

جوانب قانونی و ملاحظات اخلاقی در رجیستری بیماری: مرور دامنه‌ای

لیلا شاهمرادی^۱، رویا نعیمی^۲

مقاله مروری

چکیده

با جمع‌آوری داده‌های دقیق در فرایند رجیستری، دولت‌ها قادر به پیشگیری از بروز بیماری‌های خطرناک می‌باشند. از طرف دیگر، نگرانی در زمینه افشای اطلاعات افزایش یافته است. پژوهش حاضر با هدف بررسی جوانب قانونی و اخلاقی رجیستری بیماری در قالب عناصر اساسی حفاظت از محرمانگی رجیستری بیماری، ارزیابی تأثیرات حریم خصوصی، اقدامات حفظ محرمانگی داده‌ها، مالکیت داده‌ها و رضایت شرکت‌کنندگان انجام شد. مطالعه از نوع مروری دامنه‌ای بود و داده‌ها از طریق جستجو در پایگاه‌های اطلاعاتی PubMed، Scopus، Web of Science و Google Scholar بدون محدودیت زمانی جمع‌آوری شد. برآیند مطالعات انجام گرفته حاکی از آن است که اطمینان مردم از محرمانگی اطلاعات، ارایه اطلاعات به رجیستری را به همراه دارد و تحلیل اطلاعات حاصل از آن، موجب حفاظت از سلامتی مردم خواهد شد. بنابراین، تدوین الزاماتی در خصوص نحوه استفاده، تجزیه و تحلیل، به اشتراک‌گذاری و حفاظت از داده‌های رجیستری ضرورت دارد.

واژه‌های کلیدی: جوانب قانونی؛ اصول اخلاقی؛ رجیستری؛ بیماری

پیام کلیدی: رجیستری بیماری حاوی مقادیر زیادی اطلاعات شخصی است و باید یک سیاست مدیریتی برای حفظ اعتماد بین رجیستری و شرکت‌کنندگان وجود داشته باشد. تدوین الزاماتی در خصوص نحوه استفاده، تجزیه و تحلیل، به اشتراک‌گذاری و حفاظت از داده‌های رجیستری، منجر به جلب اعتماد و مشارکت افراد در تحقیقات پزشکی خواهد شد و ارتقای ایمنی و بهبود کیفیت مراقبت در سطح فرد و جامعه را به همراه خواهد داشت.

تاریخ انتشار: ۱۳۹۸/۳/۱۵

پذیرش مقاله: ۱۳۹۸/۳/۱۲

دریافت مقاله: ۱۳۹۷/۱۰/۲۲

ارجاع: شاهمرادی لیلا، نعیمی رویا. جوانب قانونی و ملاحظات اخلاقی در رجیستری بیماری: مرور دامنه‌ای. مدیریت اطلاعات سلامت ۱۳۹۸؛ ۱۶ (۲): ۹۳-۸۷

مقدمه

اطلاعات بهداشتی هستند (۲). الزامات اخلاقی حریم خصوصی، نحوه ایجاد و نگهداری رجیستری، به اشتراک‌گذاری داده‌ها و انتشار گزارش‌ها را در برمی‌گیرد (۵). بنابراین، تدوین الزاماتی در خصوص نحوه استفاده، تجزیه و تحلیل، به اشتراک‌گذاری و حفاظت از داده‌های رجیستری ضرورت دارد (۶). با توجه به این که مطالعات کمی در این زمینه انجام شده است، هدف از انجام پژوهش حاضر، بررسی جوانب قانونی و ملاحظات اخلاقی رجیستری بیماری در قالب عناصر اساسی حفاظت از محرمانگی در رجیستری بیماری، ارزیابی تأثیرات حریم خصوصی (PIA) (Impact Assessment Privacy)، اقدامات لازم برای حفظ محرمانگی داده‌ها، مالکیت داده‌ها و رضایت شرکت‌کنندگان بود.

دولت‌ها مدت‌هاست که از شهروندان خود در برابر بحران‌های بهداشتی محافظت می‌کنند و مداخله در برابر بیماری‌های خاص به یکی از ویژگی‌های اصلی بهداشت عمومی در کشورهای توسعه یافته تبدیل شده است (۱). در حال حاضر، سیستم‌های رجیستری بالینی با جمع‌آوری داده‌های دقیق و باکیفیت، دولت‌ها را قادر به نظارت، ردیابی و پیشگیری از بروز بیماری‌های خطرناک می‌سازد و موجب ارتقای ایمنی، اثربخشی و مداخلات خاص به ذی‌نفعان می‌گردد (۲، ۱). رجیستری، یک پایگاه اطلاعاتی ساختارمند حاوی اطلاعات کلینیکی و جمعیت‌شناسی در مورد یک گروه خاص از بیماران با شرایط ویژه می‌باشد (۳، ۴). اولین ثبت بیماری مربوط به سرطان بود و به تدریج در رابطه با سایر بیماری‌ها و شرایط مورد استفاده قرار گرفت (۳). رجیستری بیماری مخزن اطلاعات بالینی است و با ارایه اطلاعات دقیق، معتبر، جامع و به‌موقع، نقش مهمی را در تحقیقات علمی، نظارت بر گروه‌های در معرض خطر، برنامه‌ریزی و تأمین خدمات سلامت، سیاست‌گذاری، ارزیابی بهداشت عمومی و بهبود کیفیت فرایندها ایفا می‌نماید (۵). از طرف دیگر، با نظارت دولت بر سلامت عمومی، نگرانی مردم در رابطه با حریم خصوصی افزایش یافته است (۱). از جمله این نگرانی‌ها می‌توان به دسترسی نامناسب به داده‌ها و سوء استفاده از اطلاعات بهداشتی اشاره کرد که پتانسیل آسیب‌های اقتصادی، اجتماعی یا روانی به افراد یا اشخاص ثالث را دارد. با پیشرفت سریع فن‌آوری اطلاعات طی دو دهه اخیر، این نگرانی‌ها بیشتر شده است و مردم خواهان توجه بیشتر به محرمانگی

مقاله حاصل تحقیق مستقل بدون حمایت مالی و سازمانی است.

