

## طراحی الگوی اصول محرمانگی اطلاعات پرونده سلامت الکترونیک برای ایران؛ ۱۳۸۶

مهرداد فرزندی پور<sup>۱</sup> / فرحناز صدوقی<sup>۲</sup> / مریم احمدی<sup>۳</sup> / ایرج کریمی<sup>۴</sup>

چکیده

**مقدمه:** امروزه رشد روزافزون اطلاعات سلامت، موجب بکارگیری فناوری‌های نوین جهت اداره و بهره‌برداری مناسب از اطلاعات از جمله ایجاد پرونده سلامت الکترونیکی شده است. ظرفیت روبه رشد فناوری‌های اطلاعات برای جمع‌آوری، ذخیره و انتقال اطلاعات در حجم زیاد، نگرانی‌های قابل درکی ایجاد کرده است زیرا پرونده‌های کامپیوتری توسط کاربران مختلف و از محل‌های متعدد قابل دسترس است. اکنون با توجه به رویکرد کشورمان به سمت طراحی و ایجاد پرونده سلامت الکترونیک، سؤال اساسی این است که آیا الگوی اصول محرمانگی آن توسط متولیان امر طراحی شده است؟

**روش بررسی:** مطالعه به روش توصیفی در سال ۱۳۸۶ انجام شد. اطلاعات اصول محرمانگی پرونده سلامت الکترونیک سه کشور استرالیا، کانادا و انگلستان بر اساس مطالعه تطبیقی انجام شده استخراج گردید و سپس الگوی اولیه طراحی شد. الگوی مذکور از طریق پرسشنامه و با استفاده از آزمون دلفی به رأی صاحب نظران گذاشته شد و موارد کمتر از ۵۰ درصد از الگو حذف، ۵۱ تا ۷۵ درصد مجدداً به نظر سنجی گذاشته شد و موارد ۷۵ درصد و بالاتر از آن پذیرفته و در الگوی نهایی منظور شد. **یافته‌ها:** الگوی پیشنهادی برای کشورمان بر محوریت رضایت بیمار در اصول محرمانگی پرونده سلامت الکترونیک تأکید دارد و استفاده و افشای اطلاعات سلامت برای بازاریابی، مقاصد خارج از چرخه مراقبت و درمان بدون رضایت بیمار، اعضای خانواده و افراد دیگری که ارتباط شخصی نزدیکی با بیمار دارند و عدم دسترسی فرد به اطلاعات سلامت خود در بعضی موارد مورد تأیید قرار نگرفته است. همچنین در الگوی پیشنهادی، به اعمال جریمه‌های افشاء و امحاء پرونده سلامت الکترونیک، مالکیت داده‌ها، شمول قوانین دسترسی به اطلاعات در تمام سازمان‌ها، مسئول عدم دسترسی سریع به اطلاعات و شرایط انتقال اطلاعات به خارج از کشور اشاره شده که در اصول محرمانگی کشورهای منتخب اشاره‌ای به آن نشده است. **نتیجه‌گیری:** در این پژوهش الگوی اصول محرمانگی پرونده سلامت الکترونیک برای ایران طراحی شده است که جهت حفظ محرمانگی اطلاعات بیمار آن تصویب و اجرای آن توسط مراجع ذیصلاح توصیه می‌شود.

**کلید واژه‌ها:** اصول محرمانگی، محرمانگی اطلاعات، پرونده سلامت الکترونیک، الگوی محرمانگی

◇ وصول مقاله: ۸۷/۴/۲، اصلاح نهایی: ۸۷/۸/۱۳، پذیرش نهایی: ۸۷/۹/۲۴

۱- استادیار گروه مدارک پزشکی، دانشکده پیراپزشکی، دانشگاه علوم پزشکی کاشان، نویسنده مسئول؛ (Email: farzandipour-m@kaums.ac.ir)

۲- استادیار گروه مدیریت اطلاعات بهداشتی و درمانی، دانشکده مدیریت و اطلاع‌رسانی پزشکی، دانشگاه علوم پزشکی ایران

۳- دانشیار گروه مدیریت اطلاعات بهداشتی و درمانی، دانشکده مدیریت و اطلاع‌رسانی پزشکی، دانشگاه علوم پزشکی ایران

۴- استادیار گروه مدیریت خدمات بهداشتی و درمانی، دانشکده مدیریت و اقتصاد، دانشگاه آزاد اسلامی تهران، واحد علوم و تحقیقات

## مقدمه

همچنین مطالعه سال ۸۲ نشان داد که بخش مدارک پزشکی بیمارستان‌های ایران از استانداردهای مربوط به محرمانگی اطلاعات فاصله و انحراف دارد. [۱۲] در برخی کشورها برای نقض مقررات محرمانگی پرونده سلامت الکترونیک، هم جرمه‌های مدنی و هم کیفری اعمال می‌شود. [۱۳] بنابراین اکنون که سیاست وزارت بهداشت، درمان و آموزش پزشکی ایران استفاده از فناوری اطلاعات به طور گسترده در حوزه بهداشت و درمان و ایجاد پرونده سلامت الکترونیک است سؤال اساسی این است که آیا جهت تضمین محرمانگی اطلاعات بیماران، الگوی اصول محرمانگی اطلاعات پرونده سلامت الکترونیک توسط متولیان امر طراحی شده است؟

## روش بررسی

مطالعه به روش توصیفی در سال ۱۳۸۶ انجام شد. اطلاعات اصول محرمانگی پرونده سلامت الکترونیک سه کشور منتخب استرالیا، کانادا و انگلستان براساس مطالعه تطبیقی انجام شده استخراج گردید. [۱۴] سپس اطلاعات مذکور جهت طراحی الگوی پیشنهادی اولیه درشش محور، شامل شرایط جمع‌آوری اطلاعات، اصول استفاده از اطلاعات، اصول افشای اطلاعات، اصول دسترسی فرد به اطلاعات، شرایط نگهداری اطلاعات و مسئولیت‌های متولی اطلاعات با یکدیگر مقایسه گردید و برای جلوگیری از تکرار، موارد مشابه حذف و تمامی موارد متفاوت در هر یک از محورهای مذکور، در الگوی پیشنهادی اولیه، گنجانده شد. در طراحی الگو هیچ‌گونه بومی‌سازی انجام نگردید و تمامی موارد از طریق پرسشنامه و با آزمون دلفی به رأی صاحب‌نظران گذاشته شد. اعتبار علمی پرسشنامه الگوی پیشنهادی با استفاده از نظر جمعی از صاحب‌نظران دانشگاهی و متخصصین مدارک پزشکی و مدیریت اطلاعات سلامت تعیین شد. پایایی سؤالات پرسشنامه با استفاده از روش براون پیرسون با ضریب اطمینان ۹۵ درصد تعیین گردید. پرسشنامه به تعدادی از متخصصان ارائه گردید و پس از پاسخگویی، جمع‌آوری و ۱۰ روز بعد مجدداً همان پرسشنامه‌ها از همان افراد نظرخواهی شد. در هر دو مرحله تأیید خبرگان به ابزار و

