Original Article **Open Access**

Health Law Journal

2024; 2: e12

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

Comparative Study of Health Data Security under GDPR and HIPAA: Challenges and Implementation Opportunities in Iran

Davoud Soltanian[1*], Abolfazl Ghahari[1]

1. Department of Law, Faculty of Law, Islamic Azad University, Tonekabon, Iran.

ABSTRACT

Background and Aim: Data security has emerged as a critical challenge in the domain of electronic health, particularly with the rising adoption of digital technologies in healthcare systems. Ensuring the confidentiality and integrity of patient health information is not only a legal obligation but also an ethical imperative, necessitating innovative approaches and the establishment of comprehensive legal frameworks. This study aims to conduct a comparative analysis between two prominent regulatory frameworks, namely the Health Insurance Portability and Accountability Act (HIPAA) in the United States and the General Data Protection Regulation (GDPR) in the European Union. The focus is on identifying the strengths and weaknesses of each regulation to provide actionable recommendations for developing a localized framework in Iran.

Methods: This qualitative and comparative study is based on content analysis of the HIPAA and GDPR regulations.

Ethical Considerations: Throughout the research, principles of originality, honesty and integrity have been strictly adhered to.

Results: The analysis revealed that HIPAA, with its emphasis on protecting medical information within the U.S. healthcare system through provisions like the Privacy Rule and Security Rule, focuses on confidentiality, security and accessibility of data. In contrast, GDPR adopts a more comprehensive approach, incorporating principles such as Privacy by Design and Data Minimization, which apply to all sectors processing personal data across the EU.

Conclusion: Despite Iran's ongoing efforts to enhance its electronic infrastructure, there are notable gaps in comprehensive health data protection laws. It is recommended that a localized legal framework inspired by the principles of both HIPAA and GDPR be developed. Such an approach could enhance data security, build public trust and improve the quality of healthcare services in Iran.

Keywords: Data Privacy; Cybersecurity; Electronic Health Records; Digital Health; Regulatory Challenges

Corresponding Author: Davoud Soltanian; **Email:** davodsoltanian@yahoo.com

Received: October 13, 2024; **Accepted:** November 27, 2024; **Published Online:** January 05, 2025

Please cite this article as:

Soltanian D, Ghahari A. Comparative Study of Health Data Security under GDPR and HIPAA: Challenges and Implementation Opportunities in Iran. Health Law Journal. 2024; 2: e12.

دسترسی آزاد | مقاله پژوهشی

مجله حقوق سلامت

دوره دوم، ۱۴۰۳

مطالعه تطبیقی امنیت داده‌های سلامت در قوانین GDPR و HIPAA؛ چالش‌ها و فرصت‌های پیاده‌سازی در ایران

داود سلطانیان[1*]، ابولفضل قهاری[1]

۱. گروه حقوق، دانشکده حقوق، دانشگاه آزاد اسلامی، تنکابن، ایران.

چکیده

زمینه و هدف: امنیت داده‌ها به عنوان یکی از چالش‌های بنیادین و حیاتی در حوزه سلامت الکترونیک مطرح است، به ویژه با افزایش استفاده از فناوری‌های دیجیتال در سیستم‌های بهداشتی. حفظ محرمانگی و یکپارچگی اطلاعات سلامت بیماران، نه‌تنها یک اولویت قانونی، بلکه یک تعهد اخلاقی است که مستلزم اتخاذ رویکردهای نوین و تدوین چهارچوب‌های قانونی جامع و دقیق است. هدف از این پژوهش، انجام یک تحلیل تطبیقی میان دو چهارچوب قانونی برجسته، یعنی HIPAA (قانون قابلیت انتقال و پاسخگویی بیمه سلامت) در ایالات متحده و GDPR (مقررات عمومی حفاظت از داده‌ها) در اتحادیه اروپا، با تمرکز بر نقاط قوت و ضعف هر یک از این قوانین برای ارائه پیشنهادات کاربردی در زمینه پیاده‌سازی یک چهارچوب بومی در ایران است.

روش: این مطالعه از نوع کیفی و تطبیقی بوده و بر اساس تحلیل محتوای قوانین HIPAA و GDPR انجام شده است.

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

یافته‌ها: تحلیل‌ها نشان داد که HIPAA با تمرکز بر حفاظت از اطلاعات پزشکی در سیستم بهداشت و درمان آمریکا، از طریق مقرراتی نظیر Privacy Rule و Security Rule، بر محرمانگی، امنیت و دسترسی‌پذیری داده‌ها تأکید دارد. در مقابل، GDPR با رویکردی جامع‌تر و با معرفی اصولی همچون Privacy by Design و Data Minimization، به تمامی بخش‌های پردازش داده‌های شخصی در سطح اتحادیه اروپا می‌پردازد.