۱- دانشیار، مدیریت اطلاعات سلامت، گروه مدیریت اطلاعات سلامت، دانشکده پیراپزشکی، دانشگاه علوم پزشکی تهران، تهران، ایران

۲- دانشجوی دکتری تخصصی، مدیریت اطلاعات سلامت، گروه مدیریت اطلاعات سلامت، دانشکده پیراپزشکی، دانشگاه علوم پزشکی تهران، تهران و گروه مدیریت اطلاعات سلامت، دانشکده پیراپزشکی، دانشگاه علوم پزشکی اردبیل، اردبیل، ایران (نویسنده طرف مکاتبه)

Email: naemiroya@gmail.com

۱۰ عنصر اساسی جهت حفظ محرمانگی رجیستری معرفی نموده که توسط سازمان توسعه و همکاری اقتصادی کانادا به تصویب رسیده است (۹). توضیحات مربوط به عناصر به اختصار در جدول ۱ ارائه شده است.

PIA یکی از جوانب قانونی و ملاحظات محرمانگی در رجیستری بیماری می‌باشد. PIA ابزاری جهت ارزیابی، تعیین درجه انطباق با قانون و شناسایی آینده‌نگر خطرات مربوط به حریم خصوصی است که از طریق توصیف نحوه جمع‌آوری، پردازش و انتشار اطلاعات قبل از به کارگیری یا اصلاح سیستم انجام می‌شود تا با مشاوره ذی‌نفعان، راهکارهایی جهت جلوگیری یا کاهش این خطرات ارائه شود (۸). در ارزیابی PIA عواملی مانند اندازه سازمان، میزان حساسیت اطلاعات شخصی، نوع خطر و نفوذ تکنولوژی تأثیرگذار است (۷). به کارگیری PIA در سازمان‌های بهداشتی- درمانی می‌تواند در شناسایی خطرات بالقوه و حفاظت از حقوق کاربران مؤثر باشد. در PIA عواملی همچون «مجموعه اطلاعات شخصی، رضایت، استفاده از اطلاعات شخصی، افشای اطلاعات، دقت و صحت اطلاعات، حفظ اطلاعات، شفافیت، دسترسی به اطلاعات، به چالش کشیدن خواسته‌ها و نحوه استفاده ثانویه از اطلاعات بهداشتی» بررسی می‌گردد (۸).

جوانب و اقدامات لازم جهت حفظ محرمانگی داده و اطلاعات:

برای حفظ محرمانگی اطلاعات در رجیستری، اقدامات امنیتی باید در سندی حاوی جزئیات خطرات، خط‌مشی‌ها و روش‌های مقابله با خطرات تهیه شود و در اختیار کارکنان قرار گیرد. حفاظت‌ها باید به صورت مداوم باشد و در صورت نیاز تجدید نظرهایی در خط‌مشی‌ها صورت گیرد (۸).

جوانب و اقدامات لازم جهت حفظ محرمانگی داده و اطلاعات به اختصار در جدول ۲ ارائه شده است.

مالکیت داده: مالکیت رجیستری مسأله پیچیده‌ای است. حامی مالی رجیستری در اغلب موارد مالک اطلاعات رجیستری می‌باشد. با این حال، یک رجیستری ممکن است سهامداران و حامیان متعددی داشته باشد. به دلیل این پیچیدگی‌ها، انعقاد قرارداد همکاری و حق مالکیت داده رجیستری مهم است (۶).

روش بررسی

این تحقیق به صورت یک مرور دامنه‌ای انجام شد. داده‌ها از طریق جستجو در پایگاه‌های اطلاعاتی PubMed، Scopus، Web of Science و Google Scholar بدون محدودیت زمانی و فقط به زبان انگلیسی جمع‌آوری گردید. کلمات کلیدی مورد استفاده شامل «Ethical and Legal Issues، Patient Registry، Ethical Principle، Legal Requirements، Disease Registry» بود، اما محدود به این‌ها نشد. در مطالعه حاضر، متون خارجی در زمینه جوانب قانونی و ملاحظات اخلاقی در رجیستری بیماری مورد بررسی قرار گرفت. با توجه به تعداد پژوهش‌های اندک در این زمینه، ۳۵ مقاله استخراج گردید و پس از دسته‌بندی و یکپارچه کردن مطالعات در راستای هدف تحقیق، از ۱۷ مقاله و کتاب استفاده گردید.