امروزه یکی از مهم‌ترین کاربردهای فناوری اطلاعات در حوزه بهداشت و درمان، ایجاد پرونده سلامت الکترونیک است. پرونده سلامت الکترونیک عبارت است از مجموعه کلیه اطلاعات مرتبط با سلامت شهروندان، از پیش از تولد تا پس از مرگ که به صورت مداوم و با گذشت زمان به شکل الکترونیکی ذخیره می‌گردد و در صورت نیاز، بدون ارتباط با مکان یا زمان خاص، تمام یا بخشی از آن در دسترس افراد مجاز قرار خواهد گرفت. [۱] توسعه ظرفیت الکترونیکی جمع‌آوری، توزیع، سازگاری و دستکاری اطلاعات، علی‌رغم مزایایی که دارد، خطراتی هم دارد. [۲] در طراحی پرونده سلامت الکترونیک در هر کشوری، یکی از عوامل مهم مورد توجه، ایجاد زیرساخت مناسب اطلاعات سلامت است. [۳] عملکرد صحیح زیرساخت اطلاعات سلامت به اصول محرمانگی و ایمنی اطلاعات سلامت بستگی دارد. [۴] ظرفیت رو به رشد فناوری‌های اطلاعات و ارتباطات برای جمع‌آوری، ذخیره و انتقال اطلاعات در حجم زیاد، نگرانی‌های قابل درکی ایجاد کرده است که ممکن است به دلیل افزایش قابلیت دسترسی به حجم عظیم اطلاعات از طریق فناوری‌های نوین، خصوصی بودن اطلاعات سلامت مصرف‌کنندگان خدمت در قرن الکترونیک کاهش یابد. [۵، ۶] مصرف‌کنندگان خدمات سلامت نگران هستند که فناوری اطلاعات و پرونده‌های سلامت الکترونیک، اطلاعات شخصی سلامت آنها را برای محدوده وسیعی از افراد قابل دسترس‌تر نماید. [۷، ۸] بررسی انجام شده در سال ۲۰۰۴ در آمریکا حاکی از آن است که نگرانی‌های ایمنی و محرمانگی اطلاعات، بزرگترین مانع اجرای گسترده سیستم‌های پرونده کامپیوتری و توزیع داده‌ها است. [۹] بررسی انجام شده در سال ۸۴ در خصوص محرمانگی پرونده‌های پزشکی در ایران نشان می‌دهد که در اکثریت موارد جهت دسترسی، استفاده و افشای اطلاعات پرونده بیماران ضوابط خاصی وجود ندارد. [۱۰] به نظر می‌رسد به دلیل فقدان دستورالعمل‌های واضح و مشخص در زمینه محرمانگی اطلاعات بیماران در ایران، بخش مدارک پزشکی بیمارستان‌ها سلیقه‌ای عمل نموده که این امر موجب تضییع حقوق بیمار می‌شود. [۱۱]

روش گردآوری، قوت و اعتبار بیشتری بخشید. پس از تعیین روایی و پایایی پرسشنامه الگوی پیشنهادی در شش محور گفته شده، در مرحله اول آزمون دلفی پرسشنامه مذکور برای ۳۵ نفر از صاحب نظران، شامل اعضای هیأت علمی گروه‌های آموزشی مدارک پزشکی و مدیریت اطلاعات سلامت دانشگاه‌های علوم پزشکی و کارشناسان سازمان پزشکی قانونی کشور ارسال گردید. پرسشنامه از طریق پست معمولی و بخشی از آن از طریق پست الکترونیک ارسال شد. از بین پرسشنامه‌های ارسالی، ۳۴ نفر از صاحب نظران، پرسشنامه‌های مذکور را تکمیل و پاسخ آنها را ارسال نمودند. ۶۵ درصد صاحب نظران زن و ۳۵ درصد مرد بوده‌اند. ۵۰ درصد ۲۵-۳۴ سال و ۵۰ درصد ۳۵-۵۴ سال سن داشته‌اند. سابقه کار ۵۶ درصد ۹-۳ سال و ۴۴ درصد ۱۰ و بیش از آن بوده است. مدرک تحصیلی ۶۵ درصد کارشناس ارشد، ۲۰ درصد کارشناس و ۱۵ درصد دکتری بوده است. رشته تحصیلی ۸۵ درصد مدارک پزشکی و ۱۵ درصد مدیریت اطلاعات سلامت بوده است. ۷۴ درصد عضو هیأت علمی و ۲۶ درصد غیر هیأت علمی بوده‌اند. به منظور تحلیل داده‌های گردآوری شده، از روش‌های آمار توصیفی استفاده به عمل آمد. در تکنیک دلفی مواردی از الگو که صاحب نظران کمتر از ۵۰ درصد آن را تأیید کرده بودند از الگو حذف و مواردی که ۷۵ درصد و بیش از آن تأیید شده بود، مورد قبول قرار گرفت. مواردی از الگو که بین ۵۰ تا ۷۵ درصد مورد تأیید قرار گرفته بودند و موارد پیشنهادی صاحب نظران در مرحله دوم آزمون دلفی، مجدداً به نظرخواهی گذاشته شد تا اجماع نظر حاصل شد. در مرحله دوم آزمون دلفی، پرسشنامه برای ۳۵ نفر از صاحب نظران ارسال گردید که ۳۰ نفر به پرسشنامه‌ها پاسخ دادند. نتایج حاصل در جداول آمده است.

#### یافته‌ها

بر اساس نظر صاحب نظران، جمع‌آوری اطلاعات با رضایت فرد و همچنین برای اقدام قانونی، آگاهی فرد مربوطه از چگونگی و شرایط جمع‌آوری اطلاعات و افشاء آن، شرایط جمع‌آوری اطلاعات از فردی دیگر و تعهد سازمان مبنی بر عدم افشای اطلاعات فرد بدون رضایت وی

مورد تأیید قرار گرفته است (جدول ۱).

طبق نظر صاحب نظران، استفاده از اطلاعات سلامت با رضایت بیمار و عدم استفاده از اطلاعات برای مقاصدی خارج از چرخه مراقبت و درمان بدون رضایت فرد مربوطه مورد تأیید قرار گرفته است. همچنین استفاده یا افشای اطلاعات سلامت برای مقاصدی خارج از چرخه مراقبت و درمان در صورت عدم امکان کسب رضایت فرد، توسط بخش خصوصی برای دادگاه‌ها، برای بازاریابی مستقیم، اعضای خانواده فرد یا افراد نزدیک به بیمار و در مورد اطلاعات سلامت فرد فوت شده، مورد تأیید قرار نگرفته است (جدول ۲).

نظر صاحب نظران، بر دسترسی فرد به اطلاعات پرونده سلامت الکترونیک خود بر اساس درخواست و عدم دسترسی به اطلاعات تحت شرایط خاصی تأکید دارد (جدول ۳).

بر اساس نظر صاحب نظران، بر وجود سیاست مکتوبی درباره نگهداری اطلاعات سلامت و تمامی دسترسی‌ها به آن و ردیابی داده‌ها در پرونده سلامت الکترونیک تأکید شده است (جدول ۴).

صاحب نظران در ایران، بر ایجاد حفاظت‌های اداری، فنی و فیزیکی مناسب و آگاهی تمامی عوامل متولی اطلاعات سلامت از آنها تأکید نمودند. همچنین واگذاری مالکیت داده‌ها به فراهم‌کننده خدمت و مسئولیت عدم دسترسی سریع به اطلاعات سلامت بر عهده فرد بیمار، مورد تأیید قرار نگرفت (جدول ۵).

بر اساس نظر صاحب نظران، در مرحله دوم آزمون دلفی، افشای اطلاعات سلامت توسط شخص دریافت‌کننده اطلاعات برای اهدافی غیر از آنچه که اطلاعات برای آن جمع‌آوری شده با رضایت بیمار کاملاً مورد تأیید قرار گرفته است و عدم امکان دسترسی فرد به اطلاعات خود در صورت بیهوده بودن درخواست دسترسی، ارتباط اطلاعات با اقدامات قانونی بین سازمان و فرد، لطمه به اهداف سازمان و تحویل مدارک پرونده بیمار به خود وی در صورت ضرورت امحای پرونده مورد تأیید قرار نگرفته است (جدول ۶).



