم پزشکی ایران
**** دانشیار اقتصاد بهداشت دانشکده مدیریت دانشگاه علوم پزشکی ایران

آدرس مکاتبه: کیلومتر ۳ جاده راوند – کاشان، مجتمع مسکونی دانشگاه علوم پزشکی کاشان، تلفن ۰۹۱۳۳۶۲۴۴۱۲ Email: farzandipour_m@kaums.ac.ir

تاریخ دریافت: ۸۶/۱۰/۳۰ تاریخ پذیرش: ۸۷/۸/۱۵

***چکیده**

**زمینه:** ظرفیت رو به رشد فن‌آوری اطلاعات برای جمع‌آوری، ذخیره و انتقال حجم زیاد اطلاعات، باعث نگرانی بیماران در مورد دسترسی محدوده وسیعی از افراد به پرونده الکترونیک سلامت آنها شده است. نقص در ایمنی سیستم پرونده الکترونیک سلامت می‌تواند به افشای صدها یا هزاران پرونده منجر شود.

**هدف:** مطالعه به منظور تدوین و طراحی الگوی الزامات ایمنی اطلاعات پرونده الکترونیک سلامت برای کشور ایران انجام شد.

**مواد و روش‌ها:** این مطالعه مقطعی در سال ۱۳۸۶ انجام شد. الزامات ایمنی اطلاعات پرونده الکترونیک سلامت سه کشور استرالیا، کانادا و انگلستان بر اساس یک مطالعه تطبیقی انجام شده استخراج گردید. سپس الگوی اولیه طراحی و از طریق پرسش‌نامه و با آزمون دلفی به نظر سنجی گذاشته شد. موارد کم‌تر از ٪۵۰ از الگو حذف و موارد بالای ٪۷۵ پذیرفته و در الگوی نهایی منظور شد.

**یافته‌ها:** الگوی پیشنهادی شامل الزامات سازمان‌دهی ایمنی اطلاعات، ایمنی طبقه‌بندی اطلاعات، ایمنی منابع انسانی، ایمنی مدیریت ارتباطات و عملیات و کنترل دسترسی به اطلاعات بود.

**نتیجه‌گیری:** الگوی جامع الزامات ایمنی پرونده الکترونیک سلامت برای ایران طراحی شده است و برای حفظ امنیت اطلاعات سلامت تصویب و اجرای آن توسط مراجع ذی‌صلاح توصیه می شود.

**کلیدواژه ها:** الکترونیک در پزشکی، بهداشت و تندرستی، ایمنی اطلاعات، پرونده الکترونیک سلامت، الگوی ایمنی، ایران

## *مقدمه:

امروزه یکی از مهم‌ترین کاربردهای فن‌آوری اطلاعات در حوزه بهداشت و درمان، ایجاد پرونده الکترونیک سلامت است. پرونده الکترونیک سلامت مجموعه اطلاعات مرتبط با سلامت شهروندان، از پیش از تولد تا پس از مرگ است که به صورت مداوم و با گذشت زمان به شکل الکترونیکی ذخیره می‌شود و در صورت نیاز، بدون ارتباط با مکان یا زمان خاص، تمام یا بخشی از آن در دسترس افراد مجاز قرار خواهد گرفت.[۱] ظرفیت روبه رشد فن‌آوری برای جمع آوری، ذخیره و انتقال حجم زیاد اطلاعات، باعث نگرانی بیماران در مورد دسترسی محدوده وسیعی از افراد به پرونده الکترونیک آنها شده است.[۲-۵] پرونده الکترونیک از محل‌های متعددی قابل دسترس است و نقص ایمنی در سیستم آن می‌تواند به افشای صدها یا هزاران پرونده منجر شود.[۶] بررسی انجام شده در سال ۲۰۰۴ در آمریکا حاکی از آن است که نگرانی‌های ایمنی اطلاعات، بزرگ‌ترین مانع اجرای گسترده سیستم‌های پرونده الکترونیک و توزیع داده‌ها بوده است.[۷] وجود و اجرای سیاست‌ها و زیرساخت ایمنی اطلاعات در سازمان‌ها بسیار متفاوت بوده و حدود ۷۵ درصد