یافته‌ها

برای انجام پروژه پزشکی، تصویب کمیته اخلاق مورد نیاز است. از جمله وظایف کمیته اخلاق می‌توان به نظارت بر قوانین و مقررات، هماهنگ نمودن فعالیت‌های کمیته اخلاق منطقه‌ای با کمیته اخلاق مرکزی، تجدید نظر در مورد تحقیقات رد شده و مشارکت در همکاری‌های بین‌المللی اشاره نمود (۶). کمیته‌های اخلاق باید تحقیق با کیفیت بالا را تأیید نمایند و معیارهای ارزیابی با نوع مطالعه مناسب باشد. به عنوان مثال، در دستورالعمل اروپا اخذ رضایت آگاهانه برای ثبت سرطان ضرورت ندارد (۷). عدم رعایت الزامات اخلاقی، رجیستری بیماری را غیر قابل استفاده می‌کند (۸). در ادامه، یافته‌های مرتبط با مطالعه در قالب عناصر اساسی «حفاظت از محرمانگی در رجیستری بیماری، PIA، اقدامات لازم برای حفظ محرمانگی داده، مالکیت داده و رضایت شرکت‌کنندگان» ارائه گردید.

عناصر اساسی حفاظت از محرمانگی در رجیستری بیماری: الگوی

کد انجمن استاندارد کانادا (Canadian Standards Association Model Code).

جدول ۱: عناصر اساسی حفاظت از محرمانگی در رجیستری بیماری

اصول	توضیحات
پاسخگویی (Accountability)	باید فردی به عنوان مسؤول حفاظت از اطلاعات تعیین گردد.
شناسایی اهداف (Identifying Purposes)	اهداف پژوهش باید تعیین گردد.
رضایت (Consent)	جمع‌آوری اطلاعات با رضایت افراد انجام شود.
محدود نمودن مجموعه داده (Limiting Collection)	رجیستری ملزم به جمع‌آوری حداقل مقدار داده برای رسیدن به هدف می‌باشد و نباید اطلاعات اضافی جمع‌آوری گردد.
محدود نمودن استفاده، افشا و نگهداری (Limiting Use, Disclosure and Retention)	استفاده، افشا و حفظ اطلاعات شخصی باید تا زمان تحقق هدف باشد و جهت حفظ اعتماد بین رجیستری و محقق، سیاست مدیریتی ضرورت دارد.
صحت (Accuracy)	باید اطلاعات به صورت صحیح جمع‌آوری و به‌روزرسانی شود.
حفاظت (Safeguards)	انتقال اطلاعات باید مطابق با استانداردهای امنیتی باشد و ذخیره‌سازی اطلاعات باید محدودیت زمانی داشته باشد.
سیاست‌های آشکار و در دسترس (Openness)	باید سیاست‌ها به راحتی در دسترس باشد (با ایجاد یک وب‌سایت).
دسترسی فردی (Individual Access)	ممکن است داوطلبان مجاز به مشورت در خصوص اطلاعات ذخیره شده باشند.
مقابله با چالش‌ها و شکایات (Challenging Compliance)	مسئولان باید بتوانند به هر گونه شکایات مربوط به افشای اطلاعات و... پاسخ دهند.