### جدول ۱: شرایط جمع آوری اطلاعات پرونده سلامت الکترونیک از دیدگاه کارشناسان (در مرحله اول آزمون دلغی)

مواردی که ۷۵ درصد و بیشتر مورد موافقت قرار گرفته‌اند	
بر اساس قانون و محدود به داده‌های ضروری برای دستیابی به اهداف قانونی	
یک فرد با رضایت فرد و تنها از فرد مربوطه	
برای ایجاد، اقدام یا دفاع از ادعای قانونی یا منصفانه	جمع‌آوری اطلاعات:
در صورت عدم نقض حریم خصوصی فرد مربوطه	
با رضایت صریح فرد برای مقاصد خارج از چرخه مراقبت مگر با مجوز قانون	
الف: هویت و چگونگی تماس با سازمان جمع‌آوری‌کننده اطلاعات	
ب: امکان دسترسی خود به اطلاعات	
ج: مقاصد جمع‌آوری اطلاعات توسط سازمان	
د: سازمان‌هایی که اطلاعات برای آنها فاش خواهد شد	آگاهی فرد مربوطه همزمان یا قبل از جمع‌آوری اطلاعات از:
ه: قوانین جمع‌آوری اطلاعات	
و: تبعات اصلی عدم جمع‌آوری اطلاعات	
ز: نوع اطلاعاتی که درباره او جمع‌آوری می‌شود	
الف: برای پیشگیری یا کاهش تهدید جدی برای زندگی و سلامت هر فرد	
ب: در صورت عدم توانایی فرد به دادن رضایت	
ج: در صورت عدم توانایی فرد از نظر جسمی به دادن رضایت کتبی	
د: با اجازه فرد موضوع داده‌ها (بیمار)	جمع‌آوری اطلاعات یک فرد از فرد دیگر:
ه: در صورت تعیین یک نماینده قانونی به عنوان جانشین توسط فرد	
و: در صورت احتمال جمع‌آوری اطلاعات نادرست از فرد بیمار	
ز: در صورت عدم امکان جمع‌آوری عملی اطلاعات از فرد موضوع داده‌ها (بیمار)	
تعهد سازمان مبتنی بر عدم افشای اطلاعات فرد بدون رضایت وی	
فرض فرد جمع‌آوری‌کننده اطلاعات در شرایط معقول بر وجود رضایت ضمنی بیمار مگر مواردی که بین ۵۰ تا ۷۵ درصد مورد موافقت قرار گرفته‌اند.	
تنها برای انجام وظایف یا فعالیت‌های سازمان مانند ارائه یک خدمت سلامت	جمع‌آوری اطلاعات:
عدم شناسایی دائمی اطلاعات قبل از افشای آن با گام‌های معقول سازمان جمع‌آوری‌کننده اطلاعات	

### بحث و نتیجه‌گیری

نظرات صاحب‌نظران در الگوی پیشنهادی بر جمع‌آوری اطلاعات سلامت با رضایت فرد و تنها از فرد مربوطه تأکید دارد و جمع‌آوری اطلاعات سلامت یک فرد از فرد دیگری را تحت شرایطی مجاز دانسته است. نتایج مطالعه تطبیقی نشان داد که سه کشور استرالیا، کانادا و انگلستان نیز بر موارد مذکور تأکید دارند. [۱۵-۱۸] انجمن مدیریت اطلاعات بهداشتی آمریکا [۱۲] و طاهری [۱۹] بر کسب رضایت بیمار و وجود

مدرک رضایت او در پرونده تأکید دارند. زاهدی فرد نیز در پژوهش سال ۱۳۸۱ در اصفهان نتیجه گرفت که در تمام واحدهای مورد مطالعه در سیستم دستی رضایت‌نامه‌های موجود در پشت برگ پذیرش از بیماران اخذ می‌شود. [۲۰] یافته‌های مذکور با یافته‌های این پژوهش همخوانی دارند. یافته‌های پژوهش محمدپور در سال ۱۳۸۵ [۲۱] و سرباز در سال ۱۳۸۱ [۲۲] نشان داد که ۵۸۳ درصد بین استانداردهای بیمارستانی وزارت بهداشت ایران با استانداردهای



**جدول ۲: اصول استفاده و افشای اطلاعات پرونده سلامت الکترونیک از دیدگاه کارشناسان  
(در مرحله اول آزمون دلفی)**

مواردی که ۷۵ درصد و بیشتر مورد موافقت قرار گرفته‌اند	
عدم استفاده از اطلاعات سلامت بدون رضایت فرد مربوطه	
عدم استفاده و افشای اطلاعات سلامت:	برای مقاصد خارج از چرخه مراقبت و درمان مگر با رضایت فرد مربوطه
استفاده و افشای اطلاعات سلامت برای:	برای یک شخص، هیأت یا آزمای غیر از فرد مربوطه مگر با اطلاع یا رضایت فرد مربوطه
سلامت برای:	مقاصد خارج از چرخه مراقبت و درمان، تحت مواردی که قانون تعیین نموده یا برای حفظ منافع عمومی دادگاه‌ها توسط بخش دولتی
در صورت افشای یا استفاده از اطلاعات سلامت، ثبت یک یادداشت در پرونده مبنی بر افشای یا استفاده از اطلاعات	
الف: پیشگیری، بازرسی، تحقیق، پیگرد قانونی یا مجازات عمل مجرمانه و نقض قانون	
ب: اجرای قوانین مرتبط با اعتراف به اقدامات مجرمانه	
ج: تعیین یا سرمایه‌گذاری یا پرداخت هزینه مراقبت	
د: تضمین کیفیت یا استانداردها	
ه: مواردی که فرد قادر به رضایت دادن نیست، به منظور تماس با خویشاوند یا دوست فرد	
و: کاهش یا پیشگیری تهدید جدی برای زندگی یا سلامت فرد مربوطه یا سایرین	
ز: ممیزی اطلاعات در صورت تخریب اطلاعات بلافاصله بعد از ممیزی	استفاده و افشای اطلاعات سلامت فرد بدون رضایت وی برای:
ح: آموزش فراهم کنندگان خدمت سلامت	
ل: قیم فرد یا فردی که از طرف او تعیین شده در صورت عدم توانایی و صلاحیت قانونی خود فرد به رضایت دادن	
م: ارائه مراقبت یا درمان مناسب فرد	
ن: قیم یا وکیل فرد محدود به میزان قابل قبول و ضروری	
س: مقاصد تحقیقاتی بدون ذکر نام بیمار	
ع: متولی دیگری جهت پیشگیری از تقلب و سوء استفاده از خدمات سلامت، برنامه‌ریزی، مدیریت سیستم، پایش، ارزیابی، تخصیص یا پایش منابع و تجویز داروهای خاص	
ف: نظارت بر سلامت عمومی و سایر مقاصد سلامت عمومی	
ص: کمک به خدمت دهنده به منظور انجام و ظایفش یا توسعه سیستم عمومی	
اعمال جرمه‌های مدنی و کیفری برای افشای غیر مجاز اطلاعات سلامت بیمار	
مواردی که بین ۵۰ تا ۷۵ درصد مورد موافقت قرار گرفته‌اند	
عدم استفاده و افشای اطلاعات سلامت:	توسط شخص دریافت‌کننده اطلاعات برای منظوری غیر از آنچه که اطلاعات به آن منظور داده شده
استفاده و افشای اطلاعات سلامت:	در صورت توجیه شدن متولی اطلاعات فقط برای مقاصد خاصی به هنگام ضرورت
مواردی که کمتر از ۵۰ درصد مورد موافقت قرار گرفته‌اند	
استفاده و افشای اطلاعات سلامت برای:	مقاصد خارج از چرخه مراقبت و درمان، در صورت عدم امکان کسب رضایت فرد قبل از استفاده یا افشای سلامت برای:
سلامت بدون رضایت وی برای:	دادگاه‌ها توسط بخش خصوصی
استفاده و افشای اطلاعات سلامت برای:	ط: تغییر اطلاعات برای پنهان کردن هویت فرد
سلامت فرد بدون رضایت وی برای:	ک: بازاریابی مستقیم
	ق: اعضای خانواده فرد
	ر: افراد دیگری که ارتباط شخصی نزدیکی با بیمار دارند
	ش: متقاضی در مورد اطلاعات سلامت فرد فوت شده



