Original Article Open Access

# Health Law Journal

2024; 2: e7

International ThinkTank of Human Dignity | The Bioethics and Health Law Institute | The Iranian Association of Medical Law

# Medical Data Protection: The Interaction of the Right to Privacy and Artificial Intelligence

**Navid Zamaneh Ghadim[1*], Aram Abbaspour Jalali[2]**

1. Department of Law, Roshdiyeh Institute of Higher Education, Tabriz, Iran.

## ABSTRACT

**Background and Aim:** Advances in healthcare artificial intelligence are occurring rapidly, and the debate about managing its development is increasing. Many AI technologies are ultimately owned and controlled by private entities. The nature of AI implementation could mean that such companies, clinics and public bodies will play a more than usual role in acquiring, using and protecting patient health information. This raises implementation privacy and data security issues. The first challenge involves accessing, using and controlling privately owned patient data. Some recent public-private partnerships to implement artificial intelligence have resulted in weak privacy protections. As such, there are calls for more systematic oversight of big data health research. Appropriate measures should be in place to protect patient privacy and representation. Private data custodians can be influenced by competing objectives and should be structurally incentivized to ensure data protection and prevent alternative uses. Another set of concerns relates to the external risk of privacy violations through AI-based methods. The ability to de-identify or de-identify patient health data may be compromised or even invalidated by new algorithms that have successfully de-identified such data. This can increase the risk to privately held patient data.

**Methods:** This article is written in a descriptive-analytical way.

**Ethical Considerations:** In all stages of writing the present research, while respecting the originality of the texts, honesty and trustworthiness have been observed.

**Results:** Production data can be used to fill data gaps created by these institution-driven perceptions and prevent artificial intelligence systems from becoming inoperable. As for the issue of re-identification, there will be a need for new and improved forms of data protection and anonymization.

**Conclusion:** We are currently in a situation where regulations and oversight are in danger of falling behind the technologies that govern them. Regulations should emphasize patient representation and consent and should encourage more sophisticated methods of anonymization and data protection.

**Keywords:** Right to Privacy; Artificial Intelligence; Bioethics; Medical Data

**Corresponding Author:** Navid Zamaneh Ghadim; **Email:** Navid.zamaneh@roshdiyeh.ac.ir

**Received:** August 20, 2024; **Accepted:** October 23, 2024; **Published Online:** November 26, 2024

**Please cite this article as:**

Zamaneh Ghadim N, Abbaspour Jalali A. Medical Data Protection: The Interaction of the Right to Privacy and Artificial Intelligence. Health Law Journal. 2024; 2: e7.

دسترسی آزاد | مقاله پژوهشی

مجله حقوق سلامت

دوره دوم، ۱۴۰۳

# حفاظت از داده‌های پزشکی: تعامل حق بر حریم خصوصی و هوش مصنوعی

نوید زمانه قدیم[1*]، آرام عباسپور جلالی[1]

۱. گروه حقوق، مؤسسه آموزش عالی رشدیه، تبریز، ایران.

## چکیده

**زمینه و هدف:** پیشرفت در هوش مصنوعی مراقبت‌های بهداشتی به سرعت در حال رخ‌دادن است و بحث در مورد مدیریت توسعه آن در حال افزایش است. بسیاری از فناوری‌های هوش مصنوعی در نهایت تحت مالکیت و کنترل نهادهای خصوصی هستند. ماهیت پیاده‌سازی هوش مصنوعی می‌تواند به این معنا باشد که چنین شرکت‌ها، کلینیک‌ها و نهادهای عمومی نقشی بیش از حد معمول در کسب، استفاده و حفاظت از اطلاعات سلامت بیمار خواهند داشت. این موضوع مسائل مربوط به حریم خصوصی مربوط به پیاده‌سازی و امنیت داده‌ها را ایجاد می‌کند. اولین چالش شامل دسترسی، استفاده و کنترل داده‌های بیمار در مالکیت شخصی است. برخی از مشارکت‌های دولتی و خصوصی اخیر برای پیاده‌سازی هوش مصنوعی منجر به محافظت ضعیف از حریم خصوصی شده است. به این ترتیب، درخواست‌هایی برای نظارت سیستمی بیشتر بر تحقیقات سلامت کلان داده‌ها وجود دارد. برای حفظ حریم خصوصی و نمایندگی بیمار باید تدابیر مناسبی وجود داشته باشد. حافظان خصوصی داده‌ها می‌توانند تحت تأثیر اهداف رقابتی قرار گیرند و باید از نظر ساختاری تشویق شوند تا حفاظت از داده‌ها و جلوگیری از استفاده جایگزین از آن‌ها را تضمین کنند. مجموعه دیگری از نگرانی‌ها به خطر خارجی نقض حریم خصوصی از طریق روش‌های مبتنی بر هوش مصنوعی مربوط می‌شود. توانایی شناسایی یا ناشناس‌کردن داده‌های سلامت بیمار ممکن است با توجه به الگوریتم‌های جدیدی که با موفقیت مجدداً چنین داده‌هایی را شناسایی کرده‌اند، به خطر بیفتد یا حتی باطل شود. این امر می‌تواند خطر را برای داده‌های بیمار تحت سرپرستی خصوصی افزایش دهد.

**روش:** این مقاله به روش توصیفی ـ تحلیلی نگاشته شده است.

**ملاحظات اخلاقی:** در تمام مراحل نگارش پژوهش حاضر، ضمن رعایت اصالت متون، صداقت و امانتداری رعایت شده است.

**یافته‌ها:** داده‌های تولیدی می‌توانند برای پرکردن شکاف‌های داده‌ای که به دلیل این برداشت‌های تحت هدایت نهادها ایجاد شده‌اند، استفاده شوند و از غیر عملیاتی‌شدن سیستم‌های هوش مصنوعی جلوگیری کنند. در مورد مسأله بازشناسایی، نیاز به اشکال جدید و بهبودیافته‌ای از حفاظت داده‌ها و ناشناس‌سازی وجود خواهد داشت.

**نتیجه‌گیری:** در حال حاضر در موقعیتی هستیم که در آن مقررات و نظارت در معرض خطر عقب‌ماندن از فناوری‌های حاکم بر آن‌ها قرار دارد. مقررات باید بر نمایندگی و رضایت بیمار تأکید کند و باید روش‌های پیچیده‌تر برای ناشناس‌سازی و حفاظت از داده‌ها را تشویق کند.