جدول ۲: اقدامات لازم جهت حفظ محرمانگی داده و اطلاعات در رجیستری بیماری

مورد	توضیحات
مسئولیت	مدیر رجیستری مسئول حفظ محرمانگی اطلاعات است و باید اطمینان دهد که کارمندان رجیستری از مسؤلیت‌های فردی و اقدامات امنیتی در قبال محرمانه بودن آگاه هستند. لیستی به‌روز از کارکنان و اشخاص ثالث و نوع داده‌هایی که به آن دسترسی دارند، نگهداری شود (۱۰).
محکومیت نقض محرمانگی	کارکنان رجیستری باید مطابق با مقررات استخدام شوند و اظهارنامه محرمانگی اطلاعات را امضا کنند و در پرونده‌شان نگهداری شود. نقض محرمانگی منجر به اقدام انضباطی و اخراج است (۱۰).
نمایش یادآورهای دسترسی فیزیکی به رجیستری	توصیه می‌گردد یادداشت‌های یادآوری حفظ محرمانه بودن اطلاعات در واحد رجیستری نصب گردد (۱۰). محل نگهداری سیستم رجیستری باید توسط ضوابط فنی مناسب (فصل‌های مناسب و سیستم‌های هشدار) محدود شود (۱۰).
انتقال اطلاعات	خدمات پستی و پیگ مجوز انتقال داده‌های قابل شناسایی از رجیستری باید توسط مدیر اعطا شود. اطلاعات شناسه باید به طور جداگانه از اطلاعات بهداشتی ارسال شود تا پس از دریافت هر دو بسته، توسط کارکنان مجاز ترکیب شود. از پاکت‌های دوگانه (پاکت خارجی با آدرس کلی و پاکت داخلی برای باز کردن تنها توسط فرد مورد نظر) استفاده گردد (۱۰).
انتقال داده‌های الکترونیکی	الف: از صحت آدرس گیرنده از طریق مختلف (تماس قبل از ارسال داده یا کلید شناسایی) اطمینان حاصل شود. ب: اطلاعات در سطوح مختلف پیچیدگی توسط کاربران مجاز رمزگذاری شود. ج: هنگام ارسال فایل داده، داده‌های قابل شناسایی باید جدا از سایر داده‌ها ارسال شود. د: تأیید دریافت ایمن داده‌ها توسط دریافت‌کننده درخواست گردد (۱۰).
پرداش داده‌ها توسط سازمان‌های خارجی	برای به اشتراک‌گذاری داده‌ها باید توافقنامه‌ای منعقد گردد و حفاظت مضاعفی از اطلاعات صورت گیرد (۸). اگر اطلاعات رجیستری در خارج از واحد رجیستری یا در کشور دیگر پردازش شود، باید از محرمانگی اطلاعات توسط سازمان دریافت‌کننده اطلاعات اطمینان حاصل شود. از انتقال غیر ضروری داده‌های قابل شناسایی به خارج از رجیستری اجتناب شود (۱۰). در مطالعاتی که اطلاعات چندین رجیستری ادغام می‌گردد، رضایت افراد نیاز نیست. جهت حفظ محرمانگی اطلاعات در زمان به اشتراک‌گذاری داده، پاسخ محقق به پرسش‌هایی ضرورت دارد. به عنوان مثال، هدف از پیوند داده‌ها چیست؟ چه داده‌هایی جمع‌آوری خواهد شد؟ آیا داده‌ها حاوی شناسه‌های مستقیم یا غیر مستقیم هستند؟ آیا یک مجموعه داده محدود LDS (Limited Data Set) و توافق استفاده از داده (Data Use Agreement) DUA موجود است؟ آیا سیاست به اشتراک‌گذاری داده وجود دارد؟ و حداقل اقدام قابل قبول برای جلوگیری از شناسایی افراد چیست؟ (۱۱)
استفاده از تلفن و فاکس	کارکنان رجیستری نباید اطلاعات محرمانه را از طریق تلفن یا فاکس ارایه دهند. شماره فاکس قبل از انتقال اطلاعات باید با دقت بررسی شود. در موارد نادر که به کارگیری تلفن توسط مدیر قابل توجه است، هویت تماس گیرنده (نام، موقعیت، عنوان و آدرس) باید بررسی شود و با استفاده از شماره تلفن رسمی فراهخوانی شود (۱۰).
استفاده از رایانه	باید اقدامات فیزیکی و فنی جدید و مؤثر برای جلوگیری از دسترسی غیر مجاز به اطلاعات انجام گیرد. اقدامات الکترونیکی به سرعت در حال تکامل است و راه‌حل‌های بهتر ممکن است از آنچه در اینجا مورد بحث است، فراتر باشد (۱۰).
دسترسی به داده‌ها	الف: دسترسی به داده باید در یک اتاق جداگانه و محدود باشد. ب: کلمات عبور باید پیچیده باشند و هنگام تایپ نباید روی صفحه نمایش داده شود. ذخیره‌سازی خودکار کلمه عبور و نام کاربری باید غیر فعال شود و کلمات عبور در فواصل منظم تغییر یابد. ج: سطوح مختلف دسترسی به پایگاه داده باید تعریف شود و فقط کاربران مجاز بتوانند به داده‌های قابل شناسایی دسترسی داشته باشند. د: اگر سیستم بیش از ۱۰ دقیقه غیر فعال باشد، باید به طور خودکار بسته شود. رایانه‌های رجیستری باید با Firewall محافظت شوند. و: تست سخت‌افزار و نرم‌افزار جدید باید با داده‌های مختص تست (و نه داده واقعی) انجام شود. ز: در هنگام خارج نمودن رسانه‌های ذخیره‌سازی الکترونیکی به دلیل خرابی و...، باید اطلاعات پاک و نابود شود (۱۰).
نمایش پشتیبان‌گیری	هنگام نمایش پایگاه داده، داده‌های ساختگی یا ناشناس باید مورد استفاده قرار گیرد (۱۰). از پایگاه داده و تغییرات آن باید به طور مداوم و مرتب نسخه پشتیبان گرفته شود و در یک مکان فیزیکی جداگانه و ایمن از آب و آتش نگهداری شود (۱۰).
دسترسی غیر مجاز به سیستم کامپیوتری	تلاش برخی افراد جهت دسترسی از راه دور به سیستم کامپیوتری تشخیص داده شود و به مدیر و افراد مجاز گزارش گردد و از بین برود. باید مشاوره تخصصی و منظم در مورد افزایش امنیت سیستم کامپیوتری صورت گیرد (۱۰).

جدول ۲: اقدامات لازم جهت حفظ محرمانگی داده و اطلاعات در رجیستری بیماری (ادامه)