نتیجه‌گیری: با وجود تلاش‌های ایران برای بهبود زیرساخت‌های الکترونیکی، خلأهایی در زمینه قوانین جامع حفاظت از داده‌های سلامت مشاهده می‌شود. بر این اساس، پیشنهاد می‌شود یک چهارچوب قانونی بومی با الهام از اصول HIPAA و GDPR تدوین شود. این رویکرد می‌تواند به ارتقای امنیت داده‌ها، افزایش اعتماد عمومی و بهبود کیفیت خدمات بهداشتی در ایران کمک کند.

واژگان کلیدی: حریم خصوصی داده‌ها؛ امنیت سایبری؛ پرونده الکترونیکی سلامت؛ سلامت دیجیتال؛ چالش‌های قانونگذاری

نویسنده مسئول: داود سلطانیان؛ **پست الکترونیک:** davodsoltanian@yahoo.com

تاریخ دریافت: ۱۴۰۳/۰۷/۲۲؛ **تاریخ پذیرش:** ۱۴۰۳/۰۹/۰۷؛ **تاریخ انتشار:** ۱۴۰۳/۱۰/۱۶

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

Soltanian D, Ghahari A. Comparative Study of Health Data Security under GDPR and HIPAA: Challenges and Implementation Opportunities in Iran. Health Law Journal. 2024; 2: e12.

مقدمه

سلامت الکترونیک کلیدواژه‌ای آشنا در حوزه بهداشت و درمان است که تنها چند دهه از ورود آن به نظام پزشکی کشور می‌گذرد، هرچند موضوع نسخه‌های الکترونیک، مفهوم نام آشناتر در این حوزه است، اما بد نیست بدانیم سلامت الکترونیک محدوده گسترده‌تری از موضوعات، از زیرساخت‌های پردازشی و ارتباطات الکترونیکی میان نهادهای دولتی و خصوصی گرفته تا موضوع مدیریت پلتفرم‌های سلامت‌محور را دربر می‌گیرد. در این میان پرونده‌های سلامت الکترونیکی که با داده‌های حساس بیماران سروکار دارد، در قلب این جریان قرار گرفته و نیاز به حفاظت از اطلاعات در آن به شدت احساس می‌گردد. منظور از اطلاعات بیماران در این مورد، کلیه داده‌هایی است که مربوط به تاریخچه پزشکی فرد می‌شود. این سوابق می‌تواند شامل علل بیماری، تشخیص‌ها، پیش‌بینی‌های بالینی، روش‌های درمانی و شیوه‌های پرداخت هزینه‌های خدمات بهداشتی گردد (۱). در واقع مجموعه اطلاعاتی که در گذشته به صورت دستی و در نسخ کنبی نگهداری می‌شد، امروزه در مسیر ثبت الکترونیکی قرار گرفته تا در نهایت امکان دسترسی سریع، منعطف و آسان به آن‌ها در بستر فناوری‌های سلامت‌محور میسر باشد. اطلاعاتی که به ذات ارزشمندند (۲) و جزیی از حریم خصوصی بیماران تلقی می‌شوند. در حوزه سلامت الکترونیک، این داده‌ها نقش اساسی در بهبود کیفیت مراقبت‌های بهداشتی و همچنین در تحلیل‌های کلان داده ایفا می‌کنند. با این حال، به دلیل حساسیت بالای این اطلاعات، حفاظت از آن‌ها در یک چهارچوب قانونی بسیار ضروری است تا از حریم خصوصی بیماران محافظت شود. امری که در درجه اول پای حقوق را به این میدان باز می‌کند. در واقع شاهراه ارتباطی حقوق و حوزه سلامت الکترونیک، بحث قانونگذاری و رگولاتوری است. به این صورت که قانونگذاری شفاف و جامع می‌تواند استانداردهای بالایی برای حفظ حریم خصوصی بیماران ایجاد کند و علاوه بر تسهیل عملکرد نهادهای فعال در این زمینه، از حقوق افراد در برابر نشت و نقض داده‌ها محافظت نماید. با این حال، عدم وجود چهارچوب‌های قانونی کافی و رگولاتوری‌های مؤثر در این حوزه باعث شده که موضوع امنیت داده‌های شخصی به یکی از چالش‌های اساسی در سیستم‌های سلامت الکترونیک کشور تبدیل شود.