**واژگان کلیدی:** حق بر حریم خصوصی؛ هوش مصنوعی؛ اخلاق زیستی؛ داده‌های پزشکی

**نویسنده مسئول:** نوید زمانه قدیم؛ **پست الکترونیک:** Navid.zamaneh@roshdiyeh.ac.ir

**تاریخ دریافت:** ۱۴۰۳/۰۵/۳۰؛ **تاریخ پذیرش:** ۱۴۰۳/۰۸/۰۲؛ **تاریخ انتشار:** ۱۴۰۳/۰۹/۰۶

**خواهشمند است این مقاله به روش زیر مورد استناد قرار گیرد:**

Zamaneh Ghadim N, Abbaspour Jalali A. Medical Data Protection: The Interaction of the Right to Privacy and Artificial Intelligence. Health Law Journal. 2024; 2: e7.

**مقدمه**

پیشرفت‌های هوش مصنوعی در حوزه بهداشت و درمان به سرعت در حال وقوع است و به زودی تأثیر قابل توجهی در دنیای واقعی خواهد داشت. چندین فناوری جدید هوش مصنوعی به مرحله قابلیت اجرایی نزدیک می‌شوند و چند مورد نیز به ادغام در سیستم‌های بهداشتی نزدیک هستند (۱). در رادیولوژی، هوش مصنوعی در تحلیل تصاویر تشخیصی، بسیار مفید واقع شده است. به عنوان مثال، محققان در دانشگاه استنفورد الگوریتمی تولید کرده‌اند که می‌تواند در عرض چند ثانیه، تصاویر اشعه ایکس قفسه سینه را برای ۱۴ پاتولوژی مختلف تفسیر کند (۲). رادیوتراپی، تخصیص ارگان، جراحی رباتیک و چندین حوزه دیگر در مراقبت‌های بهداشتی نیز در کوتاه‌مدت تا میان‌مدت تحت تأثیر قابل توجهی از فناوری‌های هوش مصنوعی قرار خواهند گرفت (۴-۳). در ایالات متحده، سازمان غذا و دارو (FDA) به تازگی یکی از اولین کاربردهای یادگیری ماشین در مراقبت‌های بالینی را تأیید کرد ـ نرم‌افزاری برای تشخیص رتینوپاتی دیابتی از تصاویر تشخیصی ـ به دلیل این پیشرفت سریع، بحث عمومی فزاینده‌ای درباره خطرات و مزایای هوش مصنوعی و چگونگی مدیریت توسعه آن وجود دارد (۵). بسیاری از کشفیات فناوری در زمینه هوش مصنوعی در یک محیط تحقیقاتی دانشگاهی انجام می‌شود. شرکای تجاری می‌توانند برای انتشار این فناوری‌ها به منظور استفاده در دنیای واقعی ضروری باشند. به همین دلیل، این فناوری‌ها معمولاً تحت یک فرآیند تجاری‌سازی قرار می‌گیرند و در نهایت به مالکیت و کنترل نهادهای خصوصی درمی‌آیند.

علاوه بر این، برخی از فناوری‌های هوش مصنوعی در استارتاپ‌های بیوتکنولوژی یا شرکت‌های خصوصی تأسیس‌شده توسعه یافته‌اند. به عنوان مثال، هوش مصنوعی معروف برای شناسایی رتینوپاتی دیابتی توسط استارتاپ IDx توسعه و نگهداری می‌شود (۶)، چراکه خود هوش مصنوعی می‌تواند به منظور نظارت غیر شفاف باشد، بنابراین نیاز به سطح بالایی از تعامل با شرکت‌های توسعه‌دهنده و نگهدارنده این فناوری اغلب ضروری خواهد بود. سازمان غذا و داروی ایالات متحده به جای اینکه بر روی خود هوش مصنوعی که به طور مداوم در حال تغییر است، تمرکز کند، اکنون مؤسساتی را که هوش مصنوعی را توسعه و نگهداری می‌کنند، رصد می‌نماید (۷). کمیسیون اروپا قانونی را پیشنهاد کرده است که شامل قوانین هماهنگ در زمینه هوش مصنوعی می‌باشد و اصول حریم خصوصی و مسئولیت سازمانی را ترسیم می‌کند (۸) که بسیار مشابه با آنچه در مقررات عمومی حفاظت از داده‌های اروپا (GDPR) وجود دارد، است (۹). سایر کشورها مانند کانادا هنوز نتوانسته‌اند مقررات خاصی برای هوش مصنوعی تنظیم کنند. هوش مصنوعی همچنان یک مرز نسبتاً نوین در حوزه بهداشت جهانی است و در حال حاضر فاقد یک چهارچوب قانونی و نظارتی جامع جهانی می‌باشد (۱۰). ترتیبات اجرایی تجاری که ذکر شده است، نیازمند قراردادن اطلاعات سلامت بیماران تحت کنترل شرکت‌های سودآور خواهد بود، اگرچه این موضوع به خودی خود جدید نیست، اما ساختار رابط عمومی ـ خصوصی که در اجرای هوش مصنوعی در حوزه بهداشت و درمان استفاده می‌شود، می‌تواند به این معنا باشد که چنین شرکت‌هایی، همچنین کلینیک‌های تحت مالکیت و برخی از مؤسسات عمومی تأمین مالی شده، نقش بیشتری در به دست‌آوردن، استفاده و حفاظت از اطلاعات سلامت بیماران خواهند داشت. در این مقاله نگرانی‌های مربوط به حریم خصوصی در زمینه هوش مصنوعی تجاری در حوزه بهداشت و درمان بررسی می‌شود و بر روی هر دو جنبه اجرای آن و امنیت داده‌های جاری متمرکز است.

شایان ذکر است در خصوص پیشینه تحقیق چندین مقاله معتبر علمی به این موضوع پرداخته‌اند. ویلیامسون (Williamson) و همکاران در مقاله خود به بررسی چالش‌های مرتبط با حفظ حریم خصوصی در استفاده از هوش مصنوعی در سیستم‌های بهداشتی پرداخته است. مقاله روش‌های مختلفی مانند «حریم خصوصی افتراقی» و رمزنگاری را برای حفظ محرمانگی داده‌ها بررسی کرده و به اهمیت تنظیم مقررات و نظارت سیستماتیک بر این فناوری‌ها تأکید می‌کند (۱۱). جنتری (Gentry) و همکاران در مقاله