موارد	توضیحات
ذخیره و دفع داده	<p>محققان باید نحوه جمع آوری داده، افراد مجاز به دسترسی داده، مدت نگهداری داده، ذخیره با شناسه منحصر به فرد (PIN (Personal Identification Number) یا بدون آن، روش اضافی جهت جمع آوری داده، منابع داده (به عنوان مثال رجیستری علت مرگ) و نحوه ذخیره سازی داده را توصیف کنند. محققان و دیگر کاربران داده باید به طور واضح از نحوه جمع آوری، استفاده از اطلاعات و تعهدات قانونی برای اطمینان از این که اطلاعات به طور مناسب و ایمن مورد استفاده قرار می گیرد، مطلع باشند (۶). داده ثبت آنلاین باید به درستی و با شیوه مناسبی رمزنگاری و ذخیره شود. هنگام طراحی رجیستری آنلاین، اطمینان از امنیت مناسب فن آوری اطلاعات و مشاوره های شبکه ضرورت دارد (۱۲).</p> <p>داده های کاغذی باید در فایل قرار گیرند یا اسکن مدارک در رسانه های الکترونیکی ذخیره و محافظت شود. اقدامات «سوابق کاغذی» شامل الف: تعیین افرادی که به محل رجیستری دسترسی دارد. ب: تعیین کسانی که به اتاق نگهداری اطلاعات دسترسی دارند. ج: کابینت قابل قفل جهت ذخیره اطلاعات محرمانه وجود داشته باشد. د: اطمینان از این که افرادی که مجاز نیستند (به طور مثال کارکنان خدمات) نمی توانند پرونده های حاوی اطلاعات محرمانه را بررسی کنند. سیاست مناسب دفع مدارک کاغذی حاوی اطلاعات قابل شناسایی، باید تدوین شود. تخریب کاغذ شامل انهدام است. این اقدام باید در محل رجیستری صورت گیرد (۱۰).</p>
بازنگری روش های امنیتی و محرمانگی	<p>توصیه می شود که سالانه رجیستری ها روش های امنیتی خود را بررسی و دستورالعمل دسترسی را به روز نمایند (۱۰).</p>
انتشار اطلاعات	<p>داده باید برای پاسخ به سؤال مورد نیاز ارایه شود. در برنامه اخلاقی، اطلاعاتی در مورد نحوه انتشار اطلاعات تحقیق (به طور مثال ارایه در جلسات و نسخه علمی) و حمایت سازمانی (به عنوان مثال از طریق صنعت دارو) و تأثیرش بر استراتژی تحقیق درخواست گردد. انتشار داده باید بی نام بودن بیماران را تضمین کند و داده باید به شکلی جمع آوری و ارایه شود تا امکان شناسایی فرد با اطلاعاتی مانند تاریخ تولد، جنسیت و محل اقامت نباشد (۱۳).</p>
مسئولیت انتشار اطلاعات	<p>توصیه می شود قرارداد انتقال داده منعقد شود و شرایط استفاده و انتشار داده در آن شرح داده شود و پیروی از قوانین انتشار داده ها توسط مدیر تضمین گردد (۱۰).</p>
محدودیت انتشار داده	<p>الف: قوانین محرمانگی اطلاعات (حقوق بیمار) باید مورد توجه قرار گیرد. ب: رجیستری در صورت عدم وجود رضایت کتبی از همه طرفین، نباید داده قابل شناسایی را ارایه دهد. ج: داده های منتشر شده باید به هدف پژوهش محدود باشد (۱۰).</p>
انتشار داده قابل شناسایی برای اهداف بالینی	<p>جهت دسترسی به داده های قابل شناسایی در زمینه درمان بیمار باید به پزشک متخصص مراجعه شود تا مطابق قانون انتشار اطلاعات بالینی در کشور اقدام شود (۱۰). استفاده از اطلاعات قابل شناسایی بیمار به ویژه در زمینه رجیستری، طالب الزامات قانونی است. توصیه می شود که با مراجع ملی حفاظت از داده ها جهت اطمینان از رعایت استانداردهای درخواست شده رایزنی شود (۱۴).</p>
انتشار داده قابل شناسایی برای کنترل سرطان	<p>باید رویه های انتشار داده در یک سند قابل شناسایی ارایه شود. درخواست کتبی دریافت داده های محرمانه به مقامات نظارتی ارایه شود. درخواست باید شامل مواردی مانند «هدف از درخواست داده، توجیه نیاز به اطلاعات محرمانه، نام و موقعیت شخص مسئول انتشار اطلاعات، نام و موقعیت افرادی که به داده های منتشر شده دسترسی خواهند داشت، مدت زمانی که داده مورد استفاده قرار می گیرد و شیوه ای که داده پس از گذشت این دوره از بین می رود، بازگردانده و یا نابود می شود» باشد (۱۰).</p>

داده بیولوژیکی، لازم است. باید نحوه حضور شرکت کنندگان در پژوهش (از طریق معرفی پزشک، رجیستری ملی و...)، اطلاعات مربوط به زمان و نحوه اخذ رضایت آگاهانه و اطلاعات افراد مسوول ثبت شرح داده شود. این افراد باید از نحوه دسترسی، به اشتراک گذاری و مدت زمان ذخیره اطلاعات و نحوه خروج از مطالعه آگاهی داشته باشند. رضایت به مدت طولانی قابل استفاده نیست. رضایت باید به صورت آزادانه، بدون فشار و یا متقاعد کردن و بر اساس اطلاعات ارایه شده توسط افراد مجرب باشد. کمیته بازرسی اخلاقی باید فرایند اخذ رضایت را ارزیابی نماید تا از برتری مزایای تحقیق نسبت به مضرات آن اطمینان حاصل گردد. در صورتی که جمع آوری داده توسط یک کشور دیگر صورت گیرد، باید به مقررات کشور مبدأ داده و کشوری که در آن داده ها ذخیره می شود، احترام

موافقت نامه های مربوط به مالکیت داده و دسترسی به داده باید توسط چندین قرارداد تعیین گردد و حاوی اصولی باشد؛ از جمله این که همیشه سازمان باید به عنوان کنترل کننده اصلی داده باشد. هنگامی که اطلاعات پردازش می شود، به عنوان داده تحقیق تلقی می شود، مگر این که مالکیت خصوصی مورد توافق قرار گیرد. پردازنده و یا محقق اصلی داده باید به عنوان محافظ داده باشد. این شخص باید اقدامات لازم را برای حفاظت در ذخیره، استفاده و دسترسی به داده انجام دهد. از این رو، محقق با توجه به سود به اشتراک گذاری اطلاعات، دارای مالکیت معنوی نهایی می باشد (۶).