در سطح بین‌المللی، اتحادیه اروپا و آمریکا به این نیاز با وضع قوانینی جامع واکنش نشان داده‌اند. GDPR (مقررات عمومی حفاظت از داده‌ها) در اتحادیه اروپا (۳) و HIPAA (قانون قابلیت انتقال و پاسخگویی بیمه سلامت) در ایالات متحده (۴)، دو قانون کلیدی و مرجع هستند که بر حفاظت از اطلاعات شخصی بیماران و امنیت داده‌های حساس تمرکز دارند. این قوانین با فراهم‌آوردن استانداردهای حفاظتی بالا و مشخص‌کردن مسئولیت‌های قانونی نهادهای درگیر، به طور مؤثر به مقابله با چالش‌های امنیتی داده‌ها پرداخته‌اند و در تنظیم و نظارت بر فعالیت‌های حوزه سلامت نقشی محوری داشته‌اند. یکی از موضوعات اساسی که در این دو قانون به طور خاص مورد توجه قرار گرفته است، حفظ و امنیت داده‌های شخصی بیماران است. GDPR با استانداردهای حفاظتی سفت و سخت و لزوم اخذ رضایت کاربران پیش از پردازش داده‌ها، نهادهای سلامت و سایر بازیگران این حوزه را ملزم می‌کند تا از حقوق حریم خصوصی بیماران حمایت کنند. در واقع عنصر محوری در مقررات حفاظت از داده‌های عمومی (GDPR)، رویکرد مبتنی بر ریسک است که به‌منظور مواجهه با تکنولوژی‌های نوین و خدمات پیچیده پردازش داده‌های شخصی طراحی شده است. این رویکرد به سازمان‌ها این امکان را می‌دهد که ریسک‌های مرتبط با پردازش داده‌های شخصی را شناسایی کرده و تدابیر مناسبی برای مدیریت و کاهش آن‌ها اتخاذ کنند (۵). در این فرآیند، توجه ویژه‌ای به فناوری‌های نوظهور و پیچیدگی‌های سیستم‌های خدماتی که ممکن است تهدیداتی برای حریم خصوصی افراد ایجاد کنند، معطوف می‌شود. به طور مشابه، HIPAA در آمریکا نه‌تنها حفاظت از داده‌های بهداشتی را تضمین می‌کند، بلکه الزاماتی برای مدیریت داده‌ها و حفاظت از اطلاعات بیماران ارائه می‌دهد. هدف این قانون به طور خاص تضمین این مسأله است که همزمان با تسهیل جریان اطلاعات برای ارائه خدمات

سلامت الکترونیک پیشرفته، حفاظت از این اطلاعات به طور مؤثر و مطابق با استانداردهای امنیتی به عمل آید (۶).

در کشور ما، این موضوع به عنوان یکی از چالش‌های مهم در سلامت الکترونیک شناخته شده و خلأهایی قانونی در این زمینه احساس می‌گردد (۷). چنانچه می‌توان گفت در جریان گذار از مرحله ورود فناوری اطلاعات و ارتباطات به درون صنعت پزشکی و پذیرش و بومی سازی ابعاد مختلف پزشکی هوشمند (۲۵)، موضوع درج استانداردهای جامع و یکپارچه برای حفظ حریم خصوصی افراد و امنیت داده‌ها، ما را بیش از پیش به سوی تنظیم قوانین و مقرراتی مشابه GDPR و HIPAA در حوزه حقوق داخلی سوق می‌دهد. یکی از برجسته‌ترین اقدامات در این زمینه «طرح حمایت و حفاظت از داده‌ها» بوده که با هدف صیانت از حیثیت افراد و تنظیم فعالیت‌های مرتبط با پردازش داده‌های شخصی تدوین گردیده است. این طرح که تا حدودی مشابه قانون GDPR تنظیم شده، در سال ۱۴۰۰ تقدیم مجلس و در سال ۱۴۰۲ اعلام وصول گردید. مجموعه‌ای که می‌توان از آن به عنوان چهارچوبی ملی در راستای صیانت از داده‌های شخصی افراد نام برد و هم قدم با بازیگران بین‌المللی برای ارتقای سیستم سلامت الکترونیک حرکت کرد. طبیعی است که قانونگذاری‌هایی اینچنینی، بیش از هر چیز نیاز به کنجکاوی و تعقیب فعالیت‌های بین‌المللی دارد، لذا بر این اساس در مقاله حاضر تلاش می‌گردد ضمن تحلیل موقعیت حقوقی اطلاعات در حوزه سلامت الکترونیک، با استناد به دو قانون GDPR و HIPAA، راهکارهای پیش‌بینی‌شده برای حفاظت از اطلاعات مورد بررسی قرار گیرد و در نهایت به امکان‌سنجی اجرای آن در سیستم حقوق داخلی پرداخته شود.

ملاحظات اخلاقی

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

روش

این پژوهش از نوع توصیفی ـ تحلیلی بوده و با رویکرد کیفی و تطبیقی به بررسی قوانین مرتبط با حفاظت از داده‌های سلامت الکترونیک پرداخته است. به طور خاص، این مطالعه به تحلیل تطبیقی دو چهارچوب قانونی HIPAA (قانون قابلیت حمل و پاسخگویی بیمه سلامت) در ایالات متحده و GDPR (مقررات عمومی حفاظت از داده‌ها) در اتحادیه اروپا می‌پردازد. هدف اصلی این مقاله، شناسایی و بررسی شباهت‌ها و تفاوت‌های این دو قانون در راستای حفاظت از داده‌های سلامت بیماران است. در ادامه، نقاط قوت کلیدی هر دو چهارچوب استخراج شده و پیشنهاداتی برای طراحی یک مدل بهینه در زمینه حفاظت از داده‌های سلامت الکترونیک در ایران ارائه می‌شود. این رویکرد می‌تواند به تقویت سیاست‌های حفاظت از حریم خصوصی و امنیت اطلاعات در نظام سلامت الکترونیک کشور کمک کند.