آنها تمام سیاست‌های کلیدی دسترسی به اطلاعات را در محل نداشته‌اند.[۸] مطالعه انجام شده در مراکز درمانی اصفهان در سال ۱۳۸۱ نشان داد که در ۸۲ درصد واحدها، ساز و کارهای حفاظتی مقتضی جهت ایمنی پرونده‌های بیماران وجود نداشته است.[۹] ایجاد چهارچوبی خصوصی و ایمن جهت اطلاعات، جمع آوری اطلاعات محرمانه بیمار و کنترل و نگه‌داری ایمن آن را تضمین می‌کند.[۱۰] اکنون سیاست وزارت بهداشت، درمان و آموزش پزشکی استفاده از فن‌آوری اطلاعات به طور گسترده در حوزه بهداشت و درمان و ایجاد پرونده الکترونیک سلامت است، لذا این مطالعه با هدف تدوین و طراحی الزامات ایمنی اطلاعات پرونده الکترونیک سلامت جهت تضمین ایمنی اطلاعات انجام شد.

*** مواد و روش‌ها:**

این مطالعه به روش مقطعی در سال ۱۳۸۶ انجام شد. الزامات ایمنی اطلاعات پرونده الکترونیک سلامت سه کشور استرالیا، کانادا و انگلستان بر اساس مطالعه تطبیقی انجام شده استخراج گردید.[۱۱] سپس اطلاعات مذکور جهت طراحی الگوی پیشنهادی اولیه در پنج محور شامل سازمان‌دهی ایمنی اطلاعات، ایمنی طبقه‌بندی و کنترل امکانات، ایمنی منابع انسانی، ایمنی مدیریت ارتباطات و عملیات و ایمنی کنترل دسترسی به اطلاعات پرونده الکترونیک سلامت با یکدیگر مقایسه شد. برای جلوگیری از تکرار، موارد مشابه حذف و تمام موارد متفاوت در هر یک از محورهای مذکور، در الگوی پیشنهادی اولیه گنجانده شد. در طراحی الگو هیچ‌گونه بومی‌سازی انجام نشد و تمام موارد از طریق پرسش‌نامه و با آزمون دلفی به رأی صاحب نظران گذاشته شدند. اعتبار علمی پرسش‌نامه الگوی پیشنهادی با استفاده از نظر جمعی از اساتید دانشگاهی و متخصصین مدارک پزشکی و مدیریت اطلاعات سلامت تعیین شد. پایایی سؤال‌های پرسش‌نامه با استفاده از روش براون پیرسون با ضریب اطمینان ۹۵ درصد تعیین شد.

پرسش‌نامه‌ها پس از ارائه به تعدادی از متخصصان و پاسخ گویی آنها، جمع آوری شدند و ۱۰ روز بعد مجدداً در مورد همان پرسش‌نامه‌ها از همان افراد نظرخواهی شد. در هر دو مرحله تأیید خبرگان به ابزار و روش گردآوری، قوت و اعتبار بیش‌تری بخشید. پس از تعیین روایی و پایایی پرسش‌نامه در پنج محور گفته شده، پرسش‌نامه جهت انجام آزمون دلفی، برای ۳۵ نفر از صاحب نظران، شامل کارشناسان ستادی مدیریت فن‌آوری اطلاعات وزارت بهداشت، درمان و آموزش پزشکی و کارشناسان مدیریت فن‌آوری اطلاعات دانشگاه‌های علوم پزشکی سراسر کشور از طریق پست معمولی و پست الکترونیک ارسال شد. ۳۲ نفر پرسش‌نامه‌ها را تکمیل و ارسال نمودند. در روش دلفی مواردی از الگو که صاحب نظران کم‌تر از ۵۰ درصد تأیید کرده بودند، حذف و مواردی که ۷۵ درصد و بیش‌تر تأیید شده بود، مورد قبول قرار گرفتند. چنانچه مواردی از الگو بین ۵۰ تا ۷۴ درصد مورد تأیید قرار می‌گرفتند و صاحب‌نظران موارد جدیدی پیشنهاد می‌کردند، در مرحله دوم آزمون دلفی انجام می‌شد. اما به دلیل کسب نتیجه مورد نظر در مرحله اول و عدم ارائه پیشنهادی از سوی صاحب نظران، آزمون دلفی به مرحله دوم کشیده نشد. داده‌ها با استفاده از آمار توصیفی تحلیل شدند.