خود به بررسی روش‌های مختلف حفظ حریم خصوصی در کاربردهای هوش مصنوعی در پزشکی می‌پردازد. تکنیک‌هایی مانند رمزنگاری هومومورفیک و یادگیری فدرالی از جمله مواردی است که برای محافظت از داده‌های بیماران بدون افشای اطلاعات شخصی معرفی شده‌اند. همچنین به چالش‌های الگوریتم‌های هوش مصنوعی در مواجهه با حملات امنیتی پرداخته شده است (۱۲). همت و همکاران در مقاله خود به مشکلات امنیتی و حریم خصوصی در استفاده از هوش مصنوعی در مراقبت‌های بهداشتی پرداخته و استراتژی‌های مختلفی مانند محدودکردن دسترسی به داده‌ها و استفاده از پروتکل‌های رمزنگاری برای محافظت از اطلاعات بیماران را بررسی می‌کند. همچنین مقاله به اهمیت نقش پزشکان در تضمین سلامت و امنیت اطلاعات در مقابل الگوریتم‌های هوش مصنوعی اشاره دارد (۱۳). لیانگ (L.Yang) و همکاران در مقاله خود بر پیامدهای هوش مصنوعی برای حفظ حریم خصوصی در بخش بهداشت و درمان متمرکز است و به بحث در مورد چالش‌های روان‌شناختی و قانونی مرتبط با استفاده از داده‌های پزشکی توسط سیستم‌های هوش مصنوعی می‌پردازد. مقاله همچنین راهکارهای جدید برای ایجاد تعادل بین پیشرفت فناوری و حفظ حریم خصوصی را پیشنهاد می‌دهد (۱۴). موسا (Moussa) و همکاران در مقاله خود چالش‌های مرتبط با حفاظت از داده‌های بهداشتی در عصر هوش مصنوعی را تحلیل کرده و به بررسی روش‌های نوین حفظ حریم خصوصی همچون استفاده از «یادگیری ماشین ایمن» پرداخته است. نویسندگان به اهمیت ایجاد چهارچوب‌های قانونی برای جلوگیری از نقض حریم خصوصی در نتیجه کاربرد گسترده هوش مصنوعی اشاره دارند (۱۵).

## ملاحظات اخلاقی

در پژوهش حاضر جنبه‌های اخلاقی مطالعه کتابخانه‌ای شامل اصالت متون، صداقت و امانتداری رعایت شده است.

## روش

این مقاله به روش توصیفی ـ تحلیلی نگاشته شده است.

## یافته‌ها

یافته‌های تحقیق نشان می‌دهد که در حال حاضر در موقعیتی هستیم که در آن مقررات و نظارت در معرض خطر عقب‌ماندن از فناوری‌های حاکم بر آن‌ها قرار دارد. مقررات باید بر نمایندگی و رضایت بیمار تأکید کند و باید روش‌های پیچیده‌تر برای ناشناس‌سازی و حفاظت از داده‌ها را تشویق کند.

## بحث

**۱. داده‌های پزشکی و لزوم حفاظت از آن:** داده‌های پزشکی شامل اطلاعاتی است که درباره سلامت جسمی، روانی و سابقه پزشکی افراد جمع‌آوری می‌شود. این داده‌ها می‌توانند به صورت فردی یا عمومی مورد استفاده قرار گیرند و شامل اطلاعاتی چون سوابق درمانی، نتایج آزمایش‌های پزشکی، تصاویر پزشکی (مثل رادیولوژی)، علائم حیاتی، تشخیص‌های پزشکی و داروهای مصرفی باشند. داده‌های پزشکی شامل موارد زیر هستند:

داده‌های تشخیصی: اطلاعات مرتبط با وضعیت سلامتی فرد، شامل نتایج آزمایش‌ها، بررسی‌های بالینی و تشخیص‌های پزشکی.

داده‌های درمانی: اطلاعات مربوط به درمان‌های انجام شده بر روی فرد، شامل داروها، جراحی‌ها و برنامه‌های درمانی.

داده‌های سلامتی: شامل علائم حیاتی مثل فشار خون، ضربان قلب و سایر معیارهای مربوط به وضعیت سلامت عمومی افراد.

داده‌های ژنتیکی: اطلاعات مرتبط با دی‌ان‌ای و ژنوم فرد که می‌تواند نشان‌دهنده ریسک بیماری‌های ژنتیکی باشد.

این داده‌ها می‌توانند به شکل الکترونیکی یا کاغذی ثبت شوند و در سیستم‌های بهداشتی مختلف (مثل پرونده الکترونیکی سلامت Electronic Health Records) ذخیره شوند (۱۶).

از منظر حقوقی، داده‌های پزشکی به عنوان اطلاعات حساس و شخصی در نظر گرفته می‌شوند که نیازمند حفاظت‌های خاص هستند. در بیشتر قوانین ملی و بین‌المللی، این داده‌ها تحت قوانین حفاظت از داده‌ها و حریم خصوصی قرار می‌گیرند. به عنوان مثال: قانون ( GDPR: General Data Protection Regulation) در اتحادیه اروپا داده‌های پزشکی را به عنوان «داده‌های حساس شخصی» تعریف می‌کند که تحت حمایت‌های ویژه‌ای قرار دارند. بر اساس ماده ۹ این قانون، پردازش داده‌های پزشکی تنها با رضایت صریح فرد یا تحت شرایط قانونی خاص مجاز است (۱۷). قانون HIPAA ( Health Insurance Portability and Accountability Act) در ایالات متحده آمریکا نیز حفاظت از داده‌های پزشکی را الزامی می‌داند و برای نهادهای بهداشتی و درمانی دستورالعمل‌هایی برای حفظ محرمانگی و امنیت این اطلاعات تعیین می‌کند (۱۸). بر اساس این قوانین، داده‌های پزشکی تنها باید با رضایت صریح افراد پردازش شود و نهادهای مسئول موظف به اتخاذ تدابیر امنیتی برای جلوگیری از افشای غیر مجاز این داده‌ها هستند.