### جدول ۳: اصول دسترسی فرد به اطلاعات پرونده سلامت الکترونیک از دیدگاه کارشناسان (در مرحله اول آزمون دلغی)

مواردی که ۷۵ درصد و بیشتر مورد موافقت قرار گرفته‌اند	
دسترسی داشتن فرد به اطلاعات سلامت خود بر اساس درخواست	
الف: امکان وجود تهدید جدی و حتمی برای زندگی یا سلامت هر فرد	
ب: امکان افشای اطلاعات شخص دیگر	
و: مغایرت با قانون	عدم دسترسی فرد به اطلاعات سلامت در صورت:
ز: لطمه به پیشگیری، بازرسی، تحقیق، پیگرد قانونی یا تنبیه عمل مجرمانه	
ح: لطمه به اجبار قانونی در ارتباط با اعتراف به اقدامات مجرمانه	
ط: لطمه به حفظ منافع عمومی	
شمول قوانین دسترسی به اطلاعات سلامت برای بخش خصوصی علاوه بر بخش دولتی	
شمول قوانین دسترسی به اطلاعات سلامت برای مستندات نگهداری شده در سازمانی غیر از سازمان ارائه دهنده خدمت	
مواردی که بین ۵۰ تا ۷۵ درصد مورد موافقت قرار گرفته‌اند	
ج: درخواست بیهوده یا بی‌دلیل برای دسترسی	
د: ارتباط اطلاعات به اقدامات قانونی بین سازمان و فرد	عدم دسترسی فرد به اطلاعات سلامت در صورت:
ه: آشکارسازی ولطمه به اهداف سازمان در ارتباط با مذاکرات یا فرد	
ی: گردآوری اطلاعات برای بررسی همگنان، کمیته استانداردها یا ارزیابی مدیریت خطر	
دسترسی افراد به تمام انواع اطلاعات ثبت شده بر پایه صریح نیاز به دانستن	

### جدول ۴: شرایط نگهداری اطلاعات پرونده سلامت الکترونیک از دیدگاه کارشناسان (در مرحله اول آزمون دلغی)

مواردی که ۷۵ درصد و بیشتر مورد موافقت قرار گرفته‌اند	
حفظ اطلاعات سلامت از استفاده نایجا، خسارت، دسترسی غیر مجاز، تغییر یا افشاء	
تصحیح، کامل و روزآمد نمودن اطلاعات سلامت	
نگهداری اطلاعات سلامت به میزان کافی، مرتبط و غیر زاید	
وجود مقیاس‌های مناسبی برای نگهداری و دسترسی مناسب به اطلاعات سلامت	
وجود استانداردهایی برای نگهداری اطلاعات سلامت و تضمین استمرار و تسهیل دسترسی به اطلاعات توسط افراد مجاز	
وجود سیاست مکتوبی درباره نگهداری اطلاعات سلامت	
عدم صلاحیت سازمان‌ها جهت حذف اطلاعات بالینی قبل از زمان قانونی انقضاء اطلاعات	
نگهداری تمامی دسترسی‌ها به اطلاعات سلامت و ردیابی داده‌ها در پرونده	
مواردی که بین ۵۰ تا ۷۵ درصد مورد موافقت قرار گرفته‌اند	
عدم نگهداری اطلاعات سلامت افراد بیش از زمان لازم	



**جدول ۵: مسئولیت‌های متولی اطلاعات پرونده سلامت الکترونیک از دیدگاه کارشناسان  
(در مرحله اول آزمون دلفی)**

مواردی که ۷۵ درصد و بیشتر مورد موافقت قرار گرفته‌اند	
ارزیابی تأثیر خصوصی بودن اطلاعات سلامت بر جمع‌آوری، استفاده و افشای اطلاعات	
حفظ اطلاعات سلامت به هنگام افشاء یا انتقال اطلاعات از فقدان، استفاده، تغییر، دسترسی یا افشای غیر مجاز	
پیروی و اجرای سیاست‌ها و اقدامات قانونی مربوطه	
تعیین فرد رابط یا قیمی برای تضمین رعایت و پیروی از قانون	
اعلام استفاده یا افشای اطلاعات سلامت بدون رضایت فرد به وی و اخذ رضایت فرد در صورت استمرار استفاده یا افشاء	
دسترسی واضح عموم به سیاست‌ها و اقدامات محرمانگی اطلاعات	
تهیه حفاظت‌های ایمنی مناسب توسط متولیان که اطلاعات سلامت را به مدیر اطلاعات می‌سپارند	
ایجاد حفاظت‌های اداری، فنی و فیزیکی اطلاعات و آگاهی تمامی عوامل متولی اطلاعات سلامت از آنها	
تداوم حفاظت‌های اداری، فنی و فیزیکی	
اطمینان از صحیح، کامل و روزآمد بودن اطلاعات	
افشای اطلاعات برای شخص مجاز به دریافت اطلاعات	
بکارگیری ضمانت‌های اجرایی مناسب برای تخلف از الزامات محرمانگی اطلاعات	
ایجاد اخطارهای مقتضی درباره محدودیت‌های افشای اطلاعات در پرونده‌ها	
قبول مسئولیت: ج: فرد بیمار به عنوان مالک داده‌ها	
ایجاد هیأتی برای سرپرستی حفظ محرمانگی اطلاعات	
ممنوعیت انتقال اطلاعات سلامت برای کشور فاقد سطوح حفاظت کافی از محرمانگی اطلاعات	
الف: قانونی و الزام‌آور بودن دریافت اطلاعات و پیروی از قوانین جابه‌جایی اطلاعات	انتقال اطلاعات سلامت به خارج از کشور
ب: رضایت فرد برای انتقال اطلاعات	در صورت:
ج: انتقال اطلاعات برای نفع فرد	
الف: فراهم کننده خدمت است	مسئولیت عدم دسترسی سریع به
ب: متولی اطلاعات سلامت است	اطلاعات سلامت برای مراقبت از بیمار بر
ج: هیأت سرپرست محرمانگی اطلاعات است	عهده:
مواردی که بین ۵۰ تا ۷۵ درصد مورد موافقت قرار گرفته‌اند	
مجاز به خودداری از دادن اطلاعات به فرد بیمار در صورت ملزم یا مجاز بودن به این امر	
ب: متولیان اطلاعات سلامت به عنوان مالک داده‌ها	قبول مسئولیت:
د: هیأت سرپرست محرمانگی اطلاعات به عنوان مالک داده‌ها	
مواردی که کمتر از ۵۰ درصد مورد موافقت قرار گرفته‌اند	
الف: فراهم کنندگان خدمت به عنوان مالک داده‌ها	قبول مسئولیت:
انتقال اطلاعات سلامت به خارج از کشور در صورت عدم امکان کسب رضایت از فرد	
مسئولیت عدم دسترسی سریع به اطلاعات سلامت برای مراقبت از بیمار بر عهده فرد بیمار است	