***یافته‌ها:**

موارد مورد تأیید اکثر صاحب نظران عبارت بودند از: تشکیل گروه مدیریت ایمنی اطلاعات در سازمان، تبیین مسؤولیت موضوع ایمنی فن‌آوری اطلاعات سازمان توسط این گروه و محاسبه تمام دارایی‌های فن‌آوری اطلاعات سازمان و تعیین مالک برای آنها و

طبقه‌بندی اطلاعات به سه طبقه با سطوح محرمانه جهت دسترسی به آن تأکید داشتند (جدول شماره ۱). صاحب نظران، ایجاد سیاست کنترل و مدیریت دسترسی به شبکه، تعیین مسؤولیت‌های کاربر، پایش دسترسی به سیستم و ایمنی رایانه‌های سیار را مورد تأیید قرار دادند (جدول شماره۲).

**جدول۱- الزامات ایمنی طبقه بندی و کنترل امکانات پرونده الکترونیک سلامت از دیدگاه کارشناسان**

| الزامات | مواردی که ۷۵ درصد و بیش‌تر مورد تأیید قرار گرفت |
|---|---|
| مسؤولیت | محاسبه تمام دارایی‌های فن آوری اطلاعات سازمان و تعیین مالک برای آنها |
| طبقه‌بندی اطلاعات | تعیین گزینشی سطوح دسترسی داخلی به اطلاعات و ممانعت از دسترسی خارجی به آنها |
| | حفظ اطلاعات درون سازمان به صورت محرمانه و حفاظت آن از دسترسی بیرونی |
| | حفظ اطلاعات به صورت سری و حفاظت آن از دسترسی غیر مجاز درونی یا بیرونی |
| | طبقه‌بندی تمامی داده‌های سلامت درسازمان‌ها، به صورت محرمانه به عنوان اطلاعات شخصی سلامت |
| ممیزی | آگاهی کاربران در تمامی سازمان‌ها از محرمانه بودن اطلاعات سلامت به وسیله برچسب زنی بر روی اطلاعات |
| | ممیزی منظم فهرست موجودی امکانات، طرح برچسب زنی، طبقه بندی اطلاعات و رویه های جابجایی |

**جدول۲- الزامات ایمنی کنترل دسترسی به اطلاعات پرونده الکترونیک سلامت از دیدگاه کارشناسان**

| الزامات | مواردی که ۷۵ درصد و بیشتر مورد تأیید قرار گرفت |
|---|---|
| سیاست کنترل دسترسی | تعریف و ثبت شرایط کاری کنترل دسترسی و محدودسازی دسترسی بر اساس سیاست بازرسی |
| مدیریت دسترسی کاربر | اختصاص مشخصه شناسایی منحصر به فرد برای هر کاربر |
| | ایجاد محدودیت زمانی ورود کاربران به سیستم اطلاعاتی سازمان |
| | اعطای دسترسی به کاربران بر اساس نقش آنها در سازمان |
| | دسترسی هر کاربر به اطلاعات در هر دوره کاری تنها در یک نقش واحد |
| | امکان اعطای دسترسی به کاربران در گروه‌های کاری |
| | امکان لغو به هنگام حق دسترسی کاربر به اطلاعات |
| کنترل دسترسی به شبکه | دسترسی مستقیم کاربران فقط به سرویس‌های مجاز |
| | کنترل مسیر راه از پایانه کاربر تا سرویس رایانه |
| | اخذ مجوز جهت دسترسی کاربران از راه دور |
| | کنترل مطمئن دسترسی به درگاه‌های تشخیصی |
| | کنترل دسترسی به سیستم‌های عامل |
| کنترل دسترسی برنامه کاربردی | محدودسازی دسترسی به اطلاعات و عملکردهای سیستم تجاری مطابق با سیاست کنترل دسترسی تعریف شده شغلی |
| پایش دسترسی به سیستم | همزمانی ساعت‌های رایانه ای برای ثبت دقیق حوادث ایمنی |
| رایانه سیار | انجام بازرسی‌های مناسب در مقابل خطرات ناشی از کار با امکانات سیار رایانه ای |
| | توسعه رویه‌ها و سیاست‌ها برای تأیید و کنترل فعالیت‌های ارتباط از راه دور |

***بحث و نتیجه‌گیری:**

مطالعه حاضر بر تشکیل گروه مدیریت ایمنی اطلاعات در سازمان جهت تضمین ایمنی اطلاعات پرونده الکترونیک سلامت و تبیین واضح مسؤولیت‌های ایمنی اطلاعات توسط گروه مدیریت تأکید داشت. یافته‌های مطالعه تطبیقی سه کشور استرالیا، کانادا و انگلستان نیز بر موارد مذکور تأکید دارد.[۱۲-۱۴] اجلاس مشترک اعتباربخشی آمریکا با توجه به اهمیت و حساسیت اطلاعات الکترونیک در محیط‌های درمانی، بر مسؤولیت مدیر بخش مدارک پزشکی در حفاظت از این اطلاعات تأکید کرده است.[۱۵] شواکتل در مقاله‌ای بیان کرده که هر سازمانی باید فعالیت‌هایی تحت عنوان مدیریت ایمنی داشته باشد.[۱۶]