یافته‌ها

مقایسه قوانین HIPAA و GDPR نشان می‌دهد که هر دو قانون به طور مؤثر به حفاظت از داده‌های سلامت الکترونیک توجه دارند، اما تفاوت‌های قابل توجهی در الزامات قانونی و رویکردهای اجرایی آن‌ها وجود دارد. HIPAA تمرکز ویژه‌ای بر حفاظت از اطلاعات سلامت در سیستم بهداشت و درمان ایالات متحده دارد و بیشتر به حوزه‌های مرتبط با ارائه‌دهندگان خدمات سلامت محدود می‌شود. از سوی دیگر، GDPR رویکرد جامع‌تری اتخاذ کرده و تمامی داده‌های شخصی در تمامی بخش‌ها، از جمله بخش سلامت، را تحت پوشش قرار می‌دهد. این قانون اصولی نظیر Privacy by Design و Data Minimization را برای اطمینان از حفظ حریم خصوصی افراد معرفی می‌کند.

در مورد وضعیت ایران، بررسی‌ها نشان می‌دهد که علی‌رغم تلاش‌های صورت‌گرفته برای توسعه زیرساخت‌های الکترونیکی، از جمله تصویب مصوبه شماره ۱۲۱۷۶/ت۵۵۲۸۵هـ مورخ ۹ اردیبهشت ۱۳۹۷ هیأت وزیران و تقدیم طرح حمایت و

حفاظت از داده‌ها در سال ۱۴۰۰ به مجلس، هنوز خلأهای قانونی و اجرایی در زمینه حفاظت از داده‌های سلامت وجود دارد. این خلأها شامل نبود استانداردهای جامع و عدم انطباق کامل با استانداردهای بین‌المللی است. همچنین یکی از چالش‌های اساسی در ایران، کمبود آموزش و فرهنگ‌سازی در حوزه امنیت داده‌هاست که به عنوان مانعی برای اجرای مؤثر قوانین حفاظتی شناخته شده است. بنابراین بازنگری در سیاست‌ها، تقویت آموزش‌های مرتبط و ایجاد چهارچوب‌های قانونی جامع‌تر، ضروری به نظر می‌رسد.

بحث

۱. تاریخچه امنیت داده در سلامت الکترونیک و تصویب قوانین GDPR و HIPAA: با توسعه فناوری اطلاعات و افزایش دیجیتالی‌سازی داده‌های پزشکی، نیاز به حفاظت از اطلاعات حساس بیماران به شدت افزایش یافت. تا دهه ۱۹۹۰ میلادی، بیشتر داده‌های بیماران به صورت کاغذی ذخیره می‌شد و دسترسی و به اشتراک‌گذاری آن‌ها نیازمند طی مراحل متعدد و کاغذبازی‌های اداری بود (۸). با ظهور سیستم‌های سلامت الکترونیک، پرونده‌های سلامت به شکل دیجیتالی نگهداری شدند که این موضوع باعث افزایش دسترسی، سرعت و کارایی در ارائه خدمات شد، اما همزمان با این تغییر، نگرانی‌های مربوط به امنیت و حریم خصوصی داده‌ها نیز شدت گرفت (۹).

در پاسخ به این نیاز، قانون قابلیت انتقال و پاسخگویی بیمه سلامت (HIPAA) در سال ۱۹۹۶ در آمریکا به تصویب رسید. این قانون با هدف حفاظت از اطلاعات بهداشتی و افزایش امنیت داده‌های سلامت، شامل دو بخش اساسی بود: یکی قواعد حفظ حریم خصوصی (Privacy Rule) و دیگری قواعد امنیتی (Security Rule) (۱۰). این دو بخش با تعیین الزامات و استانداردهای لازم برای نهادهای ارائه‌دهنده خدمات سلامت و مسئولیت‌های قانونی آن‌ها، کنترل و امنیت داده‌های بیماران را تضمین می‌کنند. قوانین حریم خصوصی HIPAA تمامی نهادها و افراد فعال در حوزه سلامت را ملزم می‌کند که داده‌های بیماران را به طور محرمانه نگه دارند و دسترسی به این اطلاعات را محدود کنند. قوانین امنیتی HIPAA نیز شامل دستورالعمل‌های دقیقی برای نحوه نگهداری، دسترسی و انتقال امن داده‌ها می‌شود و از سازمان‌ها می‌خواهد تا پروتکل‌های امنیتی مناسبی برای جلوگیری از دسترسی غیر مجاز اتخاذ کنند. HIPAA همچنین مفاهیم حقوقی جدیدی نظیر انتقال امن اطلاعات و رضایت‌گیری را به قوانین بهداشت آمریکا معرفی کرد (۱۱) و باعث شد تا آمریکا به یکی از پیشروهای حوزه امنیت داده‌های بهداشتی تبدیل شود.