رضایت شرکت کنندگان در مطالعه: اخذ رضایت آگاهانه در مطالعاتی که محقق با شرکت کنندگان تعامل دارد (به طور مثال پرسش نامه های فردی و یا

گذاشته شود و حداکثر حمایت از حقوق بیماران به عمل آید (۱۴، ۶).

در مورد داده‌های موجود در سیستم، محققان باید مجدد با افراد تماس بگیرند تا رضایت مطالعه جدید را به دست آورند. اگر کسب رضایت غیر ممکن باشد، یک هیأت بررسی اخلاقی باید رضایت خود را برای استفاده از داده‌ها ارایه دهد (۱۴). چنانچه تحقیقی توسط کمیته اخلاق تأیید گردد، فرض می‌شود که شرکت‌کنندگان با تحقیق مبتنی بر رجیستری موافق هستند و توافق‌نامه به اشتراک‌گذاری اطلاعات در قرارداد غیر رسمی بین محقق و دولت منعقد می‌شود (۱۳). در تحقیق مبتنی بر رجیستری، به ندرت رضایت آگاهانه از شرکت‌کنندگان درخواست می‌گردد؛ چرا که منجر به سوگیری در تحقیقات با مقیاس گسترده می‌گردد. استدلال‌های عدم نیاز به رضایت آگاهانه در مطالعات مبتنی بر رجیستری شامل «تعداد زیادی شرکت‌کننده در این پژوهش‌ها (گاهی اوقات بیش از ۱ میلیون نفر) وجود دارد، درخواست رضایت فردی موجب کاهش میزان مشارکت افراد می‌شود که تهدیدی بر اعتبار علمی مطالعه است، کسب رضایت به ویژه در انتخاب گروه‌های پرخطر (با پیامد مثبت) مانند کودکان بسیار دشوار است، رجیستری ممکن است شامل افرادی باشد که در قید حیات نیستند و نمی‌توان رضایتشان را به دست آورد، هزینه به دست آوردن رضایت میلیون‌ها نفر بیش از حد خواهد بود و از تحقیقات در مقیاس بزرگ جلوگیری خواهد کرد» می‌باشد. در کشورهای شمال اروپا، کمیته اخلاق موافقت شرکت‌کنندگان در تحقیق را با تصویب کمیته اخلاق جایگزین می‌کند (۱۳).

نگرانی‌های جدی اخلاقی و حقوقی، منجر به تدوین الزامات قانونی و اخلاقی شده است که همیشه هم یکسان نیست. این الزامات قانونی ممکن است بر انتخاب عناصر داده‌ای، سازماندهی اطلاعات، استفاده بعدی از داده‌ها، قابلیت همکاری رجیستری‌ها و نیز انتشار اطلاعات تأثیر بگذارد (۱۴، ۸). Myers و همکاران در مطالعه خود اذعان داشتند که سازمان‌های بهداشت عمومی، تعادل بین منافع بهداشت عمومی با حقوق و امتیازات افراد را به چالش کشیده‌اند. سازمان‌های بهداشت عمومی باید همه تهدیدات احتمالی را ارزیابی کنند و از سیاست‌ها، آموزش و مهندسی پیشگیرانه مناسبی استفاده نمایند. اگرچه تضمین حفظ حریم خصوصی کامل اطلاعات بهداشتی و شخصی غیر ممکن است، اما سازمان‌های بهداشت عمومی باید با ارتقای مهارت‌های کارکنان در کسب، استفاده، نگهداری، ذخیره و به اشتراک‌گذاری اطلاعات، خطرات را به حداقل برسانند (۱۶) که با نتایج پژوهش Kralj و Zaletel (۸) همسو بود.

اطمینان مردم از امنیت اطلاعات، ارتباط مستقیمی با ارایه اطلاعات شخصی بهداشتی افراد به رجیستری دارد. سازمان‌های بهداشت عمومی باید امنیت داده‌ها را فعالانه تأمین کنند. ترویج و محافظت از سلامتی مردم به اطلاعاتی که از آن‌ها دریافت می‌کنند، بستگی دارد (۱۶). دسترسی به اطلاعات رجیستری بدون نقض محرمانگی، به تفکر و برنامه‌ریزی نیازمند است (۱۴). عدم رعایت الزامات اخلاقی و قانونی مربوط به حریم خصوصی، رجیستری بیمار را غیر قابل استفاده می‌کند (۸). ساختار، عملیات و فرایندهای رجیستری متفاوت است. با این حال، اصول اخلاقی و قانونی مشترکی در ایجاد و استفاده از رجیستری‌ها وجود دارد، اما در برخی از رجیستری‌ها با توجه به هدف، وضعیت توسعه دهنده آن، ماهیت داده‌ها و میزان اطلاعات موجود در آن، الزامات قانونی اختصاصی‌تر می‌گردد (۶، ۵). از این‌رو، هر رجیستری باید با توجه به گزینه‌های فنی در دسترس، الزامات قانونی خاصی را جهت جمع‌آوری، نگهداری، پردازش و گزارش اطلاعات مراقبت‌های بهداشتی تدوین نماید تا خطرات احتمالی را کاهش دهد (۱۶، ۵). Hopper و همکاران عقیده دارند که قانون حفاظت از داده‌ها مانعی برای جمع‌آوری داده‌ها نیست، بلکه چارچوب ایمنی جهت حفظ محرمانگی و حریم شخصی افراد و تسهیل جمع‌آوری و به اشتراک‌گذاری داده‌ها می‌باشد (۵) که این یافته با نتایج تحقیق حاضر همخوانی داشت. بر اساس نتایج به دست آمده از بررسی حاضر، حفاظت مناسب اطلاعات منجر به جلب اعتماد و مشارکت بیشتر افراد در تحقیقات پزشکی خواهد شد و ارتقای ایمنی و بهبود کیفیت مراقبت در سطح فرد و جامعه را به همراه خواهد داشت (۱۶، ۸). ترویج و محافظت از سلامت مردم به اطلاعاتی که از آن‌ها دریافت می‌شود، بستگی دارد