حفاظت از داده‌های پزشکی به دلایل مختلف حقوقی و اخلاقی امری ضروری است. داده‌های پزشکی اطلاعاتی حساس و شخصی هستند که نه‌تنها وضعیت سلامتی فرد را نشان می‌دهند، بلکه می‌توانند در صورت سوءاستفاده، منجر به آسیب‌های اجتماعی، روانی یا اقتصادی شوند. قوانین حقوقی در بسیاری از کشورها به طور خاص به حفاظت از این داده‌ها می‌پردازند و مقررات سخت‌گیرانه‌ای برای جمع‌آوری، پردازش، و افشای آن‌ها تعیین کرده‌اند. قانون GDPR که در سال ۲۰۱۸ در اتحادیه اروپا به اجرا درآمد، یکی از جامع‌ترین و سخت‌گیرانه‌ترین قوانین مربوط به حفاظت از داده‌های شخصی است. این قانون به طور ویژه داده‌های پزشکی را در دسته «داده‌های حساس» قرار داده و آن‌ها را مستلزم حفاظت بیشتری می‌داند. بر اساس ماده ۹ این قانون، پردازش داده‌های سلامت تنها در صورتی مجاز است که رضایت صریح فرد گرفته شود یا این عمل تحت شرایط قانونی خاص، نظیر منافع عمومی یا پزشکی، انجام شود. ماده ۹ این قانون به وضوح بیان می‌کند که جمع‌آوری، پردازش و نگهداری این داده‌ها باید تحت پروتکل‌های دقیق امنیتی انجام شود تا از افشای غیر مجاز یا دسترسی بدون اجازه جلوگیری شود. همچنین افراد حق دارند بدانند داده‌های شخصی‌شان چگونه و توسط چه کسانی استفاده می‌شود که این امر به افزایش شفافیت و اطمینان افراد کمک می‌کند. قانون HIPAA که در سال ۱۹۹۶ در ایالات متحده تصویب شد، یکی از اولین تلاش‌ها برای حفاظت از داده‌های پزشکی و حریم خصوصی افراد در حوزه سلامت بود. این قانون به ویژه به «قواعد حریم خصوصی (Privacy Rule)» و «قواعد امنیت (Security Rule)» اشاره دارد که نهادهای بهداشتی و درمانی را ملزم می‌کند تا تدابیر سخت‌گیرانه‌ای برای حفاظت از داده‌های سلامت بیماران اتخاذ کنند. بر اساس این قانون، تمامی مؤسسات درمانی، بیمه‌گران سلامت و ارائه‌دهندگان خدمات بهداشتی باید اطمینان حاصل کنند که اطلاعات پزشکی افراد به شیوه‌ای امن ذخیره و پردازش می‌شود. همچنین، HIPAA به افراد این حق را می‌دهد که به داده‌های پزشکی خود دسترسی داشته باشند و در صورت نیاز درخواست تصحیح یا حذف این داده‌ها را ارائه کنند.

حفاظت از داده‌های پزشکی نه‌تنها یک الزام قانونی، بلکه از حقوق بنیادین بشر نیز محسوب می‌شود. حق بر حریم خصوصی که در بسیاری از اسناد بین‌المللی نظیر اعلامیه جهانی حقوق بشر (ماده ۱۲) و میثاق بین‌المللی حقوق مدنی و سیاسی (ماده ۱۷) مورد تأکید قرار گرفته، به این معناست که هر فرد حق دارد که اطلاعات شخصی و پزشکی او بدون رضایت مورد افشا یا سوءاستفاده قرار نگیرد. این حقوق نه‌تنها در چهارچوب حفاظت از کرامت انسانی، بلکه به عنوان یک ابزار مهم برای جلوگیری از تبعیض، سوءاستفاده و بهره‌برداری‌های غیر قانونی از اطلاعات پزشکی افراد، اهمیت دارد.

**۲. حق بر حریم خصوصی و هوش مصنوعی:** حق بر حریم خصوصی یکی از حقوق بنیادین بشر است که در اسناد بین‌المللی نظیر اعلامیه جهانی حقوق بشر (ماده ۱۲) و میثاق بین‌المللی حقوق مدنی و سیاسی (ماده ۱۷) به رسمیت

شناخته شده است. این حق به ویژه در زمینه‌های جدیدی مانند هوش مصنوعی که به طور فزاینده‌ای در حال گسترش است، با چالش‌های تازه‌ای مواجه شده است. استفاده از هوش مصنوعی برای جمع‌آوری، تحلیل و پردازش داده‌های شخصی، به ویژه در بخش‌هایی مانند سلامت و امنیت، پرسش‌های حقوقی و اخلاقی گسترده‌ای را در مورد حفاظت از حریم خصوصی افراد ایجاد کرده است.

حق بر حریم خصوصی به معنای حفظ و محافظت از اطلاعات شخصی افراد در برابر هرگونه دخالت یا دسترسی غیر مجاز است. این حق نه‌تنها در سطح فردی، بلکه به عنوان یک بخش از حقوق بنیادین بشر در بسیاری از قوانین ملی و بین‌المللی به رسمیت شناخته شده است. برای مثال، ماده ۸ کنوانسیون اروپایی حقوق بشر به صراحت از حق افراد برای حفاظت از زندگی خصوصی و اطلاعات شخصی خود حمایت می‌کند (۱۹). در دوران دیجیتال، این حق به چالش‌های جدیدی برخورده است. افزایش جمع‌آوری داده‌های شخصی توسط دولت‌ها و شرکت‌ها و به ویژه کاربرد هوش مصنوعی برای پردازش حجم عظیمی از داده‌ها، این حق را بیش از پیش در معرض خطر قرار داده است. در واقع، توانایی هوش مصنوعی برای تجزیه و تحلیل داده‌ها و استخراج اطلاعات حساس از آن‌ها، می‌تواند به راحتی موجب نقض حریم خصوصی شود.

هوش مصنوعی با توانایی تحلیل و پردازش حجم وسیعی از داده‌ها، به طور مستقیم بر حق بر حریم خصوصی تأثیر می‌گذارد. یکی از بزرگترین چالش‌ها در این حوزه، مسأله شناسایی مجدد (Re-Identification) است، حتی اگر داده‌های فردی به صورت ناشناس ذخیره شوند، الگوریتم‌های پیشرفته هوش مصنوعی می‌توانند از طریق تحلیل الگوها و داده‌های دیگر، هویت افراد را دوباره شناسایی کنند. این مسأله، به ویژه در مورد داده‌های حساس پزشکی یا ژنتیکی، یک چالش حقوقی و اخلاقی جدی محسوب می‌شود (۲۰).

یکی از مهم‌ترین قوانین بین‌المللی که به حفاظت از داده‌های شخصی در برابر تهدیدات فناوری‌های نوین، از جمله هوش مصنوعی، می‌پردازد، مقررات عمومی حفاظت از داده‌های اتحادیه اروپا (GDPR) است. این قانون، استفاده از داده‌های شخصی را به شدت محدود می‌کند و شرکت‌ها را ملزم به رعایت اصول شفافیت، امنیت و رضایت کاربران برای پردازش داده‌های شخصی می‌کند. بر اساس GDPR، هرگونه پردازش داده‌های شخصی که شامل استفاده از الگوریتم‌های هوش مصنوعی می‌شود، تنها در صورتی مجاز است که:

رضایت صریح و آگاهانه افراد جلب شود؛

حقوق افراد در برابر تصمیم‌گیری‌های خودکار تضمین شود؛

اقدامات حفاظتی مناسب برای جلوگیری از دسترسی غیر مجاز به داده‌های شخصی صورت گیرد.