در اروپا، نیاز به یک قانون جامع و هماهنگ در حوزه امنیت داده‌ها و حریم خصوصی با رشد روزافزون دیجیتالی‌سازی اطلاعات و توسعه خدمات آنلاین بیش از پیش حس شد. در سال ۲۰۱۸، مقررات عمومی حفاظت از داده‌ها (GDPR) در اتحادیه اروپا به اجرا درآمد (۴). GDPR با هدف اصلی محافظت از داده‌های شخصی تمامی شهروندان اتحادیه اروپا، استانداردهای امنیتی و الزامات دقیقی برای هر سازمانی که با داده‌های کاربران اروپایی کار می‌کند، تعیین کرد. برخلاف HIPAA که مخصوص داده‌های سلامت است، GDPR تمامی داده‌های شخصی، از جمله داده‌های سلامت را پوشش می‌دهد و سازمان‌ها را ملزم به رعایت اصولی چون رضایت صریح کاربران و حق فراموشی می‌کند (۱۲). از ویژگی‌های برجسته GDPR می‌توان به موارد زیر اشاره کرد:

ـ حق دسترسی و کنترل کاربران بر داده‌های خود (۱۳): افراد حق دارند بدانند که چه اطلاعاتی از آن‌ها جمع‌آوری شده و از سازمان‌ها بخواهند که این داده‌ها را حذف یا به‌روزرسانی کنند.

ـ الزامات امنیتی شدید برای پردازش داده‌ها (۱۴): سازمان‌ها موظف‌اند تا برای امنیت داده‌ها، تدابیر مناسبی مثل رمزنگاری و استفاده از فناوری‌های امن اتخاذ کنند.

ـ اعمال جریمه‌های سنگین برای تخلفات (۱۵): یکی از مهم‌ترین خصوصیات GDPR اعمال جریمه‌های سنگین مالی برای سازمان‌هایی است که مقررات را نقض می‌کنند.

در مقام مقایسه HIPAA و GDPR در حوزه سلامت الکترونیک باید گفت هر دو قانون GDPR و HIPAA بر

حفاظت از داده‌های شخصی، به ویژه در حوزه سلامت، تأکید دارند. HIPAA محدود به آمریکا و تنها در مورد داده‌های سلامت کاربرد دارد، اما GDPR تمامی سازمان‌های بین‌المللی را که به داده‌های شهروندان اتحادیه اروپا دسترسی دارند، دربر می‌گیرد و دامنه وسیع‌تری دارد. هر دو قانون، ایجاد استانداردهای امنیتی، نظارت دقیق و تعیین مسئولیت‌های قانونی برای نهادها را ضروری می‌دانند، اما GDPR به دلیل گستره بین‌المللی و جامعیت بیشتر، تأثیر عمیق‌تری بر سیاست‌های امنیت داده در سطح جهانی داشته است.

در حقوق ایران، تاکنون مقررات منسجم و جامعی برای حمایت از حریم خصوصی و داده‌های شخصی تبیین و تصویب نشده است. توضیح اینکه در بدنه کارشناسی حقوق فناوری اطلاعات، مقررات عمومی حفاظت از داده شخصی در حوزه هوش مصنوعی قرار می‌گیرد (۲۸)، البته چهارچوب‌های کلی آن را باید در قانون مجازات اسلامی و قانون تجارت الکترونیک جستجو کرد. همچنین می‌توان با مراجعه به قانون اساسی کشور و وامداری از اصول کلی موجود به بسترهایی در این زمینه دست یافت، چنانچه در اصل ۲۲ قانون اساسی می‌خوانیم: «بازرسی و نرساندن نامه‌ها، ضبط و فاش‌کردن مکالمات تلفنی، افشای مخابرات تلگرافی و تلکس، سانسور، عدم مخابره و نرساندن آن‌ها، استراق سمع و هرگونه تجسس ممنوع است، مگر به حکم قانون» (۲۶). این اصل صراحتاً عمده مصادیق داده‌های شخصی افراد را مصون می‌دارد. در واقع در حقوق موضوعه ایران، حفاظت از داده‌های شخصی و حریم خصوصی دو اصطلاح مترادف هستند و به جای هم به کار می‌روند (برخلاف حقوق اتحادیه اروپا)، لذا در قوانین و مقرراتی که برای حمایت از داده‌های شخصی قابل استناد است، اصطلاح حریم خصوص یا حریم خصوصی اطلاعاتی نیز در خصوص داده‌های شخصی به کار رفته است (۲۷)، اما همانطور که گفته شد، این اشارات کافی نیست و بستر سلامت الکترونیک نیاز به قوانینی روشن‌تر دارد تا بتواند همسو با رشد فناوری در حوزه پزشکی، ابعاد حقوقی فعالیت‌های مرتبط را تحت پوشش قرار دهد. در این زمینه، هرچند طرح حمایت از داده‌های شخصی تنظیم و تقدیم مجلس شده، اما این طرح نیز صرف نظر اینکه هنوز به تصویب نرسیده، دارای ایرادات مشخصی است. برای مثال ما حمایتی از خسارت‌های معنوی در این بستر مشاهده نمی‌کنیم و حذف داده‌ها نه‌تنها الزامی نیست، بلکه کنترلگران را تا ۱۸ ماه موظف به نگهداری داده‌ها می‌داند. موضوعاتی مانند رضایت و موقعیت داده از جهت مال تلقی‌شدن نیز در این طرح مورد بحث است (۳۰) و ابهام آن زنگ خطری برای جامع و مانع‌بودن این قانون خواهد بود. این موضوعات و موارد مشابه نیاز به تحقیق، تطبیق و شناسایی کارکرد و پیامدهای سیاست‌های بین‌المللی در این زمینه را بیش از پیش ضروری می‌نماید.