### جدول ۶: اصول محرمانگی اطلاعات پرونده سلامت الکترونیک از دیدگاه کارشناسان (در مرحله دوم آزمون دلفی)

شرایط جمع‌آوری اطلاعات سلامت (مواردی که ۷۵ درصد و بیشتر مورد موافقت قرار گرفته‌اند)	
جمع‌آوری اطلاعات توسط سازمان:	برای انجام وظایف یا فعالیت‌های همان سازمان
	مشروط بر ناشناس کردن اطلاعات قبل از افشای آن توسط سازمان جمع‌آوری‌کننده اطلاعات
اصول استفاده از اطلاعات سلامت (مواردی که ۷۵ درصد و بیشتر مورد موافقت قرار گرفته‌اند)	
استفاده از اطلاعات سلامت فرد بدون رضایت وی:	به هنگام ضرورت برای مقاصد خاص در صورت توجیه شدن متولی اطلاعات در خصوص لزوم استفاده از اطلاعات
	جهت تعیین وضعیت او برای دریافت مراقبت درمانی فعلی
اصول افشاء اطلاعات سلامت (مواردی که ۷۵ درصد و بیشتر مورد موافقت قرار گرفته‌اند)	
	افشای اطلاعات سلامت فرد بیمار توسط شخص دریافت‌کننده اطلاعات برای اهدافی غیر از آنچه که اطلاعات برای آن جمع‌آوری شده است با رضایت وی
اصول دسترسی فرد به اطلاعات سلامت خود (مواردی که ۷۵ درصد و بیشتر مورد موافقت قرار گرفته‌اند)	
	امکان دسترسی فرد به اطلاعات خود وجود داشته باشد مگر در صورت گردآوری اطلاعات برای ارزیابی و کمیته استاندارد
	دسترسی افراد به تمام اطلاعات ثبت شده خود بر اساس اصل صریح نیاز به دانستن
شرایط نگهداری اطلاعات سلامت در سازمان (مواردی که ۷۵ درصد و بیشتر مورد موافقت قرار گرفته‌اند)	
نگهداری اطلاعات سلامت افراد:	تا زمان قانونی مصوب
	بیش از زمان قانونی مصوب در صورت نیاز سازمان متولی اطلاعات
اعمال مجازات‌هایی برای تخریب یا امحای پرونده‌های الکترونیکی قبل از موعد قانونی آن	
مسئولیت‌های متولی اطلاعات سلامت (مواردی که ۷۵ درصد و بیشتر مورد موافقت قرار گرفته‌اند)	
الف: واگذاری مالکیت داده‌های پرونده سلامت الکترونیک علاوه بر فرد بیمار بر عهده متولیان اطلاعات سلامت	
ب: واگذاری مالکیت داده‌های پرونده سلامت الکترونیک علاوه بر فرد بیمار بر عهده هیأت سرپرست محرمانگی اطلاعات	
اصول دسترسی فرد به اطلاعات سلامت خود (مواردی که کمتر از ۵۰ درصد مورد موافقت قرار گرفته‌اند)	
الف: بیهوده و بی‌دلیل بودن درخواست برای دسترسی به اطلاعات	
ب: ارتباط اطلاعات با اقدامات قانونی بین سازمان و فرد و امکان پایمال شدن حقی بدلیل دسترسی به اطلاعات	امکان دسترسی فرد به اطلاعات خود وجود داشته باشد مگر:
ج: موجب آشکارسازی و لطمه به اهداف سازمان در ارتباط با مذاکرات موجود بین سازمان و فرد بیمار گردد	
تحويل مدارک پرونده بیمار به خود وی در صورت ضرورت امحاء پرونده طبق قانون	

در پرونده سلامت الکترونیک و از طرفی عدم وجود اصول مدون و هماهنگ در این خصوص در کشور، به نظر می‌رسد شرایط موجود موجب اعمال سلیقه و عدم رعایت کامل حق بیمار گردیده است. با عنایت به اهمیت موضوع و آغاز طراحی پرونده سلامت الکترونیک در وزارت بهداشت، درمان و آموزش پزشکی، توصیه می‌گردد برای این منظور فرم رضایت‌نامه الکترونیک جامعی طراحی شود و رضایت

بین المللی حقوق بیمار تطابق وجود نداشته است و بسیاری از حقوق مسلم بیمار در منشور حقوق بیماران مد نظر قرار نگرفته است. این امر نشان می‌دهد که وزارت بهداشت ایران در زمینه حقوق بیمار و رضایت آگاهانه تقریباً استاندارد را تدوین نکرده است یافته‌های مذکور با یافته‌های پژوهش همخوانی ندارد. با توجه به تأکید اکثریت صاحب نظران بر کسب رضایت بیماران برای جمع‌آوری اطلاعات سلامت





بیمار به عنوان محور اصلی شرایط جمع‌آوری اطلاعات مورد توجه جدی قرار گیرد.

یافته‌ها نشان می‌دهد که صاحب‌نظران بر عدم استفاده از اطلاعات سلامت بدون رضایت بیمار تأکید دارند و استفاده از اطلاعات سلامت فرد برای مقاصد خارج از چرخه مراقبت و درمان را فقط با رضایت فرد مربوطه مجاز می‌دانند مگر اینکه استفاده در موارد قانونی یا برای حفظ منافع عمومی صورت گیرد. نتایج مطالعه تطبیقی نشان داد که هر سه کشور استرالیا، کانادا و انگلستان نیز بر موارد مذکور تأکید دارند. [۱۸-۱۵] کلاگ در پژوهش استرالیا در سال ۱۹۹۵ بیان می‌کند که داده‌های پرونده باید برای مقاصد قانونی مجاز مورد استفاده قرار گیرند [۲۳] که با یافته‌های این پژوهش همخوانی دارد. طبق پژوهش بهنام [۱۰] و فرزندی پور [۲۴]، در ایران در اکثریت موارد جهت استفاده از اطلاعات پرونده در سیستم دستی ضوابط خاصی وجود ندارد و دسترسی به اطلاعات توسط متخصصان درمانی در سیستم دستی در اکثر موارد با درخواست پزشک و استفاده کارکنان در اغلب موارد متناسب با مسئولیت شخصی و اختیار آنها جهت اداره امور بیمارستان صورت می‌گرفت. یافته‌های مذکور با یافته‌های این پژوهش مغایرت دارد. به نظر می‌رسد به دلیل عدم وجود اصول محرمانگی اطلاعات به صورت مدون و مصوب، مراکز درمانی به صورت موردی و بر اساس شرایط اقدام نموده و عملاً در این خصوص توجهی به حق بیمار نمی‌کنند. با توجه به قابلیت‌های پرونده سلامت الکترونیک و افزایش امکان دسترسی به اطلاعات و توزیع آن، لازم است که کمیته محرمانگی و ایمنی اطلاعات سلامت در حوزه وزارت بهداشت با حضور متخصصین مدیریت اطلاعات سلامت تشکیل و نسبت به تدوین چارچوب محرمانگی و ایمنی اطلاعات مشتمل بر مجموعه‌ای از سیاست‌ها و اقدامات و دستورالعمل‌های سازمانی در این خصوص اقدام نمایند.

طبق نظرات صاحب‌نظران در الگوی پیشنهادی، افشای اطلاعات پرونده سلامت الکترونیک برای مقاصد خارج از چرخه مراقبت و درمان تحت قانون یا برای حفظ منافع عمومی و افشای اطلاعات تحت شرایطی خاص مورد تأیید قرار گرفته است و افشای اطلاعات سلامت برای دادگاه‌ها

