الزامات امنیتی پرونده‌ی الکترونیک سلامت در کشورهای منتخب؛ یک مطالعه‌ی تطبیقی*

مهرداد فرزندی پور[1]، فرحناز صدوقی[2]، مریم احمدی[2]، ایرج کریمی[3]

چکیده

مقدمه: امروزه افزایش روزافزون تولید اطلاعات در حوزه بهداشت و درمان، موجب به کارگیری فن‌آوری‌های نوین برای بهره‌برداری مناسب از اطلاعات از جمله ایجاد پرونده‌ی الکترونیک سلامت شده است. ظرفیت روبه رشد فن‌آوری‌های اطلاعات برای جمع‌آوری، ذخیره و انتقال اطلاعات در مقادیر بی‌سابقه، نگرانی‌های قابل درکی برای بیماران ایجاد کرده زیرا پرونده‌ی کامپیوتری از محل‌های متعددی قابل دسترس است و نقص امنیتی آن می‌تواند منجر به افشای صدها یا هزاران پرونده شود. حال با توجه به حرکت کشور به سمت ایجاد پرونده‌ی الکترونیک سلامت، سؤال اساسی این است که آیا الزامات امنیتی آن توسط متولیان امر مورد توجه قرار گرفته است؟

روش بررسی: مطالعه به روش توصیفی – تطبیقی در سال ۸۶ در خصوص الزامات امنیتی اطلاعات پرونده‌ی الکترونیک سلامت کشورهای استرالیا، کانادا، انگلستان و ایران انجام شده است. ابزار گردآوری داده‌ها چک لیست و منابع اطلاعاتی شامل: مقالات، کتب و مجلات به روش مطالعه‌ی متون از کتابخانه‌ها و سایت‌های معتبر انگلیسی زبان مربوط به سال‌های ۱۹۹۵ تا ۲۰۰۶ بوده است. سپس داده‌های گردآوری شده جدول بندی، مورد مقایسه قرار گرفتند و توصیف شدند.

یافته‌ها: کشورهای مورد مطالعه الزاماتی را در خصوص امنیتی پرونده‌ی الکترونیک سلامت، شامل تشکیلات امنیتی اطلاعات، امنیتی طبقه‌بندی و کنترل امکانات، ایمنی منابع انسانی، ایمنی مدیریت ارتباطات و عملیات و ایمنی کنترل دسترسی به اطلاعات پیش‌بینی کرده و به کار می‌برند اما کشور ما فاقد الزاماتی در خصوص امنیتی پرونده‌ی الکترونیک سلامت است.

نتیجه‌گیری: ایمنی اطلاعات پرونده‌ی الکترونیک سلامت یکی از ضروریات ایجاد پرونده‌ی الکترونیک سلامت است و کشور ما فاقد الزاماتی در این زمینه می‌باشد. با توجه به رویکرد وزارت بهداشت، درمان و آموزش پزشکی در خصوص ایجاد پرونده‌ی الکترونیک سلامت برای هر ایرانی، تهیه و تدوین این الزامات توسط متولیان امر با استفاده از تجربیات سایر کشورها توصیه می‌شود.

واژه‌های کلیدی: *راز داری؛ الکترونیک در پزشکی؛ الکترونیک؛ مدارک پزشکی؛ نظام‌های کامپیوتری مدارک پزشکی.*

نوع مقاله: *تحقیقی*

دریافت مقاله: ۸۶/۵/۴ اصلاح نهایی: ۸۶/۷/۹ پذیرش مقاله: ۸۷/۳/۱۱

ارجاع: فرزندی‌پور مهرداد، صدوقی فرحناز، احمدی مریم، کریمی ایرج. الزامات امنیتی پرونده‌ی الکترونیک سلامت در کشورهای منتخب؛ یک مطالعه تطبیقی. مدیریت اطلاعات سلامت ۱۳۸۶؛ ۴(۱): ۱-۹.

مقدمه

امروزه افزایش روزافزون تولید اطلاعات در حوزه‌ی بهداشت و درمان، موجب به کارگیری فن‌آوری‌های نوین برای بهره‌برداری مناسب از اطلاعات در این حوزه شده است. یکی از این فن‌آوری‌ها، ایجاد پرونده‌ی الکترونیک سلامت است. پرونده‌ی الکترونیک سلامت عبارت است از یک پرونده‌ی

*این مقاله برگرفته از پایان‌نامه‌ی دکترای تخصصی می‌باشد.