۲. تعریف و بررسی امنیت داده در سلامت الکترونیک:

امنیت داده در سلامت الکترونیک شامل مجموعه‌ای از استانداردها، اقدامات حفاظتی و چهارچوب‌های قانونی است که به منظور حفاظت از اطلاعات سلامت الکترونیکی (EHR) و اطلاعات بهداشتی محافظت‌شده (PHI) از دسترسی، تغییر یا نشت غیر مجاز، تعریف شده‌اند. در این حوزه، حریم خصوصی و محرمانگی اطلاعات بیماران اصلی‌ترین دغدغه‌ها محسوب می‌شوند، چراکه اطلاعات سلامت شامل داده‌های حساس فردی و طبی است که افشا یا دستکاری آن‌ها می‌تواند اثرات جبران‌ناپذیری بر حقوق افراد بگذارد (۱۶). در ایالات متحده، قانون HIPAA به عنوان پایه‌ای برای امنیت داده‌های سلامت الکترونیک عمل می‌کند. قوانین حریم خصوصی HIPAA، استفاده و اشتراک‌گذاری داده‌های سلامت را محدود می‌کنند و استانداردهای دقیقی برای کنترل دسترسی و رمزگذاری اطلاعات تعیین می‌کنند. برای مثال در ماده 45 CFR § 164.502 ضمن اشاره به به محدودیت‌های دسترسی و افشای اطلاعات بهداشتی محافظت‌شده، نهادهای بهداشتی موظف به محافظت از حریم خصوصی افراد و محدودکردن اشتراک‌گذاری داده‌ها می‌گردند یا بر اساس ماده 45 CFR § 164.306 می‌بایست با استفاده از اقدامات امنیتی «اداری، فیزیکی و فنی» از داده‌ها محافظت کنند که شامل مجموعه‌ای از فعالیت‌ها از کنترل‌های دسترسی گرفته تا رمزگذاری برای حفظ امنیت و

محرمانگی داده‌های سلامت می‌شود. از سوی دیگر بر اساس ماده 45 CFR § 164.400-414 سازمان‌ها موظف می‌شوند در صورت نقض داده‌ها، سریعا به افراد آسیب‌دیده اطلاع دهند و اقدامات فوری برای کاهش تأثیر نقض داده‌ها را انجام دهند (۱۷).

از طرف دیگر، GDPR (مقررات عمومی حفاظت از داده‌ها) که در اتحادیه اروپا اجرایی شده است، نیز چهارچوبی جامع و الزامی جدی برای حفاظت از داده‌های شخصی فراهم کرده و شامل معیارهایی چون اصل کاهش داده، اصل پاسخگویی و حق دسترسی داده برای افراد است. بنا بر ماده ۳۲ این قانون تمام کنترل‌کنندگان داده موظفند با توجه به «ماهیت، گستره، زمینه و هدف پردازش»، تدابیر حفاظتی مناسبی اتخاذ کنند. استفاده از رمزگذاری (Encryption)، یکپارچگی داده‌ها و بازیابی به موقع اطلاعات نیز از این الزامات است. از سوی دیگر ماده ۳۵ فعالان فوق را ملزم به ارزیابی تدابیر به کار رفته و تأثیر آن بر حریم خصوصی مخاطبین می‌نماید. این امر در حوزه سلامت الکترونیک بسیار حیاتی است و هدف آن کاهش ریسک ناشی از دسترسی غیر مجاز به داده‌ها جلوگیری تعریف می‌شود. و در نهایت ماده ۳۷ برای نهادهای بزرگ‌تر یا آن دسته از سازمان‌هایی که حجم زیادی از اطلاعات حساس را پردازش می‌کنند، تعیین یک شخص به عنوان «مسئول حفاظت از داده‌ها» را الزامی می‌داند. این فرد به طور خاص وظیفه نظارت بر پایبندی به مقررات و اطمینان از امنیت داده‌ها را بر عهده دارد (۱۸).

در کنار مطالب فوق باید اشاره گردد که امنیت داده‌ها در سلامت الکترونیک تحت تأثیر فناوری‌های جدید نظیر رایانش ابری و هوش مصنوعی است (۱۶). این فناوری‌ها امکان بهبود دسترسی و پردازش سریع داده‌های پزشکی را فراهم کرده‌اند، اما در عین حال، چالش‌های امنیتی جدیدی نیز ایجاد می‌کنند. به همین دلیل، کشورها و سازمان‌های بین‌المللی در حال بازنگری مداوم قوانین هستند تا بتوانند همراه با پیشرفت فناوری، حفاظت از داده‌های حساس را تضمین کنند (۳).