فقط توسط بخش دولتی لازم دانسته شده و اعمال جریمه‌های مدنی و کیفری برای افشای غیر مجاز اطلاعات سلامت بیمار را مجاز دانسته‌اند. یافته‌های مطالعه تطبیقی نشان داد که در هر سه کشور منتخب، افشای اطلاعات پرونده سلامت الکترونیک برای مقاصد خارج از چرخه مراقبت و درمان تحت قانون یا برای حفظ منافع عمومی امکان‌پذیر است. [۱۵-۱۸] و استرالیا و کانادا، افشای اطلاعات سلامت فرد بدون رضایت وی را تحت شرایط و اصول خاصی مجاز دانسته‌اند، ضمن این که در کشورهای منتخب از افشای اطلاعات برای دادگاه‌ها توسط بخش خصوصی و اعمال جریمه برای افشای غیر مجاز اطلاعات سخنی به میان نیامده است. [۱۶، ۱۷] کلاگ در پژوهشی بیان می‌کند که داده‌های پرونده بیمار نباید به صورت بیرونی افشای شود مگر با رضایت رسمی فرد مربوطه یا بر حسب اختیار قانونی و یا اقدام در فرایند قانون باشد. [۲۳] بر اساس قوانین ولز جنوبی، دادگاه حق دسترسی به پرونده‌های ایجاد شده در بخش خصوصی را ندارد. [۲] قوانین ایالتی آمریکا برای نقض مقررات محرمانگی هم جریمه‌های مدنی و هم کیفری اعمال می‌کند. [۱۳] یافته‌های مذکور با یافته‌های این پژوهش مطابقت دارد. بر اساس پژوهش بهنام و فرزندی پور در مورد پرونده‌های بیماران در سیستم دستی، در اکثریت موارد جهت ارائه و افشای اطلاعات بیماران ضوابط خاص و خط مشی یکنواختی وجود نداشته است. [۱۰، ۲۴] بر اساس پژوهش زاهدی فر [۱۹] و صلاحی [۲۵]، ۹ درصد واحدهای مورد مطالعه برای افشای اطلاعات بیماران خارج از مرکز درمانی از بیمار رضایت کتبی می‌گرفتند و تنها ۲۸۶ درصد بیمارستان‌ها دارای دستورالعملی در زمینه افشای اطلاعات مدارک پزشکی در سیستم دستی بودند. یافته‌های مذکور با یافته‌های این پژوهش مغایرت دارد. به نظر می‌رسد با توجه به تحقیقات انجام شده در ایران به فاصله ۱۰ سال، عملاً همچنان ضوابط و اصول خاصی بر افشای اطلاعات بیماران حاکم نیست و متولیان امر نسبت به ایجاد ضوابط بی‌تفاوت یا بی‌اطلاع بوده‌اند. ضمناً با توجه به نقش بخش خصوصی در حوزه بهداشت و درمان کشور و لزوم نظارت بر عملکرد بخش خصوصی، علی‌رغم نظرات صاحب‌نظران لازم است



مناسبی از اطرافیان بیمار گذاشته شود. یافته‌های مذکور با یافته‌های این پژوهش مطابقت دارد. یافته‌های مطالعه تطبیقی نشان داد که در استرالیا و کانادا بر عدم دسترسی فرد به اطلاعات سلامت خود در صورت بیهوده و بی دلیل بودن درخواست دسترسی، ارتباط اطلاعات با اقدامات قانونی بین سازمان و فرد و آشکار سازی و لطمه به اهداف سازمان در ارتباط با مذاکرات موجود بین سازمان و فرد بیمار تأکید شده است. [۱۷، ۱۶] نتایج پژوهش بهنام نشان داد که بندرت با بیمار در رابطه با بیماری، اقدامات و نحوه درمان وی صحبت می شود و بیمار در اکثر موارد هیچگونه دسترسی به اطلاعات پزشکی مربوط به خود در سیستم دستی نداشته است. [۱۰] زاهدی فرد در پژوهشی نتیجه گرفت که ۳۶/۴ درصد واحدها، در مواردی که به تشخیص پزشک، بیمار از شرایط روحی و روانی مناسبی برخوردار باشد، اجازه دسترسی به پرونده در سیستم دستی به وی داده می شود. [۱۹] پژوهش سال ۱۹۹۹ مؤسسه سلامت ولز جنوبی استرالیا در خصوص مشکلات دسترسی مشتری به پرونده نشان داد که مشتریان در بیمارستان‌ها یا از طریق پزشکان خانواده به پرونده‌ها دسترسی کمی دارند یا به پرونده‌ها دسترسی ندارند. [۲۷] این یافته‌ها با یافته‌های این پژوهش همخوانی ندارد. به نظر می رسد جهت حفظ حقوق بیمار و با این اعتقاد که داده‌های پرونده متعلق به بیمار است، تمامی کشورهای مورد مطالعه بر ضرورت دسترسی بیمار به اطلاعات پرونده خود جز در برخی موارد تأکید دارند و لازم است این مسئله توسط تمامی سازمان‌ها اعم از خصوصی و دولتی مورد توجه قرار گیرد. توصیه می شود در طراحی پرونده سلامت الکترونیک، شناسه سلامت واحد برای تمامی مشتریان سلامت ایجاد گردد و چگونگی دسترسی فرد بیمار به پرونده خود و مکانیسم آن مد نظر قرار گیرد، زیرا آگاهی بیمار از اطلاعات پرونده خود موجب ارتباط بهتر و عادلانه تر پزشک با بیمار شده رضایت آگاهانه را ارتقا داده و استمرار مراقبت بین فراهم کنندگان مختلف را تضمین می کند و به مشتری کنترل بیشتری بر سلامت خودش می دهد. [۲۸]

نظرات صاحب نظران در الگوی پیشنهادی بر تصحیح، کامل و روزآمد نمودن اطلاعات سلامت تأکید دارد و

که هم بخش خصوصی و هم بخش دولتی پاسخگویی اطلاعات مورد نیاز دادگاه‌ها بوده و پرونده بیماران را در صورت درخواست، در اختیار دادگاه‌ها قرار دهند، ضمن اینکه ضوابط قانونی و ضمانت‌های اجرایی لازم برای تضمین حفظ محرمانگی اطلاعات پرونده سلامت الکترونیک و تخطی از سیاست‌های محرمانگی اطلاعات و افشاء غیر مجاز آن تدوین و به اجرا در آید.

بر اساس نظرات صاحب نظران در الگوی پیشنهادی، دسترسی فرد به اطلاعات سلامت خود بر اساس درخواست و بر پایه صریح نیاز به دانستن مجاز شمرده شده، ضمن اینکه محدودیت‌هایی برای دسترسی فرد به اطلاعات سلامت خود در نظر گرفته شده است. همچنین برای اجرای قوانین دسترسی فرد به اطلاعات سلامت خود هم در بخش خصوصی و هم بخش دولتی و هم سازمانی غیر از سازمان ارائه دهنده خدمت سلامت تأکید شده است و عدم دسترسی فرد به اطلاعات سلامت خود در صورت بیهوده و بی دلیل بودن درخواست دسترسی، ارتباط اطلاعات با اقدامات قانونی بین سازمان و فرد و آشکار سازی و لطمه به اهداف سازمان در ارتباط با مذاکرات بین سازمان و فرد بیمار، مورد تأیید قرار نگرفته است. مطالعه تطبیقی حاکی از آن است که کانادا و استرالیا بر دسترسی فرد به اطلاعات سلامت خود بر اساس درخواست تأکید دارند و دسترسی فرد به اطلاعات سلامت خود در تحت شرایط خاصی مجاز ندانسته اند [۱۸-۱۶] و انگلستان بدون هیچ گونه محدودیتی دسترسی افراد به تمام انواع اطلاعات ثبت شده بر پایه صریح نیاز به دانستن را مجاز شمرده است. [۱۵] بر اساس یافته‌ها در سال ۲۰۰۰، در استرالیا قانون خصوصی بودن و دسترسی به پرونده‌های سلامت برای پرونده‌های بخش خصوصی و دولتی و هم چنین برای مستنداتی به کار می رفته که در سازمانی غیر از سازمان ارائه کننده خدمات سلامت نگهداری می شدند. [۶] بیانیه انجمن بیمارستان‌های آمریکا [۲۶] و پژوهش گلاک [۲۳] اعلام می کند که بیمار باید حق دسترسی به اطلاعات پرونده سلامت الکترونیک و کسب اطلاعات تشخیصی و درمانی از پزشک خود داشته باشد و زمانی که در اختیار گذاشتن چنین اطلاعاتی به صلاح نیست، اطلاعات باید در اختیار شخص