بحث

تدوین و اجرای ملاحظات اخلاقی و الزامات قانونی کارآمد، انعطاف‌پذیر و به‌موقع، به موفقیت رجیستری کمک می‌کند (۱۴). بر طبق نظرات Richesson و Vehik، سیستم‌های رجیستری فرایندی اساسی برای تحقیق هستند (۱۵) و بررسی الزامات قانونی سیستم رجیستری نشان می‌دهد که این سیستم‌ها باید با استانداردهای بالای امنیت مطابقت داشته باشند و به طور منظم به‌روزرسانی شوند تا از صحت اطلاعات جمع‌آوری شده اطمینان حاصل گردد. بنابراین، ضمانت‌های امنیتی باید اطلاعات را از دسترسی غیر مجاز محافظت نماید و اطلاعات حساس با حمایت‌های امنیتی مناسب همراه باشد. استفاده، افشا و حفظ اطلاعات شخصی تا زمان لازم برای تحقق هدف توصیه می‌گردد. دوره زمانی کوتاه، احتمال افشای اطلاعات را کاهش می‌دهد. اگرچه نیاز به اطمینان از وجود رجیستری بلندمدت وجود دارد. زمانی که اهداف رجیستری دنبال نمی‌شود، نباید اطلاعات شخصی حفظ گردد. هنگامی که رجیستری برای تحقق اهداف مفید نیست یا فاقد بوجه است و یا هیچ کس نمی‌تواند به درستی با رجیستری کار کند، اطلاعات باید نابود شود. سیاست رجیستری باید به راحتی قابل دسترسی باشد و فردی به عنوان مسؤوّل حفاظت از اطلاعات تعیین گردد تا بتواند به هرگونه شکایات پاسخ دهد (۹).

آژانس بین‌المللی تحقیقات سرطان IARC (International Agency for Research on Cancer) اظهار می‌دارد که رعایت محرمانگی با سوگند پزشکان برابری می‌کند. به عبارت دیگر، تکمیل اظهارنامه رعایت محرمانگی کارکنان رجیستری به هنگام استفاده ضرورت دارد. کارکنان متخصص ثبت باید مطابق با اهداف و مقررات عملیاتی منصوب شوند. توصیه می‌گردد که به عنوان بخشی از قرارداد استخدام، هر کارمند رجیستری مجبور باشد اظهارنامه ویژه‌ای را امضا کند تا اطلاعات محرمانه

تحلیل، به اشتراک‌گذاری و حفاظت از داده‌های رجیستری در سندی حاوی جزئیات خطرات، خطمشی‌ها و روش‌های مقابله با خطرات تدوین گردد و در اختیار کارکنان قرار گیرد. همچنین، سالانه روش‌های امنیتی رجیستری بررسی و به‌روزرسانی شود. بهتر است قبل از به کارگیری یا اصلاح سیستم، درجه انطباق با قانون تعیین و خطرات مربوط به حریم خصوصی شناسایی شود تا با مشاوره ذی‌نفعان، راهکارهایی جهت جلوگیری یا کاهش خطرات ارائه شود.

تشکر و قدردانی

بدین وسیله از کلیه نویسندگانی که از مطالب آن‌ها در نگارش این پژوهش استفاده شد، تشکر و قدردانی به عمل می‌آید.

تضاد منافع

در انجام مطالعه حاضر، نویسندگان هیچ‌گونه تضاد منافی نداشته‌اند.

(۱۶). در نتیجه، متخصصان بهداشت عمومی باید بهترین رویکردهای اخلاقی را برای پیشرفت اجتماعی، علمی، عدالت و سلامت عمومی به کار گیرند (۱۷، ۱۴).

نتیجه‌گیری

مقرراتی مانند محرمانه بودن داده‌ها، ایمنی و رضایت افراد، نظارت بر رعایت مقررات و قوانین مربوط به نقض محرمانگی داده‌ها، در ایجاد رجیستری بیماری تأثیر می‌گذارد. بدیهی است که تدوین و اجرای ملاحظات اخلاقی و الزامات قانونی کارآمد، انعطاف‌پذیر و به‌موقع، در موفقیت رجیستری مؤثر خواهد بود. الزامات اخلاقی حریم خصوصی، نحوه ایجاد و نگهداری رجیستری، به اشتراک‌گذاری داده‌ها و انتشار گزارش‌ها را در برمی‌گیرد. تدوین الزاماتی در خصوص نحوه استفاده، تجزیه و تحلیل، به اشتراک‌گذاری و حفاظت از داده‌های رجیستری ضرورت دارد.