مطالعه حاضر بر آگاهی کاربران از محرمانه بودن اطلاعات سلامت در تمام سازمان‌ها، محاسبه دارایی‌های فن‌آوری اطلاعات، تعیین مالک برای آنها و طبقه‌بندی اطلاعات به سه طبقه محرمانه تأکید داشت. سه کشور استرالیا، کانادا و انگلستان نیز بر موارد مذکور تاکید دارند. با این تفاوت که در استرالیا بر طبقه‌بندی اطلاعات به چهار طبقه حساس، در کانادا بر طبقه‌بندی اطلاعات به صورت کلی و محرمانه و در انگلستان بر طبقه‌بندی اطلاعات توسط مالک امکانات اطلاعاتی تأکید شده است.[۱۲-۱۴] پژوهش زاهدی‌فر بیان‌گر آن است که در ۹۰/۹ درصد از مراکز درمانی، اوراق مالی مربوط به درمان بیماران جزو اوراق محرمانه محسوب می‌شوند.[۹] در مطالعه صلاحی ۱۸/۲درصد واحدها، ساز و کارهای حفاظتی مقتضی جهت ایمنی پرونده‌های مربوط به درمان مبتلایان به ایدز، بیماران روانی و سایر بیماری‌های حساس را داشته‌اند.[۱۷] به نظر می‌رسد به دلیل عدم وجود الزاماتی در خصوص ایمنی طبقه‌بندی و کنترل امکانات اطلاعاتی در کشورمان و فقدان طبقه‌بندی مناسب برای اطلاعات سلامت، مراکز درمانی از یک رویه استاندارد پیروی نمی‌کنند. لذا، در صورت ایجاد پرونده الکترونیک سلامت، لازم است اطلاعات بیماران بر اساس درجه محرمانگی به سه طبقه اطلاعات اداری و مالی، تشخیصی و درمانی و در سه طبقه داخلی، محرمانه و سری تقسیم‌بندی شده و ضمن تعریف میزان دسترسی به هر طبقه، ساز و کارهایی جهت حفاظت از اطلاعات به اجرا در آید.

مطالعه حاضر بر حفظ محرمانگی اطلاعات توسط کارکنان و تعیین مسؤولیت‌ها و وظایف آنان در این زمینه تأکید داشت. یافته‌های مطالعه تطبیقی در سه کشور استرالیا، کانادا و انگلستان نیز بر موارد مذکور تاکید دارد.[۱۲-۱۴] نتایج یک بررسی در کانادا حاکی از آن است که ۹۰ درصد کارکنان سازمان‌ها ملزم به امضای توافق‌های محرمانه اطلاعات هستند.[۷] یانگ وکوکی اظهار داشته‌اند که مدیریت باید از طریق سرمایه‌گذاری در آموزش نیروی کار به کاهش احتمال خطر، آسیب یا صدمه به دارایی‌های سازمان نظیر اطلاعات کمک کند.[۱۵] با توجه به آغاز طراحی پرونده الکترونیک سلامت در ایران، ضمن لزوم تدوین و رعایت الزامات ایمنی، آموزش مناسب کارکنان و طراحی برنامه‌های آموزش بدو خدمت و ضمن خدمت برای مشمولین بازآموزی ضرورت دارد.

مطالعه حاضر بر پیروی از رویه‌های عملی استاندارد در نگه‌داری، جابه‌جایی و ایمنی رسانه رایانه‌ای و تبادل الکترونیکی تأکید داشت. یافته‌های مطالعه تطبیقی در سه کشور استرالیا، کانادا و انگلستان نیز بر موارد مذکور تأکید دارد.[۱۲-۱۴] ضمن این‌که تنها کانادا بر نگه‌داری اطلاعات پشتیبان در یک محیط ایمن از لحاظ فیزیکی، خارج از جایگاه اصلی و واقعه نگاری ممیزی اطلاعات تأکید دارد.[۱۳] در ایران علی رغم عدم وجود الزامات ایمنی مدیریت ارتباطات و عملیات پرونده الکترونیک سلامت به دلیل پراکندگی سیستم‌های اطلاعات