۱. استادیار مدیریت اطلاعات بهداشتی درمانی دانشگاه علوم پزشکی کاشان (نویسنده‌ی مسوول)

E-mail: farzandipour_m@kaums.ac.ir

۲. استادیار مدیریت اطلاعات بهداشتی درمانی دانشگاه علوم پزشکی ایران

۳. استادیار اقتصاد بهداشت دانشگاه علوم پزشکی ایران

پزشکی بیمار به شکل الکترونیک که برای هدف اولیه ارائه مراقبت سلامت به وسیله‌ی کامپیوترهای یک شبکه قابل دسترس است (۱). ظرفیت روبه رشد فن‌آوری‌های اطلاعات و ارتباطات برای جمع‌آوری، ذخیره و انتقال اطلاعات در مقادیر بی‌سابقه، نگرانی‌های قابل درکی برای بیماران ایجاد کرده است (۲،۳). بیماران نگران دسترسی محدوده‌ی وسیعی از افراد به پرونده‌ی الکترونیک خود می‌باشند (۴ و ۵). پرونده‌ی کامپیوتری از محل‌های متعددی قابل دسترسی است و نقص ایمنی در سیستم آن می‌تواند منجر به افشای صدها یا هزاران پرونده شود (۶). 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 شده است (۷). همچنین بررسی دیگری در خصوص محرمانگی پرونده‌های پزشکی در سال ۸۴ در ایران نشان می‌دهد که در بیشتر موارد برای دسترسی، استفاده و افشای اطلاعات پرونده بیماران ضوابط خاصی وجود ندارد (۸). مطالعه‌ی انجام شده در مراکز درمانی اصفهان در سال ۱۳۸۱ بیانگر این است که در ۸۲ درصد واحدها، مکانیسم‌های حفاظتی مقتضی برای ایمنی پرونده‌های بیماران وجود ندارد (۹). ایجاد چارچوب خصوصی بودن و ایمنی اطلاعات، به مردم امکان می‌دهد که اطلاعات شخصی جمع‌آوری شده درباره‌ی آنها کنترل شود، ضمن آن که جنبه‌های محرمانه و ایمن آن را نیز تضمین می‌کند (۱۰). بنابراین اکنون که سیاست وزارت بهداشت، درمان و آموزش پزشکی استفاده از فن‌آوری اطلاعات به طور گسترده در حوزه‌ی بهداشت و درمان با ایجاد پرونده‌ی الکترونیک سلامت در دست بررسی است، سؤال اساسی این است که آیا جهت تضمین ایمنی اطلاعات، اصول ایمنی اطلاعات پرونده‌ی الکترونیک سلامت تدوین شده است؟

روش بررسی

مطالعه‌ی حاضر به روش توصیفی-تطبیقی در سال ۱۳۸۶-۱۳۸۵ انجام شد. جامعه‌ی پژوهش شامل مکانیسم ایمنی اطلاعات پرونده‌ی الکترونیک سلامت در کشورهای استرالیا، کانادا، انگلستان و ایران بوده است. این مکانیسم‌ها در ۷ محور، شامل الزامات سازماندهی، الزامات ایمنی طبقه‌بندی و کنترل امکانات، الزامات ایمنی منابع انسانی، الزامات ایمنی فیزیکی و محیطی، الزامات ایمنی مدیریت ارتباطات و عملیات، الزامات ایمنی کنترل دسترسی و الزامات ایمنی توسعه و حفظ سیستم‌ها می‌باشد که با یکدیگر مورد مقایسه قرار گرفت.

ابزار گردآوری داده‌ها شامل چک لیست و منابع اطلاعاتی، اسناد، مدارک، مقالات، کتب و مجلات بوده است که از طریق اینترنت و سازمان‌های مربوط به اطلاعات سلامت کشورهای منتخب و با جستجوی کتابخانه‌ای، داده‌ها جمع‌آوری گردید. گردآوری اطلاعات به روش مطالعه‌ی متون از کتابخانه‌ها و سایت‌های معتبر و شناخته شده‌ی اینترنتی از جمله خدمات ملی سلامت انگلیس National Health Services (NHS)، ارتباط سلامتHealth Connect و سلامت پیوسته Health Online استرالیا، شورای مشورتی زیرساخت اطلاعات سلامت Advisory Council of Health Infoway (ACHI) و بزرگراه اطلاعاتی سلامت کانادا Health Infoway انجام شده است. سایت‌های ناشناخته مورد استفاده قرار نگرفته، مقالات مورد استفاده به زبان انگلیسی و مربوط به سال‌های ۱۹۹۵ تا ۲۰۰۶ بوده است. کشورهای منتخب در این پژوهش با استفاده از منابع کتابخانه‌ای، اینترنت و مشاوره با متخصصان و بر اساس ویژگی‌های زیر انتخاب شدند:

ایجاد پرونده‌های به هم متصل بیماران به صورت الکترونیکی یکی از اولویت‌های بسیاری از کشورها است (۱۰). در قاره‌ی اقیانوسیه، دو کشور استرالیا و نیوزیلند پرونده‌ی الکترونیک سلامت دارند اما در خصوص اجرای سبک ملی پرونده‌ی الکترونیک سلامت، استرالیا، سابقه‌ی بیشتری دارد (۱۱). بنابراین از این قاره کشور استرالیا انتخاب گردید. در قاره‌ی آمریکا نیز سه کشور آمریکا، برزیل و کانادا بر روی پرونده‌ی الکترونیک سلامت کار کرده‌اند. برزیل جهت دستیابی به پرونده‌ی الکترونیک یک‌پارچه راه درازی در