نگهداری اطلاعات سلامت افراد را بیش از زمان قانونی مصوب در صورت نیاز سازمان متولی اطلاعات مجاز می‌داند، ضمن اینکه اعمال مجازات‌هایی برای تخریب یا امحای پرونده الکترونیکی قبل از موعد قانونی آن را لازم دانسته است. یافته‌های مطالعه تطبیقی نشان داد که هر سه کشور منتخب بر تصحیح، کامل و روزآمد نمودن اطلاعات سلامت تأکید دارند. [۱۵-۱۸] اندرسن (Anderson) در سال ۱۹۹۷ در اصول ایمنی خود عنوان نموده که هیچکس صلاحیت حذف اطلاعات بالینی را ندارد مگر اینکه دوره زمانی مقتضی آن، منقضی شده باشد. [۲۹] دیویس و لاکور (Davis Lacour) در سال ۲۰۰۲ چنین اظهار کرده‌اند که داده‌ها برای سودمند واقع شدن باید صحیح باشند. اگر داده‌ها صحیح نباشند، تصورات و دانش نادرست به کاربران انتقال می‌یابد. کامل بودن داده‌ها به گردآوری یا ثبت داده‌ها به صورت تمام و کمال اشاره دارد. همچنین اطلاعات باید به هنگام ارائه، به روز باشد. [۳۰] یافته‌های مذکور با یافته‌های این پژوهش همخوانی دارد. بر اساس یافته‌های مطالعه تطبیقی در سه کشور منتخب نگهداری اطلاعات سلامت افراد بیش از زمان لازم مجاز نمی‌باشد. [۱۵-۱۸] صلاحی در پژوهشی نتیجه گرفت که در ایران رویه‌ای برای امحاء پرونده‌های کاغذی وجود ندارد و دستورالعمل مدت نگهداری پرونده‌ها تنها در ۱۱ درصد موارد رعایت می‌شود [۲۵] که با یافته‌های این پژوهش مغایرت دارد. با توجه به اهمیت لزوم نگهداری اطلاعات بیماران در پرونده سلامت الکترونیک به طور صحیح و کامل و از طرفی تعریف وزارت بهداشت، درمان و آموزش پزشکی ایران از پرونده سلامت الکترونیک [۱] حفظ اطلاعات از امحاء و تخریب و جلوگیری از دستکاری و تحریف آن تا زمان مورد نیاز کاملاً ضروری به نظر می‌رسد، لذا پیشنهاد می‌شود یک مخزن مرکزی داده‌های پرونده سلامت الکترونیک در هر استان یا در سطح وزارت بهداشت ایجاد شود که قابلیت نگهداری ایمن اطلاعات تمامی مشتریان سلامت را تا زمان قانونی مصوب در ایران داشته باشد و با عنایت به عدم رعایت ضوابط موجود در پرونده‌های دستی، مجازات‌هایی در مورد افراد یا سازمان‌هایی که بدون رعایت موارد قانونی اقدام به تخریب یا

امحاء و یا حتی بی‌مبالاتی در حفظ و نگهداری پرونده‌های کامپیوتری می‌کنند اعمال گردد. نظرات صاحب‌نظران در الگوی پیشنهادی بر دسترسی عموم به سیاست‌ها و اقدامات محرمانگی اطلاعات پرونده سلامت الکترونیک به طور واضح تأکید دارد، تعیین فرد رابط یا قیمی را برای تضمین رعایت و پیروی از قانون لازم می‌دانند و بکارگیری ضمانت‌های اجرایی مناسب برای تخلف از الزامات محرمانگی اطلاعات را ضروری می‌دانند. همچنین واگذاری مالکیت داده‌ها علاوه بر فرد بیمار به متولیان اطلاعات سلامت و هیأت سرپرست محرمانگی اطلاعات، ممنوعیت انتقال اطلاعات سلامت برای کشورهای فاقد سطوح حفاظت کافی از محرمانگی اطلاعات، انتقال اطلاعات سلامت افراد به خارج از کشور تحت شرایطی خاص و مسئولیت عدم دسترسی سریع به اطلاعات سلامت برای مراقبت از بیمار بر عهده فراهم‌کننده خدمت، متولی اطلاعات و هیأت سرپرست محرمانگی اطلاعات مورد تأیید قرار گرفته است. یافته‌های مطالعه تطبیقی نیز بر موارد مذکور تأکید دارد اما در خصوص مالکیت داده‌ها، چگونگی انتقال اطلاعات به سایر کشورها و مسئولیت عدم دسترسی سریع به اطلاعات صراحتاً اشاره‌ای نشده است. [۱۷-۱۵] دستورالعمل حفظ داده‌های اتحادیه اروپا در اکتبر سال ۱۹۹۸، انتقال اطلاعات را برای هر کشوری که فاقد سطوح حفاظت کافی باشد منع می‌کند مگر اینکه این کار با رضایت بیمار صورت گیرد [۳۱] فولر و جفریز (Fuller Jeffries) مسئولیت شاغلین مدیریت اطلاعات بهداشتی را در مورد حفاظت از اطلاعات، آگاهی از قوانین محرمانگی اطلاعات، اطمینان از اجرای قوانین و پایش محتویات هر پرونده پزشکی می‌دانند. [۳۲] دنیس کالاهان (Denis Callahan) در مقاله‌ای بیان کرده است که نیازهای سازمان خدمات درمانی برای مسئول محرمانگی با سایر مشاغل فرق دارد و شاغلین مدیریت اطلاعات بهداشتی بنابر خاصیت آموزش‌ها و تجاربی که دارند، بسیاری از مهارت‌های مورد نیاز را دارا می‌باشند. [۳۳] پژوهش بهنام [۱۰] و زاهدی فر [۱۹]، نشان داد که در کشور پرسنل مدارک پزشکی به عنوان حافظ محرمانگی اطلاعات بیماران در بیمارستان محسوب شده و ضمن

## فهرست منابع

1. Riazi H, Fathiroodsari B, Bitaraf E. Electronic Health Record, Concepts, Standards and Development Approaches. Tehran: Ministry of Health, Treatment and Medical Education; 2007. [Persian]
2. Carter M. should patients have access to their Medical records? The Medical Journal of Australia 1998; 169: 96-70.
3. Commonwealth of Australia. International approaches to the electronic health record. 2003 January. Available from: URL: <http://www.healthconnect.gov.au>.
4. National committee on vital and Health statistics. Information for health. 2001 November. Available from: URL: <http://www.ncvhs.com>.
5. National electronic health Records taskforce. A National Approach to electronic health Records for Australia. 2000 March. Available from: URL: <http://www.healthconnect.gov.au>.
6. National electronic health Records taskforce. A health information Network for Australia. 2000 July. Available from: URL: <http://www.health.gov.au>.
7. Lyons R, Payne C, McCabe M, Fielder C. legibility of doctor's hand writing: quantitative comparative study. BMJ 1998; 317: 863-4.
8. Woodward B. The computer-based patient record and confidentiality. New England Journal of Medicine 1995; 333: 1419-22.
9. HIMSS. HIMSS National health information infrastructure survey. 2004 July. Available from: URL: <http://www.himss.org/content/files/healthinfoInfrastructureSurvey.pdf>.
10. Behnam S. A Comparative Study of Accessibility levels Confidentiality of Medical Records in Selected Countries. [M.Sc. Thesis]. School of Management and Medical Information Science, Iran university of Medical Sciences; 2005. [Persian]

آشنایی آنان با رازداری و محرمانگی اطلاعات بیماران، پاسخگوی موضوعات محرمانگی اطلاعات و رعایت مقررات حفظ امنیت اطلاعات پرونده بیماران می باشند، که با یافته های این پژوهش مطابقت دارد. بررسی انجام شده نشان داد که طبق قانون فعلی استرالیا، بیماران مالک پرونده های کامپیوتری مربوط به خود نیستند. در آمریکا، مسئله مالکیت داده های پرونده های کامپیوتری حل نشده است [۳۴] که با یافته های این پژوهش مغایرت دارد. به نظر می رسد برای حفظ و نگهداری پرونده بیماران افرادی تحت عنوان متخصص مدارک پزشکی تربیت می شوند که مسئولیت مدارک پزشکی بیماران بر عهده آنان گذاشته می شود. لذا لازم است همین افراد مسئولیت پرونده سلامت الکترونیک را در آینده به عهده بگیرند و مراجع ذی صلاح ضمن تدوین اصول قانونی لازم و تکمیل و اصلاح شرح وظایف این افراد آنها را به عنوان قیم پرونده سلامت الکترونیک و مسئول رعایت و پیروی از قوانین محرمانگی اطلاعات بشناسند. با توجه به اینکه مالکیت داده های پرونده های کامپیوتری هنوز به طور کامل حل نشده است لازم است تولید پرونده های سلامت الکترونیک مورد توجه قرار گرفته و بر عهده متولیان اطلاعات سلامت گذاشته شود، به طوری که ضمن رعایت اصول محرمانگی اطلاعات، مسئولیت عدم دسترسی سریع به اطلاعات سلامت در مواقع لزوم بر عهده آنان باشد.