بیمارستانی در برخی مراکز درمانی، رویه‌هایی برای ایمنی اطلاعات مورد استفاده قرار گرفته است.[۱۱] مطالعه زاهدی‌فر نشان می‌دهد که در تمام مراکز درمانی، دیسکت‌های حاوی اطلاعات بیماران در محل‌های امن نگه‌داری شده‌اند که با یافته‌های این پژوهش همخوانی دارد.[۹] صلاحی در پژوهشی نشان داد که مطابقت سیستم امنیتی برای خروج پرونده با استانداردهای امنیت اطلاعات در بیمارستان‌های کشور ۶۲/۳ درصد است که نشان دهنده کمبود دستورالعمل‌ها و استانداردهایی در این زمینه در کشور است.[۱۷] نتایج یک مطالعه در آمریکا نشان داد که ۴۳ درصد افراد، وجود توافق بین فراهم‌کنندگان مراقبت برای مبادله اطلاعات درمانی را لازم دانسته‌اند و در کانادا حدود ۶۶ درصد واحدها طرح‌هایی برای ممیزی منظم و گزارش دسترسی غیر معمول داشتند که با یافته‌های این پژوهش مغایرت دارد.[۷و۸] به نظر می‌رسد علی رغم فقدان الزامات ایمنی مدیریت ارتباطات و عملیات پرونده الکترونیک سلامت در ایران، مراکز درمانی تا حدودی به این مقوله توجه دارند، اما این توجه کافی نیست. لذا ثبت تمام ارتباطات با سیستم پرونده الکترونیک سلامت ضروری است. استفاده از برنامه‌های ضد کدهای مضر برای حفاظت از پایگاه‌های اطلاعاتی و دیواره آتش برای حفاظت از سیستم‌های تحت شبکه، پشتیبان‌گیری منظم از اطلاعات موجود بر روی سیستم و رمزگذاری اطلاعات لازم است. همچنین باید استفاده از زیر ساخت کلید عمومی و انجام مستمر واقعه نگاری‌های سیستم، امنیت اطلاعات حفظ شده و دستورالعمل‌های جامع در این خصوص توسط متولیان امر ابلاغ گردد.

مطالعه حاضر بر لزوم ایجاد سیاست کنترل دسترسی کاربر به اطلاعات سلامت، تأکید داشت. یافته‌های مطالعه تطبیقی در سه کشور استرالیا، کانادا و انگلستان نیز بر این موارد تأکید دارند.[۱۲-۱۴] مطالعه انجام شده در اصفهان نشان دادکه در ۸۱/۸ درصد مراکز درمانی، ورود اطلاعات به رایانه توسط کارکنان مجاز که رمز عبور دارند انجام گرفته و در تمام واحدها، کاربران فقط به بخشی از برنامه‌های رایانه‌ای که مربوط به حیطه وظایفشان است، دسترسی داشته‌اند.[۹] بر اساس پژوهشی در آمریکا، حدود ۸۸ درصد افراد روش استفاده از رمز عبور را برای دسترسی ایمن به اطلاعات ترجیح می‌دهند.[۷] بر اساس پژوهشی در کانادا، بیش از ۸۰ درصد سازمان‌ها دسترسی کارمندان و پزشکان به پرونده‌های بالینی را تنظیم کرده‌اند. تمام سازمان‌ها کنترل دسترسی به سیستم‌های بالینی با شناسه کاربری و رمز عبور داشته‌اند و حدود ۹۰ درصد سازمان‌ها شناسه کاربری و رمز عبور واحدی داشته‌اند که با یافته‌های این پژوهش مشابه است.[۸] یافته‌های پژوهش انجام شده در آمریکا بیان‌گر آن است که عمده‌ترین مانع ایجاد یک زیر ساخت ملی اطلاعات سلامت، فقدان سیاست مربوط به دسترسی به اطلاعات بیمار است. تنها ۵ درصد افراد دسترسی الکترونیکی به اطلاعات داشته‌اند و حدود ۳۷ درصد افراد اعتقادی به لزوم استفاده از اجازه الکترونیکی جهت دسترسی به اطلاعات محرمانه بیمار نداشته‌اند.[۷] طبق پژوهش انجام شده در کانادا، سیاست دسترسی به اطلاعات به طور گسترده‌ای در سازمان‌ها متفاوت است. حدود ۲۵ درصد سازمان‌ها سیاست‌های خصوصی بودن و دسترسی به اطلاعات در محل، بیش از ۵۰ درصد سازمان‌ها سیاست مربوط به دستیابی به اطلاعات بالینی از راه دور، کم‌تر از ۵۰ درصد سازمان‌ها جنبه‌های ایمنی برای دسترسی از راه دور و حدود ۳۳ درصد کنترل دسترسی به اطلاعات الکترونیکی بیمار را ذکر کرده‌اند.[۸] با توجه به تأیید بیش از ۷۵ درصد بر کنترل دسترسی به اطلاعات در پژوهش حاضر، یافته‌های فوق با یافته‌های پژوهش حاضر همخوانی ندارد. با طراحی و ایجاد پرونده الکترونیک سلامت لازم است شناسه بیمار، مؤسسه و فراهم کنندگان خدمت تعیین و مورد استفاده قرار گیرد و برای تمام کاربران مجاز، نام کاربری و رمز