همچنین ماده ۲۲ این قانون تأکید دارد که افراد حق دارند از تصمیم‌گیری‌های خودکار (که توسط هوش مصنوعی انجام می‌شود) دوری کنند، مگر اینکه رضایت صریح داشته باشند یا این تصمیم‌گیری در راستای منافع قانونی و مشروع باشد.

یکی از چالش‌های دیگر در استفاده از هوش مصنوعی در رابطه با حریم خصوصی، خطر تبعیض است. الگوریتم‌های هوش مصنوعی می‌توانند از طریق داده‌های شخصی، تصمیم‌گیری‌هایی انجام دهند که به طور غیر مستقیم منجر به تبعیض شود. برای مثال، در حوزه‌های بهداشت، امنیت و استخدام، الگوریتم‌ها می‌توانند بر اساس اطلاعات جمع‌آوری‌شده، نتایج نامتعادلی ایجاد کنند که افراد یا گروه‌های خاصی را به طور ناعادلانه‌ای در معرض خطر قرار می‌دهد (۲۱). حفظ توازن بین نوآوری در حوزه هوش مصنوعی و حفظ حریم خصوصی یکی از چالش‌های اساسی دوران دیجیتال است. فناوری هوش مصنوعی دارای پتانسیل عظیمی برای بهبود خدمات اجتماعی و اقتصادی است، اما همزمان نیازمند ایجاد مکانیسم‌های قانونی و فنی است که از نقض حریم خصوصی جلوگیری کند. برخی از تکنیک‌ها مانند یادگیری فدرالی و حریم خصوصی افتراقی تلاش می‌کنند تا این توازن را حفظ کنند، به گونه‌ای که داده‌های شخصی افراد بدون نقض حریم خصوصی پردازش شوند (۲۲).

**۳. نگرانی در مورد دسترسی، استفاده و کنترل:** هوش مصنوعی دارای چندین ویژگی منحصر به فرد در مقایسه با

فناوری‌های بهداشتی سنتی است، به ویژه ممکن است به نوع خاصی از خطاها و تعصبات مستعد باشد و گاهی اوقات نمی‌توان به راحتی یا حتی به طور عملی توسط متخصصان (انسانی) پزشکی نظارت شود. این امر به دلیل مشکل به اصطلاح «جعبه سیاه» در ابزارهای هوش مصنوعی پزشکی در حفاظت از داده‌ها است که در آن روش‌های الگوریتم‌های یادگیری و «استدلال» مورد استفاده برای رسیدن به نتایجشان می‌تواند به طور جزئی یا کاملاً برای ناظران انسانی غیر شفاف باشد (۲۳). اگر تدابیر مناسب حفاظتی در دسترس نباشد، این عدم شفافیت ممکن است به نحوه استفاده و دستکاری اطلاعات سلامت و شخصی نیز مربوط باشد، به ویژه، در پاسخ به این مشکل، بسیاری از پژوهشگران در حال توسعه اشکال قابل تفسیر از هوش مصنوعی هستند که ادغام آن‌ها در مراقبت‌های پزشکی آسان‌تر خواهد بود (۲۴). به دلیل ویژگی‌های منحصر به فرد هوش مصنوعی، سیستم‌های نظارتی که برای تأیید و نظارت مداوم استفاده می‌شوند نیز باید منحصر به فرد باشند. بخش قابل توجهی از فناوری‌های موجود مرتبط با یادگیری ماشین و شبکه‌های عصبی در دست شرکت‌های بزرگ فناوری قرار دارد. گوگل، مایکروسافت، آی‌بی‌ام، اپل و سایر شرکت‌ها همه به طور خاص در حال «آماده‌سازی، به شیوه‌های خود، پیشنهادهایی برای آینده سلامت و جنبه‌های مختلف صنعت بهداشت و درمان جهانی» هستند (۲۵). توافق‌نامه‌های اشتراک‌گذاری اطلاعات می‌توانند برای اعطای دسترسی به اطلاعات سلامت بیماران به این مؤسسات خصوصی مورد استفاده قرار گیرند. همچنین برخی از مشارکت‌های عمومی ـ خصوصی اخیر برای پیاده‌سازی یادگیری ماشین منجر به حفاظت ضعیف از حریم خصوصی شده است. به عنوان مثال، دیپ‌مایند که متعلق به شرکت آلفابت (که از این پس به عنوان گوگل اشاره می‌شود) است، در سال ۲۰۱۶ با بنیاد NHS رویال فری لندن همکاری کرد تا از یادگیری ماشین برای کمک به مدیریت آسیب حاد کلیه استفاده کند (۲۶). منتقدان اشاره کردند که به بیماران اجازه داده نشده بود که در مورد استفاده از اطلاعات خود تصمیم‌گیری کنند و همچنین تأثیرات حریم خصوصی به طور کافی مورد بحث قرار نگرفته بود. یک مشاور ارشد در وزارت بهداشت انگلستان اذعان نمود که اطلاعات بیماران بر اساس «پایه قانونی نامناسب» به دست آمده است (۲۷). جدال بیشتری پس از آن به وجود آمد که گوگل به طور مستقیم کنترل اپلیکیشن دیپ‌مایند را به دست گرفت و به طور مؤثر کنترل داده‌های ذخیره‌شده بیماران را از بریتانیا به ایالات متحده منتقل کرد (۲۸). توانایی به طور اساسی «ضمیمه» کردن مقادیر انبوهی از داده‌های خصوصی بیماران به حوزه قضایی دیگر، واقعیت جدیدی از داده‌های کلان است و در زمان پیاده‌سازی هوش مصنوعی در حوزه بهداشت و درمان تجاری، در معرض خطر بیشتری قرار دارد. تمرکز نوآوری‌های فناوری و دانش در شرکت‌های بزرگ فناوری، عدم تعادل قدرتی ایجاد می‌کند که در آن نهادهای عمومی می‌توانند وابسته‌تر و کمتر به عنوان یک شریک برابر و داوطلب در پیاده‌سازی فناوری‌های بهداشتی عمل کنند.