با توجه به رویکرد وزارت بهداشت درمان و آموزش پزشکی در ایجاد پرونده سلامت الکترونیک برای هر ایرانی و نگرانی های افزایش دسترسی به اطلاعات ناشی از راه اندازی پرونده سلامت الکترونیک و از طرفی عدم وجود قوانین مدون و جامعی در این زمینه در کشور، بکارگیری الگوی جامع اصول محرمانگی اطلاعات پرونده سلامت الکترونیک و تصویب قوانین محرمانگی اطلاعات با توجه به الگوی پیشنهادی برای کشور توصیه می شود.

تقدیر و تشکر: از زحمات سرکار خانم اکبرزاده کارشناس محترم مدارک پزشکی سازمان پزشکی قانونی که پژوهشگران را در تکمیل پرسشنامه هایاری نمودند صمیمانه تشکر و قدردانی می نمایم.

- Hospitals Sponsored by Isfahan University of Medical Sciences [M.Sc Thesis]. Management and Medical Information Science School, Iran University of Medical Sciences; 2001. [Persian]
21. Mohammadpour A. A Comparative Study on the Hospital Standards of Ministry of Health and International Standards of Joint Commission on Accreditation of Hospitals [M.Sc Thesis]. Management and Medical Information Science School, Iran University of Medical Sciences; 2006. [Persian]
22. Sarbazzarinabad M. A Comparative Investigation of Patients' Rights Charter in Some Selected Countries and Finding a Suitable Solution for Iran [M.Sc Thesis]. Management and Medical Information Science School, Iran University of Medical Sciences; 2002. [Persian]
23. Kluge EH. Patients, patient records, and ethical principles. MEDINFO 1995; 8:1596-600.
24. Farzandipour M. An Investigation on Policies of Delivering Medical Records in Tehran University's Hospitals [M.Sc Thesis]. Management and Medical Information Science School, Iran University of Medical Sciences; 1995. [Persian]
25. 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 [M.Sc Thesis]. Management and Medical Information Science School, Iran University of Medical Sciences; 1998. [Persian]
26. Mcmillar K. Brady being a Medical Record clerk. New Jersey: Prentice Hall Inc; 1992.
27. Advisory Council on Health infostructure. Canada Health infoway. 1999 February. Available from: URL: <http://www.hc-sc.gc.ca>.
28. Consumer's Health Forum of Australia. The use of
11. Drayeh S. A Comparative Investigation of Organization and Procedures in Health Records Departments in Teaching Hospitals. [M.Sc. Thesis]. School of Management and Medical Information Science, Iran university of Medical Sciences; 1995. [Persian]
12. Meidani M. A Comparative Investigation on Standards of Medical Records in Selected Countries and Iran. [M.Sc Thesis]. Management and Medical Information Science School, Iran university of Medical Sciences; 2003. [Persian]
13. Aspen Reference Group. Health information management manual. Maryland: Aspen publication; 1999
14. Farzandipour M. Designing Model of Electronic Health Record Confidentiality and Security Mechanism for Iran. [Ph.D Dissertation]. Management and Medical Information Science School, Iran university of Medical Sciences; 2008. [Persian]
15. National Health Services. IM & T security policy. 2004 November. Available from: URL: <http://www.northumberlandcaretrust.nhs.uk>.
16. Health and the information highway Division, Health Canada. Pan-Canadian Health information privacy and Confidentiality Framework. 2005 January. Available from: URL: <http://www.hc-sc.gc.ca>.
17. The office of the privacy commissioner. National privacy principles. 2001. Available from: URL: <http://www.privacy.gov.au>.
18. The office of the privacy commissioner. Information privacy principles under the privacy Act 1988. 2001. Available from: URL: <http://www.privacy.gov.au>.
19. Taheri H. Is the Physician a Guarantor? Journal of Medicolegal Organization of Iran 1998; 14: 25-30. [Persian]
20. Zahedifar R. An Investigation over the Observance of Patients' Rights in Medical Record Department in



- consumers' health information for research purposes, consumers' health forum of Australia; 1998.
29. Anderson R.J. An update on the BMA security policy. In: Personal Medical Information-Security, Engineering and Ethics. Berlin: Springer; 1997.
30. Davis N, Lacour M. Introduction to Health Information Technology USA. Philadelphia: W.B. Saunders; 2002.
31. European commission, European Union Directive. On the protection of individuals with regard to the processing of personal data and on the free movement of such data. Brussels: European commission; 1995.
32. Fuller B, Jeffries J. From DNA to data privacy. Journal of AHIMA 2001; 72(3): 4-50.
33. Callahan D. The new privacy officer's game plane. Journal of AHIMA 2001; 72(6): 26-32.
34. Tang PC, Hammond WE. A progress report on computer-based patient records in the United States. Washington DC: National Academy press; 1997.



## Designing a Confidentiality Principles Model of Electronic Health Record for Iran; 2007

Farzandipour M.<sup>1</sup> / Sadoughi F.<sup>2</sup> / Ahmady M.<sup>3</sup> / Karimi I.<sup>4</sup>

### Abstract

**Introduction:** Today increasing growing of health information is results in applying of new technologies for suite manages and utilization of information technologies such as electronic health record. A growing capacity of information technologies in collection, storage and transmission of information has added a great deal of concerns since electronic records can be accessed by numerous consumers at various locations. Now considering Iran's new approach to make electronic health records, the basic question is "what is the appropriate model for their confidentiality principles?"

**Methods:** The present study is a descriptive investigation made in Iran in 2007. confidentiality principles of Electronic Health Record, gathered from comparative study that carried out about Australia, Canada and England countries. Then designed initial model. Final model information gathered by questionnaire and use of Delphi Technique. Rate under 50 percent eliminated from model and 75 percent and up added to model. The items from the pattern confirmed among 50 percent up to 75 percent and suggested items from participants, again put to votes.

**Results:** Offered model for our country emphasize on patient consent. no emphasis on the use and release of health information in marketing and purposes outside the care cycle without the patient's consent or any other people having an intimate relation with the patient, and the unavailability to his health information by the patient in certain cases. But in contrast to the selected countries, there is a reference in the suggested model to fines for disclosure of electronic health records, data ownership, and inclusion of information accessibility laws in all organizations, responsibility for inaccessibility to information, and finally the conditions for movement of data abroad.

**Conclusion:** Comprehensive model of Electronic Health Records Confidentiality principles is Designed for Iran and Recommend approve and applying of regulations with usage of proposed model for Protection of Electronic Health Information Confidentiality.

**Keywords:** *Confidentiality Principles, Information Confidentiality, Electronic Health Record, Confidentiality Model*

1- Assistant Professor, School of Paramedical Science, Kashan University of Medical Sciences

2- Assistant Professor, School of Management and Medical Information Science, Iran University of Medical Sciences

3- Associate Professor, School of Management and Medical Information Science, Iran University of Medical Sciences

4- Assistant Professor, School of Management and Economy, Islamic Azad University of Tehran, Science and research branch