عبور تعریف و در موارد لزوم از سیستم‌های بیومتریک استفاده شود تا امکان شناسایی کاربران اطلاعات و ردیابی داده‌ها فراهم شود.

با توجه به الگوی پیشنهادی، تصویب و اجرای الزامات ایمنی اطلاعات پرونده الکترونیک سلامت توسط مراجع ذی‌صلاح با استفاده از فن‌آوری‌های روز اطلاعات برای کشور توصیه می‌شود.

## *مراجع:


1. Riazi H, Fathi Roodsari B, Bitaraf E. Electronic Health Record, Concepts, Standards and Development Approaches. 1st ed. Tehran: Ministry of Health, and Medical education; 2007. 125. [In Persian]

2. National Electronic Health Records taskforce. A national approach to electronic health records for Australia. Available at: URL: http://www.healthconnect.gov.au. Accessed in: 2000/ Mar

3. National Electronic Health Records taskforce. A health information Network for Australia. Available at: URL: http://www.health.gov.au. Accessed in: 2000/ Jul.

4. Lyons R, Payne C, Mccabe M, Fielder C. Legibility of doctor's hand writing: quantitative comparative study. BMJ 1998; 317: 863-4

5. Woodward B. The computer– based patient record and confidentiality. Engl J Med 1995; 333:1419-22

6. Aspen Reference Group. Health information management manual. 1st ed. Maryland: Aspen publication; 1999. 5

7. HIMSS. 2004 Himss National health information infrastructure survey. Available at: URL: http://www.ncvhs.com . Accessed in: 2004/ July

8. Canada Health infoway. Infoway pan-Canadian EHR survey phase I Results and analysis. Available at: URL: http://www.canadahealthinfoway.ca. Accessed in: 2003 Jan

9. Zahedifar R. Study Rate of respect for patients Rights in Medical Records Units of Isfahan University of Medical Sciences [Thesis]. Medical Information Management Faculty, Tehran: Iran University of Medical Sciences; 2002. [In Persian]

10. Cornwall A. Electronic health Records: An intentional perspective. Available at: URL:http://www.home.vicnet.net.an. Accessed in: 2002

11. Farzandipour M, Ahmadi M, Sadoughi F, Karimi A. Security Requirements of Electronic Health Records in the selected countries, A Comparative Study. Health Information Journal, spring & summer 2007; 7(1):1-9. [In Persian]

12. NHS. IM&T security policy: version 1.1. Available at URL:http://www.northumberlandcaretrust.nhs.uk. Accessed in: 2004 Nov.

13. Canada Health infoway. Electronic Health Record privacy and security Requirements. Available at: URL: http://www.itacontario.com. Accessed in: 2005

14. ABC pty Ltd IT Services. Information Security Controls and procedures manual. Available at: URL: http://www.maralan.com.au. Accessed in: 2006

15. Mohammad pour A. A Comparative Study on the Hospital Standards of Ministry of Health and International Standards of Joint Commission on Accreditation of Hospital [Thesis]. Medical Information Management Faculty, Tehran: Iran

University of Medical Sciences; 2006 [In Persian]
16. Schaectel D. How to build safety management system. Version 1. USA: Professional Safety; 1997. 22
17. Salahi M. An Investigation on Conditions of Storage and Retrieval of Patients' Medical Records in Teaching Hospitals of Iran University of Medical Sciences and Their Comparison with National Standards and Standards in the US. [Thesis]. Medical Information Management Faculty, Tehran: Iran University of Medical Sciences; 1998 [In Persian]