پیش دارد. آمریکا و کانادا تا سال ۱۹۷۳ مدل‌های مشابهی از مراقبت سلامت داشتند. سپس تغییرات سیستم کانادا موجب بروز تفاوت عمده‌ای با سیستم آمریکا در این زمینه شد (۱۲). اکنون زیر ساخت اطلاعات سلامت کانادا در خصوص پرونده‌ی الکترونیک سلامت، به خوبی جلوتر از آمریکا است (۱۳)، لذا از این قاره کشور کانادا انتخاب شد. در کشورهای اروپایی، طرح‌های پرونده‌ی الکترونیک سلامت با مدل‌های متفاوتی توسعه یافته است (۱۱). در بین آنها، بریتانیا مبالغ زیادی صرف مدرنیزه کردن مکانیسم جمع‌آوری، ذخیره و استفاده از اطلاعات مراقبت سلامت کرده است که موجب پیشرفت مناسب و مثبتی در این زمینه شده است. لذا به دلیل پیشرو بودن کشور انگلستان در این زمینه نسبت به سایر کشورهای اروپایی، این کشور انتخاب گردید. قاره‌ی آسیا و آفریقا نیز هنوز در آغاز راه هستند و کشوری که چارچوب ملی پرونده‌ی الکترونیک سلامت طراحی کرده باشد در این دو قاره یافت نشد (۱۲).

پس از انتخاب کشورهای مورد مطالعه، محورهای اصلی مکانیسم ایمنی پرونده الکترونیک سلامت در این کشورها با توجه به اهداف پژوهش مشخص و سپس جداول لازم تهیه گردید. محورهای مکانیسم ایمنی پرونده‌های الکترونیک سلامت ایران نیز از طریق مطالعه‌ی دستورالعمل‌های وزارت بهداشت، درمان و آموزش پزشکی و مطالعات انجام شده در ایران در جداول مورد نظر ثبت شد. سپس داده‌های گردآوری شده با هم مقایسه و نقاط ضعف و قوت هر یک بررسی و مورد تحلیل قرار گرفت.

یافته‌ها

یافته‌ها نشان می‌دهد که هر سه کشور استرالیا، کانادا و انگلستان، الزاماتی برای تشکیل تیم مدیریت ایمنی اطلاعات در سازمان و تعیین واضح مسئولیت‌های ایمنی اطلاعات افراد در سازمان دارند. کشور انگلستان برواگذاری مسئولیت موضوعات ایمنی اطلاعات به هیئت مدیره‌ی سازمان و کشور استرالیا برواگذاری این مسئولیت به تیم مدیریت ایمنی اطلاعات تأکید دارند (۱۴-۱۶) (جدول ۱).

هر سه کشور برای محاسبه‌ی دارایی‌های فن‌آوری اطلاعات سازمان و تعیین مالک وابسته برای آن و نیز آگاهی کاربران از محرمانگی اطلاعات با نصب برچسب بر روی اطلاعات الزاماتی دارند. کشور استرالیا بر طبقه‌بندی اطلاعات به چهار طبقه، کشور کانادا بر طبقه‌بندی تمامی اطلاعات به صورت محرمانه و کشور انگلستان بر طبقه‌بندی اطلاعات به وسیله‌ی خود دارنده اطلاعات تأکید دارند (۱۴-۱۶) (جدول ۲).

جدول ۱: مقایسه‌ی الزامات سازماندهی ایمنی اطلاعات پرونده‌ی الکترونیک سلامت در کشورهای منتخب

ردیف	الزامات سازماندهی ایمنی اطلاعات سلامت	کشورهای مورد مطالعه			
		استرالیا	کانادا	انگلیس	ایران
۱	تشکیل تیم مدیریت ایمنی اطلاعات در سازمان	✓	✓	✓	–
۲	واگذاری مسوولیت موضوعات ایمنی به تیم مدیریت ایمنی	✓	–	–	–
۳	واگذاری مسوولیت موضوعات ایمنی به هیئت مدیره‌ی سازمان متولی مراقبت	–	–	✓	–
۴	تعیین واضح مسوولیت‌های ایمنی اطلاعات توسط تیم مدیریت ایمنی اطلاعات	✓	✓	✓	–
۵	بررسی مستقل و تأیید کتبی اجرای سیاست ایمنی اطلاعات توسط سازمان	✓	✓	–	–
۶	ارزیابی و کنترل دسترسی اشخاص ثالث به امکانات فن‌آوری اطلاعات سازمان	✓	✓	–	–
۷	رعایت شرایط و سیاست‌های ایمنی به هنگام واگذاری امور به پیمانکار مستقل	✓	✓	–	–

جدول ۲: مقایسه‌ی الزامات ایمنی طبقه‌بندی و کنترل امکانات پرونده‌ی الکترونیک سلامت در کشورهای منتخب