در خصوص کشور ایران در ضمن اشاره به اهمیت داده‌های شخصی و دغدغه حفاظت از آن‌ها در بستر مبادلات اطلاعات پزشکی که بروز آن را می‌توان در موادی مثل ماده ۶ منشور حقوق بیمار ایران مصوب ۱۳۸۰ وزارت بهداشت و درمان و آموزش پزشکی به خوبی مشاهده کرد که مقرر می‌دارد: «بیمار حق دارد جهت حفظ حریم شخصی خود، از محرمانه‌ماندن محتوای پرونده پزشکی، نتایج معاینات و مشاوره‌های بالینی جز در مواردی که بر اساس وظایف قانونی از گروه معالج اعلام صورت می‌گیرد، اطمینان حاصل نماید» (۲۴)، در مقام مقایسه GDPR و HIPAA باید گفت بسیاری از اصول و روش‌های مطرح‌شده در این دو قانون می‌توانند به عنوان الگوهای مؤثری برای تدوین چهارچوب قانونی به کار روند. در حال حاضر، خلأ قوانین جامع در زمینه امنیت داده‌های سلامت، به ویژه در حوزه دیجیتال، نیازمند توجه ویژه قانونگذار است. استفاده از اصول «کاهش داده»، «رمزگذاری» و «تخصیص مسئول حفاظت از داده‌ها» می‌تواند برای رفع چالش‌های امنیتی و حفاظت از اطلاعات سلامت در ایران نقش مؤثری داشته باشد.

۳. مطالعه تطبیقی امنیت داده‌ها در HIPAA و GDPR:

برای بررسی تطبیقی امنیت داده‌ها در دو قانون فوق، ما به ترتیب به تحلیل سه موضوع اصلی می‌پردازیم: نکات کلیدی و مشترک، تفاوت‌ها و ویژگی‌های منحصر به فرد و در نهایت مزایا و معایب هرقانون در موضوع حفاظت از داده‌های سلامت.

۳-۱. نکات مشترک: هر دو قانون HIPAA و GDPR با هدف حفاظت از اطلاعات حساس طراحی شده‌اند و شامل مقرراتی برای محافظت از حریم خصوصی افراد هستند. برخی از نکات مشترک عبارتند از:

۳-۱-۱. حفاظت از داده‌های حساس: هر دو قانون تمرکز ویژه‌ای بر حفاظت از داده‌های حساس دارند HIPAA اطلاعات بهداشتی محافظت‌شده Protected Health Information یا PHI را پوشش می‌دهد (۹)، در حالی که GDPR حفاظت از «داده‌های شخصی (Personal Data)» شامل داده‌های بهداشتی را تضمین می‌کند (۱۶).

۳-۱-۲. حقوق افراد: هر دو قانون حقوقی را برای افراد در نظر گرفته‌اند که به آن‌ها اجازه می‌دهد به داده‌های خود

دسترسی داشته باشند، درخواست اصلاح داده‌ها را داشته باشند و در مواردی درخواست حذف داده‌ها کنند (۱۴).

۳-۱-۳. گزارش‌دهی نقض داده‌ها: هر دو قانون مقرراتی برای گزارش‌دهی در صورت نقض امنیت داده‌ها وضع کرده‌اند (۱۳). HIPAA ملزم می‌کند که سازمان‌ها نقض PHI را به افراد آسیب‌دیده و دولت اطلاع دهند، در حالی که GDPR محدودیت‌های سخت‌تری برای گزارش‌دهی سریع در عرض ۷۲ ساعت تعیین کرده است (۱۴).

۳-۲. تفاوت‌ها و ویژگی‌های منحصر به فرد هر قانون

۳-۲-۱. حوزه اجرا و پوشش: قانون HIPAA تنها در آمریکا اعمال می‌شود و مختص سازمان‌های بهداشتی، بیمه‌ها و شرکای تجاری آن‌ها است. محدوده آن بیشتر به PHI در سیستم‌های بهداشتی و درمانی آمریکا محدود می‌شود، در حالی که قانون GDPR در سراسر اتحادیه اروپا اعمال می‌شود و شامل هر سازمانی است که داده‌های شخصی افراد در این منطقه را پردازش می‌کند، حتی اگر خود سازمان در خارج از اروپا قرار داشته باشد (۱۹).

۳-۲-۲. مبنای قانونی برای پردازش داده‌ها: بنا بر قانون HIPAA پردازش داده‌های سلامت تنها در شرایط خاصی مجاز است، مانند اهداف درمانی، پرداخت‌ها و عملیات مراقبت‌های بهداشتی. همچنین، دریافت رضایت بیمار برای بسیاری از موارد ضروری نیست. در قانون GDPR این موضوع کمی متفاوت است و پردازش داده‌ها بر اساس یکی از شش مبنای قانونی صورت می‌گیرد، از جمله «رضایت فرد»، «اجرای قرارداد»، «تعهدات قانونی» و... . برای داده‌های بهداشتی، GDPR معمولاً به رضایت صریح فرد نیاز دارد. در همین راستا می‌توان به پرونده معروف Schrems II case در سال ۲۰۲۰ اشاره کرد که در نهایت دادگاه بعد از مقایسه و اعتبارسنجی سپر محافظتی دو قانون فوق مقرر نمود، قانون ایالات متحده به قدرت و استحکام قانون اروپا نیست و در نتیجه انتقال داده‌ها از اروپا به آمریکا نیازمند تضمین‌های امنیتی دیگر معادل GDPR است (۲۰).