در حالی که برخی از این نقض‌های حریم خصوصی بیماران ممکن است با وجود قوانین، مقررات و سیاست‌های حریم خصوصی موجود رخ داده باشد، از مثال دیپ‌مایند مشخص است که باید تدابیر مناسبی برای حفظ حریم خصوصی و اختیار بیماران در زمینه این مشارکت‌های عمومی ـ خصوصی وجود داشته باشد. فراتر از احتمال سوءاستفاده‌های عمومی از قدرت، هوش مصنوعی چالش جدیدی را به وجود می‌آورد، زیرا الگوریتم‌ها معمولاً به دسترسی به مقادیر زیادی از داده‌های بیماران نیاز دارند و ممکن است از این داده‌ها به روش‌های مختلف در طول زمان استفاده کنند. مکان و مالکیت سرورها و کامپیوترهایی که اطلاعات سلامت بیماران را برای استفاده هوش مصنوعی در حوزه بهداشت و درمان ذخیره و دسترسی می‌یابند، در این سناریوها اهمیت زیادی دارد. قوانین باید ایجاب کنند که داده‌های بیماران در حوزه قضایی که از آن به دست آمده‌اند، البته با لحاظ استثنائاتی محدود باقی بمانند. حفاظت قوی از حریم خصوصی زمانی قابل تحقق است که نهادها به طور ساختاری تشویق شوند تا با طراحی‌های خود به همکاری برای تضمین حفاظت از داده‌ها بپردازند (۲۹). پیاده‌سازی‌های تجاری هوش مصنوعی در حوزه بهداشت و

درمان می‌تواند برای اهداف حفاظت از حریم خصوصی قابل مدیریت باشد، اما اهداف متضادی را معرفی می‌کند. همانطور که مشاهده شد، شرکت‌ها اگر بتوانند از داده‌ها کسب درآمد کنند یا به نوعی از آن‌ها بهره‌برداری کنند و اگر مجازات‌های قانونی به اندازه کافی سنگین نباشند تا این رفتار را جبران کنند، ممکن است به اندازه کافی تشویق نشوند که همیشه از حریم خصوصی محافظت کنند. به این دلیل و نیز سایر نگرانی‌ها، درخواست‌هایی برای نظارت سیستماتیک بیشتر بر تحقیقات و فناوری‌های بهداشت و درمان با داده‌های کلان مطرح شده است (۳۰).

با توجه به نمونه‌هایی از سوءاستفاده‌های شرکتی از اطلاعات سلامت بیماران که در همه کشورها قابل مشاهده است، جای تعجب نیست که مسائل مربوط به اعتماد عمومی می‌تواند به وجود آید. به عنوان مثال، یک نظرسنجی در سال ۲۰۱۸ از چهار هزار بزرگسال آمریکایی نشان داد که تنها ۱۱ درصد مایل به اشتراک‌گذاری داده‌های سلامت خود با شرکت‌های فناوری بودند، در حالی که ۷۲ درصد مایل به اشتراک‌گذاری این داده‌ها با پزشکان بودند ۳۱). علاوه بر این، تنها ۳۱ درصد از افراد در مورد امنیت داده‌های شرکت‌های فناوری «تا حدی مطمئن» یا «معتمد» بودند (۳۲). در برخی کشورها مانند ایالات متحده، این موضوع مانع از آن نشده است که بیمارستان‌ها داده‌های بیماران را که به طور کامل ناشناس‌سازی نشده‌اند، با شرکت‌هایی مانند مایکروسافت و آی‌بی‌ام به اشتراک بگذارند (۳۳). عدم اعتماد عمومی ممکن است نظارت عمومی بر پیاده‌سازی‌های تجاری هوش مصنوعی در حوزه بهداشت و درمان را افزایش دهد یا حتی منجر به دعاوی حقوقی علیه آن‌ها شود.

**۴. ایراد بازشناسایی:** نگرانی دیگری که در مورد استفاده از داده‌های کلان در هوش مصنوعی تجاری وجود دارد، به خطرات خارجی نقض حریم خصوصی ناشی از سیستم‌های الگوریتمی بسیار پیشرفته مربوط می‌شود. نقض داده‌های بهداشتی در بسیاری از کشورها در سراسر جهان، از جمله ایالات متحده (۳۴)، کانادا (۳۵) و اروپا (۳۶) افزایش یافته است و در حالی که ممکن است در حال حاضر به طور گسترده‌ای توسط هکرها استفاده نشوند، هوش مصنوعی و سایر الگوریتم‌ها به ناتوانی فزاینده در حفاظت از اطلاعات سلامت کمک می‌کنند. تعدادی از مطالعات اخیر نشان داده‌اند که چگونه استراتژی‌های محاسباتی نوظهور می‌توانند برای شناسایی افراد در مخازن داده‌های بهداشتی که توسط نهادهای عمومی یا خصوصی مدیریت می‌شوند، مورد استفاده قرار گیرند و این موضوع حتی در صورتی که اطلاعات ناشناس شده و از تمام شناسه‌ها پاک شده باشد، نیز صادق است (۳۷). یک مطالعه در سال ۲۰۱۸ نتیجه‌گیری کرد که داده‌های جمع‌آوری‌شده توسط شرکت‌های نسل‌شناسی می‌تواند برای شناسایی تقریباً ۶۰ درصد از آمریکایی‌های با نژاد اروپایی استفاده شود و اینکه در آینده نزدیک، این درصد احتمالاً به طور قابل توجهی افزایش خواهد یافت (۳۸). علاوه بر این، یک مطالعه در سال ۲۰۱۹ به طور موفقیت‌آمیز از یک «چهارچوب حمله پیوندی» استفاده کرد ـ به عبارت دیگر، یک الگوریتم که هدف آن بازشناسایی اطلاعات بهداشتی ناشناس است ـ که می‌تواند داده‌های بهداشتی آنلاین را به افراد واقعی در دنیای واقعی مرتبط کند و «آسیب‌پذیری داده‌های بهداشتی آنلاین موجود» را نشان دهد (۳۹) و این تنها چند نمونه از رویکردهای در حال توسعه است که سؤالاتی را درباره امنیت اطلاعات بهداشتی که به عنوان محرمانه تلقی می‌شود، مطرح کرده است. در واقع، پیشنهاد شده است که «تکنیک‌های بازشناسایی امروزی به طور مؤثری پاک‌سازی را بی‌اثر کرده و حریم خصوصی را به خطر می‌اندازند» (۴۰).