ردیف	الزامات ایمنی طبقه‌بندی و کنترل امکانات اطلاعاتی	کشورهای مورد مطالعه			
		استرالیا	کانادا	انگلیس	ایران
۱	محاسبه تمام دارایی‌های فن‌آوری اطلاعات سازمان و تعیین مالک انتسابی برای آنها	✓	✓	✓	–
۲	طبقه‌بندی اطلاعات به چهار طبقه‌ی عمومی، داخلی، محرمانه و سری	✓	–	–	–
۳	طبقه‌بندی تمامی داده‌های سلامت درسازمان‌ها، به صورت محرمانه	–	✓	–	–
۴	انجام طبقه‌بندی اطلاعات توسط دارنده‌ی امکانات اطلاعاتی	–	–	✓	–
۵	آگاهی کاربران در تمامی سازمان‌ها از محرمانه بودن اطلاعات سلامت به وسیله نصب برچسب بر روی اطلاعات	✓	✓	✓	–
۶	ممیزی منظم فهرست موجودی امکانات، طرح برچسب زنی، طبقه‌بندی اطلاعات و رویه‌های جابجایی	–	–	✓	–

سه کشور منتخب در خصوص منابع انسانی، برای گنجاندن وظایف ایمنی در تعاریف شغلی کارکنان ایمنی اطلاعات، لزوم امضای قرارداد حفظ محرمانگی اطلاعات توسط کارکنان، تعیین مسوولیت‌ها و وظایف کارکنان در قبال ایمنی اطلاعات و آموزش رویه‌های ایمنی به تمامی کارکنان و کاربران ثالث اطلاعات سازمان الزاماتی دارند. فقط کشور کانادا الزامی برای خاتمه دادن به دسترسی کاربران به اطلاعات در زمان پایان اشتغال آنها در سازمان، دارد (۱۴–۱۶) (جدول ۳).

هرسه کشور منتخب، در زمینه‌ی الزامات ایمنی مدیریت ارتباطات و عملیات اطلاعات سازمان، الزاماتی برای تفکیک وظایف و مسئولیت‌های کارکنان، وجود رویه‌هایی برای تأیید و طراحی سیستم‌های اطلاعاتی، پشتیبان گیری منظم از داده‌ها، پیروی از رویه‌های عملی استاندارد برای جابجایی رسانه‌ی کامپیوتری و توافق رسمی بین سازمان‌ها برای تبادل اطلاعات الکترونیکی دارند (۱۴–۱۶) (جدول ۴).

هرسه کشور منتخب، در زمینه‌ی الزامات ایمنی کنترل دسترسی به اطلاعات پرونده‌ی الکترونیک سلامت و برای محدود سازی دسترسی و کنترل آن، استفاده از یک رویکرد رسمی برای دسترسی به اطلاعات، ایجاد محدودیت برای به‌کارگیری سیستم، تعریف مسوولیت‌های کاربران و اخذ مجوز برای دسترسی کاربران از راه دور الزاماتی دارند (۱۴–۱۶) (جدول ۵).

جدول ۳: مقایسه‌ی الزامات ایمنی منابع انسانی پرونده‌ی الکترونیک سلامت در کشورهای منتخب

ردیف	الزامات ایمنی منابع انسانی	کشورهای مورد مطالعه			
		استرالیا	کانادا	انگلیس	ایران
۱	گنجاندن نقش‌ها و وظایف ایمنی موجود در سیاست ایمنی سازمان درتعاریف شغلی کارکنان ایمنی اطلاعات سازمان	✓	✓	✓	–
۲	کنترل کارکنان دائمی، موقت و پیمانکاران از نظر ایجادخطر ایمنی در فرایند به کارگیری شغلی	✓	–	✓	–
۳	امضاء قرارداد حفظ محرمانگی اطلاعات توسط کارکنان به عنوان بخشی از شرایط اولیه‌ی استخدام	✓	✓	✓	–
۴	تعیین مسوولیت‌ها و وظایف کارکنان در قبال ایمنی اطلاعات درشرایط استخدام	✓	✓	✓	–
۵	آموزش رویه‌های ایمنی به تمامی کارکنان و کاربران ثالث اطلاعات سازمان	✓	✓	✓	–
۶	واکنش کاربران سازمان به حوادث ایمنی مشاهده شده و گزارش آنها از طریق کانال‌های مدیریتی	✓	–	✓	–
۷	ایجاد فرایند تنبیه‌ی رسمی برای هرگونه تخلف کاربران از سیاست‌های ایمنی اطلاعات سازمان	✓	–	✓	–
۸	پایان دسترسی کاربران به اطلاعات در زمان خاتمه‌ی اشتغال آنها در سازمان	–	✓	–	–

جدول ۴: مقایسه‌ی الزامات ایمنی مدیریت ارتباطات و عملیات پرونده‌ی الکترونیک سلامت در کشورهای منتخب