پیشنهادات

توصیه می‌گردد الزامات اخلاقی و قانونی در خصوص نحوه استفاده، تجزیه و

References

- Krent HJ, Gingo N, Kapp M, Moran R, Neal M, Paulas M, et al. Whose business is your pancreas? Potential privacy problems in New York City's mandatory diabetes registry. *Ann Health Law* 2008; 17(1): 1-37.
- Asher AL, McGirt MJ, Glassman SD, Groman R, Resnick DK, Mehrlich M, et al. Regulatory considerations for prospective patient care registries: Lessons learned from the National Neurosurgery Quality and Outcomes Database. *Neurosurg Focus* 2013; 34(1): E5.
- Nerenz DR. Ethical issues in using data from quality management programs. *Eur Spine J* 2009; 18(Suppl 3): 321-30.
- McCabe LL, McCabe ER. Down syndrome: Issues to consider in a national registry, research database and biobank. *Mol Genet Metab* 2011; 104(1-2): 10-2.
- Hopper L, Hughes S, Burke T, Irving K. A National dementia registry for Ireland: A feasibility analysis. *Proceedings of SPHeRE Network 3rd Annual Conference*; 2017 Jan 12; Dublin, Ireland.
- Gliklich RE, Dreyer NA, Leavy MB. *Registries for evaluating patient outcomes: A user's guide*. 3rd ed. Rockville, MD: Agency for Healthcare Research and Quality (US); 2014.
- Di Iorio CT, Carinci F, Azzopardi J, Baglioni V, Beck P, Cunningham S, et al. Privacy impact assessment in the design of transnational public health information systems: The BIRO project. *J Med Ethics* 2009; 35(12): 753-61.
- Zaletel M, Kralj M. *Methodological guidelines and recommendations for efficient and rational governance of patient registries*. Ljubljana, Slovenia: National Institute of Public Health; 2015.
- Levesque E, Leclerc D, Puymirat J, Knoppers B. Developing registries of volunteers: Key principles to manage issues regarding personal information protection. *J Med Ethics* 2010; 36(11): 712-4.
- European Network of Cancer Registries Working Group on Confidentiality. *Guidelines on confidentiality and ethics for population-based cancer registration and linked activities in Europe (Version 3)*. European Network of Cancer Registries, International Agency for Research on Cancer, May 2011 [Online]. [cited 2018]; Available from: URL: https://www.enrcr.eu/sites/default/files/pdf/ENCR_Eurocourse_GuidelinesConfidentialityEthics.pdf
- Saracci R, Olsen J, Seniori-Costantini A, West R. Epidemiology and the planned new Data Protection Directive of the European Union: A symposium report. *Public Health* 2012; 126(3): 253-5.
- Johnston M, Campbell C, Godlovitch G, Day L, Wysocki J, Dagenais L, et al. Online neurological registries. *Can J Neurol Sci* 2013; 40(4 Suppl 2): S41-S45.
- Ludvigsson JF, Haberg SE, Knudsen GP, Lafolie P, Zoega H, Sarkkola C, et al. Ethical aspects of registry-based research in the Nordic countries. *Clin Epidemiol* 2015; 7: 491-508.
- Rare Disease Task Force. *Patient Registries in the Field of Rare Diseases*, Apr 2009 Update Jun 2011 [Online]. [Cited 2018]; Available from: URL: https://congenitalhi.org/wp-content/uploads/2017/12/RareDiseaseTaskForce_patient-registries-in-the-field-of-rare-diseases-2011.pdf
- Richesson RL, Vehik K. Patient registries. In: Richesson RL, Andrews JE, editors. *Clinical research informatics*. London, UK: Springer London; 2012. p. 233-52.
- Myers J, Frieden TR, Bherwani KM, Henning KJ. Ethics in public health research: privacy and public health at risk: Public health confidentiality in the digital age. *Am J Public Health* 2008; 98(5): 793-801.
- Kass NE. An ethics framework for public health. *Am J Public Health* 2001; 91(11): 1776-82.

Legal Aspects and Ethical Considerations in the Disease Registry: A Scoping Review

Leila Shahmoradi¹, Roya Naemi²

Review Article

Abstract

Collecting accurate data in registries enables the governments to prevent dangerous diseases. However, concerns regarding disclosure have increased due to government involvement. The purpose of the present study was to investigate the legal and ethical aspects of the disease registry including the key elements of confidentiality in disease registry, privacy impact assessment, actions to preserve confidentiality, data ownership, and the consent of participants. This was a scoping review, collecting information through a search in Scopus, PubMed, Web of Science, and Google Scholar databases without time limitation. The findings declare that people's sureness in the confidentiality of information increases the information offered to the registry, and consequently, analysis of this information will improve people's health. Therefore, it is necessary to develop requirements for the use, analysis, sharing, and protection of registry data.

Keywords: Legal Aspects; Ethics; Registries; Disease

Received: 12 Jan., 2019

Accepted: 02 June, 2019

Published: 05 June, 2019

Citation: Shahmoradi L, Naemi R. **Legal Aspects and Ethical Considerations in the Disease Registry: A Scoping Review.** Health Inf Manage 2019; 16(2): 87-93

Article resulted from an independent research without financial support.

1- Associate Professor, Health Information Management, Department of Health Information Management, School of Allied Medical Sciences, Tehran University of Medical Sciences, Tehran, Iran

2- PhD Student, Health Information Management, Department of Health Information Management, School of Allied Medical Sciences, Tehran University of Medical Sciences, Tehran AND Department of Health Information Management, School of Allied Medical Sciences, Ardebil University of Medical Sciences, Ardebil, Iran (Corresponding Author) Email: naemiroya@gmail.com