این واقعیت به طور بالقوه خطرات حریم خصوصی را در مورد اجازه‌دادن به شرکت‌های خصوصی هوش مصنوعی برای کنترل اطلاعات سلامت بیماران افزایش می‌دهد، حتی در شرایطی که «ناشناس‌سازی» انجام می‌شود. همچنین سؤالاتی درباره مسئولیت، قابلیت بیمه و سایر مسائل عملی که با مواردی که نهادهای دولتی به طور مستقیم کنترل داده‌های بیماران را در دست دارند، متفاوت است، مطرح می‌کند. با توجه به ماهیت متغیر و پیچیده ریسک‌های قانونی که

توسعه‌دهندگان و نگهدارندگان هوش مصنوعی خصوصی ممکن است در هنگام کار با حجم بالای داده‌های بیماران با آن مواجه شوند، نیاز به تنظیم قراردادهای دقیقی است که حقوق و تعهدات طرفین درگیر و مسئولیت در قبال نتایج منفی بالقوه مختلف را مشخص کند.

یکی از راه‌هایی که توسعه‌دهندگان سیستم‌های هوش مصنوعی می‌توانند به طور بالقوه نگرانی‌های مداوم درباره حریم خصوصی را برطرف کنند، استفاده از داده‌های تولیدی است. مدل‌های تولیدی توانایی تولید داده‌های بیمار واقعی، اما مصنوعی را بدون ارتباط با افراد واقعی توسعه می‌دهند (۴۱) که می‌تواند یادگیری ماشین را بدون استفاده طولانی‌مدت از داده‌های واقعی بیماران امکان‌پذیر کند، هرچند ممکن است در ابتدا برای ایجاد مدل تولیدی به داده‌های واقعی نیاز باشد.

## نتیجه‌گیری

عصر حاضر یک دوره جالب و جذاب در توسعه و پیاده‌سازی هوش مصنوعی در حوزه بهداشت و درمان است و بیمارانی که داده‌هایشان توسط این هوش‌های مصنوعی استفاده می‌شود، باید به طور قابل توجهی، اگر نه به طور چشم‌گیری، از بهبودهای سلامتی که این فناوری‌ها ایجاد می‌کنند، بهره‌مند شوند. با این حال، پیاده‌سازی هوش مصنوعی تجاری در حوزه بهداشت و درمان با چالش‌های جدی حریم خصوصی مواجه است. اطلاعات پزشکی شخصی یکی از خصوصی‌ترین و از نظر حقوقی محافظت‌شده‌ترین اشکال داده‌ها است. نگرانی‌های قابل توجهی در مورد اینکه چگونه دسترسی، کنترل و استفاده از این اطلاعات توسط طرف‌های سودجو ممکن است با گذشت زمان و با پیشرفت هوش مصنوعی خودبه خود بهبود یابنده تغییر کند، وجود دارد. تأکید بر اختیار و رضایت بیمار در توسعه مقررات در این حوزه، ارزش‌های حقوقی و اخلاقی کلیدی دموکراسی‌های لیبرال را منعکس می‌کند. به عنوان مثال، الزامات برای کسب رضایت آگاهانه مکرر با استفاده از فناوری برای کاربردهای جدید داده‌ها، در صورت امکان، به حفظ حریم خصوصی و اختیار بیماران کمک خواهد کرد.

همچنین حق برداشت داده‌ها می‌تواند به وضوح ارتباط برقرار شود و به ویژه آسان‌تر برای اجرا فراهم گردد؛ در صورت امکان، داده‌های تولیدی می‌توانند برای پرکردن شکاف‌های داده‌ای که به دلیل این برداشت‌های تحت هدایت نهادها ایجاد شده‌اند، استفاده شوند و از غیر عملیاتی‌شدن سیستم‌های هوش مصنوعی جلوگیری کنند. در مورد مسأله بازشناسایی، نیاز به اشکال جدید و بهبودیافته‌ای از حفاظت داده‌ها و ناشناس‌سازی وجود خواهد داشت. این امر نیازمند نوآوری است و همچنین یک جنبه نظارتی برای اطمینان از اینکه نگهدارندگان خصوصی داده‌ها از روش‌های پیشرفته و ایمن برای حفاظت از حریم خصوصی بیماران استفاده می‌کنند، وجود خواهد داشت. ما در حال حاضر در وضعیتی هستیم که مقررات و نظارت ممکن است از فناوری‌هایی که بر آن‌ها حاکم هستند، عقب بمانند. با توجه به اینکه اکنون با فناوری‌هایی سروکار داریم که می‌توانند به سرعت خود را بهبود بخشند، خطر این وجود دارد که به سرعت پسروی کنیم.

## مشارکت نویسندگان

نوید زمانه قدیم: ارائه ایده و موضوع، طرح بحث، گردآوری مطالب، تدوین پژوهش.

آرام عباسپور جلالی: گردآوری مطالب، تدوین پژوهش و معرفی.

نویسندگان نسخه نهایی را مطالعه و تأیید نموده و مسئولیت پاسخگویی در قبال پژوهش را پذیرفته‌اند.

## تشکر و قدردانی

ابراز نشده است.

## تضاد منافع

نویسندگان هیچ‌گونه تضاد منافع احتمالی را در رابطه با تحقیق، تألیف و انتشار این مقاله اعلام نکرده‌اند.

**تأمین مالی**

نویسندگان اظهار می‌نمایند که هیچ‌گونه حمایت مالی برای تحقیق، تألیف و انتشار این مقاله دریافت نکرده‌اند.

**References**

1. Jiang F, Jiang Y, Dong Y, Li H, Zhi H, Ma S, et al. Artificial intelligence in healthcare: past, present and future. Stroke Vasc Neurol. 2017; 2(4): 230-243.

2. Armitage H. Artificial intelligence rivals radiologists in screening X-rays for certain diseases. Stanford Medicine News Center. 2018. Available at: https://www.med.stanford.edu/news/all-news/2018/11/ai-outperformed-radiologists-in-screening-x-rays-for-certain-diseases.html.

3. Thompson RF, Rosman G, Rus D, Meireles O. Artificial intelligence in radiation oncology: A specialty-wide disruptive transformation? Radiother Oncol. 2018; 129(3): 70-76.

4. Hashimoto DA, Rosman G, Rus D, Meireles DR. Artificial intelligence in surgery: Promises and perils. Ann Surg. 2018; 268(1): 70-76.

5. FDA. FDA permits marketing of artificial intelligence-based device to detect certain diabetes related eye problems. 2018. Available at: https://www.fda.gov/news-events/press-announcements/fda-permits-marketing-artificial-intelligence-based-device-detect-certain-diabetes-related-eye.

6. Hamid S. The opportunities and risks of artificial intelligence in medicine and healthcare. CUSPE Commun. 2016; 1-4.

7. FDA. Digital Health Software Precertification (Pre-Cert) Program. 2019. https://www.fda.gov/medical-devices/digital-health/digital-health-software-precertification-pre-cert-program.

8. European Commission. Proposal for a regulation of the European parliament and of the council laying down harmonized rules on artificial intelligence (artificial intelligence act) and amending certain union legislative acts. 2021.