ردیف	الزامات ایمنی مدیریت ارتباطات و عملیات اطلاعات سلامت	کشورهای مورد مطالعه			
		استرالیا	کانادا	انگلیس	ایران
۱	ثبت ونگهداری رویه‌های عملکردی در عملکرد رایانه‌ها	✓	–	✓	–
۲	تفکیک وظایف و مسئولیت‌های کارکنان تاحد ممکن	✓	✓	✓	–
۳	وجود رویه‌های مناسب برای تأیید و طراحی سیستم‌های اطلاعاتی	✓	✓	✓	–
۴	پشتیبان گیری منظم و ایمن از اطلاعات شغلی و نرم‌افزاری	✓	✓	✓	–
۵	رمزگذاری اطلاعات سلامت در حین انتقال واستفاده از زیر ساخت کلید عمومی	–	✓	–	–
۶	حفظ درستی داده‌های منبع و مقصد در حین انتقال اطلاعات	–	✓	–	–
۷	پیروی از رویه‌های عملی استاندارد در جابجایی و ایمنی رسانه‌ی کامپیوتری	✓	✓	✓	–
۸	وجود توافق رسمی بین سازمان وسایر سازمان‌ها برای تبادل اطلاعات الکترونیکی	✓	✓	✓	–
۹	ذخیره‌ی داده‌های پشتیبان گیری شده در یک محیط به طور فیزیکی ایمن، خارج از جایگاه اصلی	–	✓	–	–
۱۰	ایجاد واقعه نگاری‌های ممیزی ایمن درسیستم‌های الکترونیک سازمان	–	✓	–	–

جدول ۵: مقایسه‌ی الزامات ایمنی کنترل دسترسی به اطلاعات پرونده‌ی الکترونیک سلامت در کشورهای منتخب

ردیف	الزامات ایمنی کنترل دسترسی به اطلاعات سلامت	کشورهای مورد مطالعه			
		استرالیا	کانادا	انگلیس	ایران
۱	تعریف وثبت شرایط کاری کنترل دسترسی ومحدودسازی دسترسی بر اساس سیاست بازرسی	✓	✓	✓	–
۲	استفاده ازیک رویکرد رسمی در ثبت یا عدم ثبت کاربر برای دسترسی به اطلاعات	✓	✓	✓	–
۳	ایجاد محدودیت وکنترل تخصیص و کاربرد سیستم یا مزایای کاربرد سیستم	✓	✓	✓	–
۴	کنترل تخصیص کلمات عبور از طریق یک فرایند مدیریت رسمی	✓	–	✓	–
۵	اعطای دسترسی به کاربران بر اساس نقش آنها در سازمان	–	✓	✓	–
۶	دسترسی هر کاربربه اطلاعات در هر دوره‌ی کاری تنها در یک نقش واحد	–	✓	–	–
۷	امکان لغو به هنگام حق دسترسی کاربر به اطلاعات	–	✓	–	–
۸	تعریف مسئولیت‌های کاربران و پیروی از آنها	✓	✓	✓	–
۹	دسترسی مستقیم کاربران فقط به سرویس‌های مجاز	✓	–	–	–
۱۰	اخذ مجوزجهت دسترسی کاربران از راه دور	✓	✓	✓	–
۱۱	کنترل دسترسی به سیستم‌های عامل	✓	✓	–	–
۱۲	اختصاص مشخصه‌ی شناسایی ویژه به همه‌ی کاربران	✓	✓	–	–
۱۳	کنترل دسترسی به برنامه‌های کاربردی	✓	–	–	–
۱۴	پایش دسترسی به سیستم‌های اطلاعاتی	✓	–	✓	–
۱۵	توسعه‌ی رویه‌ها و سیاست‌ها برای تأیید و کنترل فعالیت‌های ارتباط از راه دور	✓	✓	–	–

بحث

بر اساس یافته‌های پژوهش، الزام تشکیلات ایمنی اطلاعات پرونده‌ی الکترونیک سلامت در هر سه کشور بر تشکیل تیم مدیریت ایمنی اطلاعات سازمان و تعیین واضح مسوولیت‌های ایمنی اطلاعات توسط این تیم تأکید دارد (۱۴-۱۶). Schaectel در مقاله‌ای بیان می‌کند که هر سازمانی باید فعالیت‌هایی تحت عنوان مدیریت ایمنی داشته باشد (۱۷). کمیسیون مشترک اعتبار بخشی آمریکا نیز با توجه به اهمیت و حساسیت اطلاعات الکترونیک در محیط‌های درمانی بر مسوولیت مدیر بخش مدارک پزشکی در حفاظت از این اطلاعات تأکید کرده است (۱۸). کشور ایران در این خصوص الزام خاصی ندارد. با توجه به اهمیت امنیت اطلاعات در سیستم‌های کامپیوتری، به نظر می‌رسد که تعیین مسوول امنیت اطلاعات در مراکز درمانی و تعریف وظایف وی ضرورت دارد و لازم است که این موضوع در تشکیلات سازمانی مراکز درمانی مورد توجه قرار گیرد.

الزامات ایمنی طبقه‌بندی و کنترل امکانات اطلاعاتی در کشورهای مورد مطالعه، حاوی نکاتی در خصوص لزوم آگاهی کاربران در تمامی سازمان‌ها از محرمانه بودن اطلاعات و طبقه‌بندی اطلاعات به نحو مقتضی برای جلوگیری از دسترسی افراد به تمامی اطلاعات است (۱۴-۱۶). بررسی انجام شده در سال ۱۳۸۱ در اصفهان حاکی از آن است که ۹۰/۹ درصد از واحدهای مورد مطالعه اوراق مالی مربوط به درمان بیماران، موجود در پرونده‌ی بیمار را جزء اوراق محرمانه محسوب می‌کنند. همچنین تنها در ۱۸/۲ درصد از واحدهای مورد مطالعه، مکانیسم‌های حفاظتی مناسب برای ایمنی پرونده‌های بیماران خاص از جمله مبتلایان به ایدز، بیماران روانی و سایر بیماری‌های حساس وجود دارد (۹). به نظر می‌رسد به دلیل نبود الزاماتی در خصوص ایمنی طبقه‌بندی و کنترل امکانات اطلاعاتی در کشورمان و فقدان طبقه‌بندی اطلاعاتی مناسب برای اطلاعات بهداشتی درمانی، مراکز درمانی در این زمینه بی‌توجهی کرده و از یک روش استاندارد پیروی نمی‌کنند.

بنابراین در صورت ایجاد پرونده‌ی الکترونیک سلامت، لازم است که اطلاعات بیماران به نحو مقتضی طبقه‌بندی شده و اطلاعات محرمانه از غیر محرمانه با تعیین درجات محرمانگی اطلاعات و مکانیسم‌هایی برای حفاظت از آنها مدنظر قرار گیرد.

کشورهای مورد مطالعه در خصوص ایمنی منابع انسانی الزاماتی دارند که با امضای قرارداد حفظ محرمانگی اطلاعات توسط کارکنان به عنوان بخشی از شرایط اولیه‌ی استخدام و آموزش رویه‌های ایمنی به تمامی کارکنان و کاربران ثالث سازمان تأکید دارد (۱۴-۱۶). نتایج بررسی سال ۲۰۰۳ کانادا حاکی از آن است که کارکنان حدود ۹۰ درصد سازمان‌ها ملزم به امضای توافقنامه محرمانگی اطلاعات هستند (۱۹). Young و Cooke اظهار می‌دارند که مدیریت باید از طریق سرمایه‌گذاری در آموزش نیروی کار به کاهش احتمال خطر در سازمان کمک کند (۲۰). در کشور ایران الزاماتی در خصوص ایمنی منابع انسانی در حوزه‌ی سلامت الکترونیک وجود ندارد و لازم است که این موضوع در طراحی پرونده الکترونیک سلامت مورد توجه قرار گیرد.

یافته‌ها نشان می‌دهد که کشورهای مورد مطالعه الزاماتی در مورد ایمنی مدیریت ارتباطات و عملیات پرونده‌ی الکترونیک سلامت دارند که مشتمل بر پیروی از رویه‌های عملی استاندارد در جابجایی و ایمنی رسانه کامپیوتری، وجود توافقنامه رسمی بین سازمان و سایر مراکز برای تبادل اطلاعات الکترونیکی و ذخیره‌ی داده‌های پشتیبان گیری شده در محیط ایمن، خارج از جایگاه اصلی و حفظ درستی داده‌ها در حین انتقال است (۱۴-۱۶).

Davis & Lacour بیان کرده‌اند که داده‌ها برای سودمند واقع شدن باید صحیح باشد. اگر داده‌ها صحیح نباشد، تصورات و دانش نادرست به کاربران انتقال می‌یابد (۲۱). در کشور ایران به دلیل نبود پرونده‌ی الکترونیک سلامت یک‌پارچه، الزامات خاصی وجود ندارد، اما برخی مراکز درمانی به صورت پراکنده با استفاده از نرم‌افزارهای نامتجانس، نسبت به ایجادسیستم اطلاعات بیمارستانی اقدام نموده ورویه‌هایی برای ایمنی

اطلاعات آن به کار می‌برند، از جمله بررسی انجام شده توسط زاهدی‌فر در سال ۱۳۸۱ نشان می‌دهد که تمامی واحدهای مورد بررسی، دیسک‌های حاوی اطلاعات بیماران را در محل امن نگهداری می‌کنند (۹) که با یافته‌های این پژوهش همخوانی دارد. مطالعه‌ی سال ۲۰۰۴ آمریکا نشان می‌دهد که ۴۳ درصد افراد وجود توافقنامه بین فراهم کنندگان مراقبت برای مبادله اطلاعات درمانی بیمار را لازم دانسته‌اند (۷). صلاحی در پژوهشی وجود سیستم ایمنی برای خروج پرونده‌ها و مطابقت آنرا با استانداردهای امنیت اطلاعات در بیمارستان‌های کشورمان ۶۲/۳ درصد بیان کرده که بیانگر کمبود استانداردها و دستورالعمل‌های آن در این زمینه می‌باشد (۲۲). به نظر می‌رسد بر خلاف فقدان الزامات ایمنی مدیریت ارتباطات و عملیات پرونده‌ی الکترونیک سلامت در کشورمان، مراکز درمانی تا حدودی به این موضوع توجه دارند، بنابراین ضرورت دارد که الزامات جامعی در این خصوص در ایران تدوین و به آن عمل گردد.