9. European Data Protection Supervisor. Accountability. https://edps.europa.eu/data-protection/our-work/subjects/accountability_en

10) Health Canada. Responsible use of artificial intelligence (AI). 2020. https://www.canada.ca/en/government/system/digital-government/digitalgovernment-innovations/responsible-use-ai.html#toc2.

11. Williamson S M, Prybutok V. Balancing Privacy and Progress: A Review of Privacy Challenges, Systemic Oversight, and Patient Perceptions in AI-Driven Healthcare. Applied Sciences. 2024; 14(2): 1-47.

12. Gentry C, Sahai A, Waters B. Homomorphic encryption from learning with errors: Conceptually simpler, asymptotically faster, attribute-based. Edited by Canetti R, Garay JA. Advances in Cryptology-CRYPTO. Berlin: Springer; 2013. Vol.8042.

13. Hamet P, Tremblay J. Artificial intelligence in medicine. Metabolism, 2017; 69: 36–40.

14. Na L, Yang C, Lo CC, Zhao F, Fukuoka Y, Aswani A. Feasibility of reidentifying individuals in large national physical activity data sets from which protected health information has been removed with use of machine learning. JAMA Network Open. 2018; 1(8): e186040.

15. Moussa M, Demurjian S. Differential privacy approach for big data privacy in healthcare. Edited by Tamane S, Solanki VK, Dey N. Privacy and Security Policies in Big Data. IGI Global. 2017; 191-213.

16. Lee CH, Yoon HJ. Medical big data: Promise and challenges. Kidney Research and Clinical Practice. 2017; 36(1): 3-11.

17. GDPR. General Data Protection Regulation, Article 9. 2018. Available at: https://www.gdpr-info.eu/art-9-gdpr.

18. HIPAA. Health Insurance Portability and Accountability Act. 1996. Available at: https://www.hhs.gov/hipaa.

19. Council of Europe. European Convention on Human Rights, Article 8. 1950. Available at: https://www.echr.coe.int/Pages/home.aspx?p=basictexts.

20. Na L, Yang C, Lo CC, Zhao F, Fukuoka Y, Aswani A. Feasibility of reidentifying individuals in large national physical activity data sets from which protected health information has been removed with use of machine learning. JAMA Network Open, 2018; 1(8): e186040.

21. Williamson SM, Prybutok V. Balancing Privacy and Progress: A Review of Privacy Challenges, Systemic Oversight, and Patient Perceptions in AI-Driven Healthcare. Applied Sciences. 2024; 14(2): 675.

22. Gentry C, Sahai A, Waters B. Homomorphic encryption from learning with errors: Conceptually simpler, asymptotically faster, attribute-based. Edited by Canetti R, Garay JA. Advances in Cryptology-CRYPTO 2013. Berlin: Springer; 2013. p.75-92.

23. Bocchi C, Olivi G. Regulating artificial intelligence in the EU: top 10 issues for businesses to consider. 2021. Available at: https://www.jdsupra.com/legalnews/regulating-artificial-intelligence-in-3639576/,

24. McKelvey TG, Ahmad MA, Teresesai A, Eckert C. Interpretable machine learning in healthcare. In: Proceedings of the 2018 ACM international conference on bioinformatics, computational biology and health informatics; 2018. p.559-560.

25. Powles J, Hodson H. Google DeepMind and healthcare in an age of algorithms. Health Technol. 2017; 7(4): 351-367.

26. Cuttler M. Transforming health care: How artificial intelligence is reshaping the medical landscape. CBC News. 2019. Available at: https://www.cbc.ca/news/health/artificial-intelligence-health-care1. 5110892.

27. Iacobucci G. Patient data were shared with Google on an "inappropriate legal basis", says NHS data guardian. 2017; 357: 2439.

28. Vincent J. Privacy advocates sound the alarm after Google grabs Deep-Mind UK health app. The Verge. 2018. Available at: https://www.theverge.com/2018/11/14/18094874/google-deepmind-health-app-privacy-concerns-uknhs-medical-data.

29. Jaremko J, Azar M, Bromwich R, Lum A, Cheong L, Gibert M, et al. Canadian Association of Radiologists White Paper on Ethical and Legal Issues Related to Artificial Intelligence in Radiology. Can Assoc Radiol J. 2019; 70(2): 107-118.

30. Vayena E, Blasimme A. Health research with big data: Time for systemic oversight. J Law Med Ethics. 2018; 46(1): 119-129.

31. Rock Health. Beyond wellness for the healthy: Digital health consumer adoption. 2018. Available at: https://www.rockhealth.com/reports/beyond-wellness-for-thehealthy-digital-health-consumer-adoption-2018/?mc_cid=0c97d 69dbe&mc_eid=452e95c5c5.

32. He J, Baxter SL, Xu J, Xu J, Zhou X, Zhang K. The practical implementation of artificial intelligence technologies in medicine. Nat Med. 2019; 25(1): 30-36.

33. Evans M. Hospitals give tech giants access to detailed medical records. Wall Street J. 2020. Available at: https://www.wsj.com/articles/hospitals-give-techgiants-access-to-detailed-medical-records-11579516200.

34. Verizon Enterprise. 2020 Data breach investigations report. 2020. Available at: https://www.enterprise.verizon.com/resources/reports/2020-data-breach-investigations-report.pdf.

35. Solomon H. Cost of Canadian data breaches continues to rise, says study. IT World Canada. 2018. Available at: https://www.itworldcanada.com/article/cost-ofcanadian-data-breaches-continues-to-rise-says-study/406976.

36. European Union Agency for Cybersecurity. From January 2019 to April 2020 Dta breach ENISA Threat Landscape. 2020. Available at: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2020-data-breach/at_download/fullReport.

37. Gymrek M, McGuire AL, Golan D, Halperin E, Erlich Y. Identifying personal genomes by surname inference. Science. 2013; 339(6117): 321-324.

38. Erlich Y, Shor T. Identity inference of genomic data using long-range familial searches. Science. 2018; 362(6415): 690-694.

39. Ji S, Gu Q, Weng H, Liu Q. De-health: all your online health information are belong to us. IEEE 36th International Conference on Data Engineering. 2020; 1609-1620.

40. Lubarsky B. Re-identification of "anonymized data". Georgetown law Technology Review. 2017; 1(1): 202-213.

41. Yoon J, Drumright LN, van der Schaar M. Anonymization through data synthesis using generative adversarial networks (ads-gan). IEEE J Biomed Health Inform. 2020; 24(8): 2378-2388.