بر اساس یافته‌های پژوهش، کشورهای مورد مطالعه در خصوص ایمنی کنترل دسترسی به پرونده‌ی الکترونیک سلامت شامل کنترل تخصیص کلمات عبور به کاربر، اعطای دسترسی به کاربران بر اساس نقش آنها در سازمان، دسترسی کاربران فقط به سرویس‌های مجاز، اخذ مجوز جهت دسترسی کاربران از راه دور و اختصاص مشخصه‌ی شناسایی ویژه به همه‌ی کاربران الزاماتی دارند (۱۴-۱۶). بررسی سال ۲۰۰۳ کانادا نشان می‌دهد که ۸۰ درصد سازمان‌ها، دسترسی کارمندان و پزشکان به پرونده‌های بالینی را فراهم می‌کنند، تمام سازمان‌ها برای کنترل و دسترسی به سیستم‌های بالینی شناسه‌ی کاربری و رمز عبور داشته و ۹۰ درصد سازمان‌ها شناسه‌ی کاربری و رمز عبور واحدی دارند (۱۹). تحقیق سال ۲۰۰۴ آمریکا حاکی از آن است که ۸۸ درصد افراد روش استفاده از رمز عبور را برای دسترسی ایمن به اطلاعات بیمار ترجیح می‌دهند (۷). برخلاف نبود پرونده‌ی الکترونیک سلامت یک‌پارچه در ایران مطالعه‌ی انجام شده در اصفهان در خصوص استفاده برخی مراکز درمانی از سیستم‌های مکانیزه پراکنده نشان می‌دهد که ۸۱/۸ درصد واحدهای مورد مطالعه، ورود اطلاعات به کامپیوتر را توسط افراد مجاز دارای رمز عبور انجام می‌دهند و در تمامی واحدها، کاربران فقط به بخشی از برنامه‌ی کامپیوتری مربوط به حیطه‌ی وظایفشان دسترسی دارند (۹). تمامی یافته‌های یاد شده با یافته‌های این مطالعه مشابهت دارد. طبق پژوهش سال ۲۰۰۳ کانادا، بیش از ۵۰ درصد سازمان‌ها، از سیاست‌های مناسبی برای دستیابی از راه دور به اطلاعات بالینی استفاده می‌کنند، ۲۵ درصد سازمان‌ها شناسه‌های چندگانه بیمار دارند، ۳۳ درصد سازمان‌ها دارای کنترل دسترسی به اطلاعات الکترونیکی می‌باشند که دسترسی متخصصان را به اطلاعات بیمار محدود می‌کند و حدود ۴۰ درصد دسترسی نامحدود برای متخصصان بالینی فراهم کرده‌اند (۱۹). بر اساس پژوهش سال ۲۰۰۴ آمریکا، عمده‌ترین مانع ایجاد پرونده‌ی الکترونیک سلامت، نبود برنامه‌ی دسترسی به اطلاعات بیمار با ۸۷ درصد بوده است و تنها ۵ درصد افراد دسترسی الکترونیکی به پرونده داشته‌اند(۷) که با یافته‌های این پژوهش مغایرت دارد. به نظر می‌رسد که برخلاف نبود الزاماتی در خصوص ایمنی کنترل دسترسی به اطلاعات پرونده‌ی الکترونیک سلامت در کشورمان، برخی مراکز درمانی به این ضرورت پی برده ودر عمل ساختاری در این خصوص به کار گرفته‌اند از این رو لازم است که با ایجاد پرونده‌ی الکترونیک سلامت در تمام مراکز درمانی کشور این موضوع به طور جامع مورد توجه قرار گیرد.

نتیجه‌گیری

ایمنی اطلاعات پرونده‌ی الکترونیک سلامت یکی از ضروریات حرکت به سمت ایجاد و استفاده از پرونده‌ی الکترونیک سلامت در هر کشوری است و کشورمان فاقد الزامات جامعی در این خصوص می‌باشد. با توجه به سیاست وزارت بهداشت، درمان و آموزش پزشکی بر ایجاد و توسعه‌ی پرونده‌ی الکترونیک سلامت برای هر ایرانی،

طراحی و تدوین الزامات ایمنی پرونده‌ی الکترونیک سلامت با استفاده از تجربیات و الگوهای کشورهای پیشرو و موفق در این زمینه برای موفقیت انجام پروژه‌ی مذکور در کشورمان توصیه می‌شود.

منابع

1. Wikipedia.Electronic Health Record.2006.Available at: http://en. wikipedia.org
2. National Electronic Health Records taskforce. A National Approach to electronic health Records for Australia.2000 March. Available at: http://www.healthconnect.gov.au.
3. National Electronic Health Records taskforce. A health information Network for Australia. 2000 July.Available at: http://www.health.gov.au .
4. Lyons R, payne C, Mccabe M, fielder C. legibility of doctor's handwriting: quantitative comparative study. BMJ 1998; 317(7162): 863-4.
5. Woodward B.The computer– based patient record and confidentiality.N Engl J Med 1995;333(21):1419-22.
6. Aspen Reference Group. Health information management manual. Maryland: Aspen publication: 1999.
7. Himss. 2004 Himss National health information infrastructure survey. 2004 July. Available at: http://www.ncvhs.com .

۸. بهنام سیاوش. مطالعه‌ی تطبیقی سطوح دسترسی و محرمانه‌سازی مدارک پزشکی در کشورهای منتخب [پایان نامه]. تهران: دانشکده‌ی مدیریت و اطلاع رسانی پزشکی، دانشگاه علوم پزشکی ایران؛ ۱۳۸۴.

۹. زاهدی فر رفعت. بررسی میزان رعایت حقوق بیمار در بخش مدارک پزشکی بیمارستان‌های وابسته به دانشگاه علوم پزشکی اصفهان [پایان نامه]. تهران: دانشکده‌ی مدیریت و اطلاع رسانی پزشکی، دانشگاه علوم پزشکی ایران؛ ۱۳۸۱.

10. Cornwall A. Electronic health Records: An intentional perspective. 2002.Available at: http://www.home.vicnet.net.an
11. Commonwealth Department of Health and Aged Care. The benefits and difficulties of introducing a national approach to electronic health records in Australia. 2002 April. Available at: http://www.health.gov.au.
12. Commonwealth of Australia. International approaches to the electronic health record. 2003 january. Available at: http://www. healthconnect. gov.au.
13. National committee on vital and Health statistics.Information for health.2001 November. Available from:URA:http://www.ncvhs.com.
14. ABCpty Ltd IT Services. Information Security Controls and procedures manual. 2006. Available at: http://www.maralan.com.au.
15. Canada Health infoway. Electronic Health Record privacy and security Requirements.2005.Available at: http://www.itacontario.com.
16. NHS. IM & T security policy.2004 nov:version 1.1.Available at: http://www. northumberlandcaretrust.nhs.uk

۱۷. حقیقی محمد حسین. بررسی تطبیقی برنامه‌ی مدیریت خطر در مراقبت‌های بهداشتی و ارتباط آن با بخش مدارک پزشکی در کشورهای منتخب و ارائه‌ی الگو [پایان نامه]. تهران: دانشکده‌ی مدیریت و اطلاع رسانی پزشکی، دانشگاه علوم پزشکی ایران؛ ۱۳۸۵.

۱۸. محمدپور علی. مطالعه‌ی تطبیقی استانداردهای بیمارستانی وزارت بهداشت با استانداردهای بین‌المللی اعتباربخشی بیمارستانی کمیسیون مشترک [پایان نامه]. تهران: دانشکده‌ی مدیریت و اطلاع رسانی پزشکی، دانشگاه علوم پزشکی ایران؛ ۱۳۸۵.

19. Canada Health infoway. Infoway pan-Canadian EHR survey phase I Results and Analysis. 2003 January. Available at: http://www.canadahealthinfoway.ca .
20. Young A, Cooke M. Managing & implementing decision in Health Care.London : Bailliere Tidal ; 2002.
21. Davis N, Lacour M.Intraduction to Health Information Technology. USA, Philadelphia : W. B Saunders Company ; 2002.

۲۲. صلاحی مریم. بررسی وضعیت ذخیره و بازیابی پرونده‌های پزشکی بیماران در بیمارستان‌های آموزشی دانشگاه علوم پزشکی ایران و مقایسه‌ی آنها با استانداردهای ملی و آمریکا [پایان نامه]. تهران: دانشکده‌ی مدیریت و اطلاع رسانی پزشکی، دانشگاه علوم پزشکی ایران؛ ۱۳۷۷.

Safety Requirements for Health Electronic File; Comparison between Selected Countries*

Mehrdad Farzandipour, PhD[1]; Farahnaz Sadoughi, PhD[2]; Maryam Ahmadi, PhD[2]; Iraj Karimi PhD[3]

Abstract

Introduction: With increasing production of health information, information technologies have been used for better management and usage of such data. This enormous increase in gathering and storing of information and widespread accessibility also concerns individuals regarding privacy and security of information. This research is concerned with this issue due to decisions on establishing individual health electronic files in Iran.

Methods: During this descriptive-comparative study, security requirements of electronic health files in Iran, England and Canada were reviewed and compared. Checklist was used for data collection. Data was collected from journal papers, and books accessed through libraries and other credible online sources between 1995-2006.

Results: Security requirements regarding health electronic file such as information security systems, safety of communication and operations management, access control were established in those countries except for Iran. There is no safety and security requirements in this regard in Iran.

Conclusion: Security and safety of health electronic file is one of the basic requirements, which lacks in Iran. Due to recent interests in establishing health electronic file in Iran by Ministry of Health and Medical Education, it is necessary that such requirements been established by responsible bodies.

Keywords: Confidentiality; Electronics, Medical; Electronics; Medical Records; Medical Records System, Computerized.

Type of article: Original Article

Citation: Farzandipour M, Sadoughi F, Ahmadi M, Karimi I. Safety requirements for health electronic file; comparison between selected countries. Health Information Management 2007; 4(1):1-9.

*This paper derived from a doctoral thesis.

1. Assistant Professor, Health Service Management, Kashan University of Medical sciences, Kashan, Iran. (Corresponding Author) E-mail: farzandipour_m@kaums.ac.ir
2. Assistant Professor, Health Information Management, Iran University of Medical Science, Tehran, Iran.
3. Assistant Professor, Health Economic, Iran University of Medical Science, Tehran, Iran.