۳-۲-۳. حق فراموش‌شدن: در HIPAA چنین حقی به طور مستقیم وجود ندارد، اما بیماران می‌توانند درخواست کنند که دسترسی به داده‌هایشان محدود شود، اما GDPR به افراد حق می‌دهد که درخواست حذف دائمی داده‌های خود را از سیستم‌ها داشته باشند، مگر در شرایطی که نگهداری داده‌ها برای اهداف قانونی لازم باشد (۲۱).

۳-۳. مزایا و معایب هر قانون در حفاظت از داده‌های سلامت: با نگاهی تخصصی می‌توان مزایای زیر را برای HIPAA برشمرد:

۳-۳-۱. تخصصی‌بودن: تمرکز آن بر بخش سلامت باعث می‌شود مقررات آن به صورت ویژه برای اطلاعات بهداشتی تنظیم شده باشند.

۳-۳-۲. استانداردهای امنیتی مشخص: شامل الزامات خاص برای امنیت فیزیکی، اداری و فنی داده‌های سلامت است. چنانچه در ارزیابی تطبیقی صورت‌گرفته در مورد HIPAA و قوانین دیگر مانند استاندارد ISO 27799:2008 و PCI-DSS مشخص گردید این قانون یکی از قوی‌ترین استراتژی‌ها در زمینه امنیت سیستم عامل را دارد (۲۹). همچنین مزایایی به شرح زیر برای GDPR متصور است.

۳-۳-۳. سترگی و جامعیت: ـ پوشش گسترده‌ای برای حفاظت از داده‌ها در تمامی صنایع دارد، نه‌فقط بخش سلامت؛ ـ حقوق گسترده‌تر برای افراد: ارائه حقوقی مانند حق فراموش‌شدن، حق اعتراض به پردازش داده‌ها و حق انتقال داده‌ها Data Portability.

۳-۳-۴. جریمه‌های سنگین: اعمال جریمه‌های شدید برای تخلفات که انگیزه‌ای قوی برای پایبندی به قوانین ایجاد می‌کند.

البته معایب زیر نیز مشاهده می‌شود: معایب HIPAA:

۳-۳-۵. محدودیت جغرافیایی: تنها در آمریکا معتبر است و برای شرکت‌های بین‌المللی که در چندین منطقه فعالیت می‌کنند، چالش‌برانگیز است.

۳-۳-۶. عدم انعطاف‌پذیری: در مقایسه با GDPR، محدودیت‌های بیشتری در نحوه پردازش داده‌ها دارد.

و همچنین معایب GDPR که عبارتند از:

۳-۳-۷. پیچیدگی در پیاده‌سازی: برای شرکت‌های کوچک و متوسط، رعایت تمامی الزامات GDPR می‌تواند دشوار و پرهزینه باشد.

۳-۳-۸. نیاز به رضایت صریح: برای پردازش داده‌های بهداشتی، نیاز به رضایت صریح ممکن است مانع دسترسی به داده‌ها در موارد اضطراری شود.

۳-۳-۹. عدم پیش بینی برخی استانداردها: رمزنگاری کامل اطلاعات دارای ۴ ویژگی است: استفاده از فناوری‌های رمزگذاری در ذخیره‌سازی، استفاده از الگوریتم‌های Hash در برنامه‌های کاربردی، امضای دیجیتال و رمزنگاری با کلیدهای نامتقارن. با بررسی و کنجکاوی در قانون HIPAA، این نتیجه حاصل می‌شود که این قانون صرفاً به دو مورد از این استانداردها، یعنی فناوری‌های رمزگذاری در ذخیره‌سازی و رمزنگاری با کلیدهای نامتقارن پرداخته و جای دو ویژگی و استاندارد بعدی در آن خالی است (۲۹).

در نتیجه این بحث می‌توان گفت در حالی که HIPAA به عنوان استانداردی طلایی برای حفاظت از داده‌های سلامت در آمریکا شناخته می‌شود، GDPR با رویکرد جامع‌تری به حفاظت از داده‌ها در سطح بین‌المللی پرداخته است. استفاده از این قوانین به عنوان چهارچوبی برای توسعه قوانین مشابه در کشورهای دیگر، به ویژه در ایران، می‌تواند به بهبود حفاظت از داده‌های بهداشتی و سلامت الکترونیک کمک کند.

۴. پیشنهادات و راه حل‌های امنیتی برای پیاده‌سازی در ایران:

برای ارائه پیشنهادات و راه حل‌های امنیتی جهت پیاده‌سازی در حوزه سلامت الکترونیک ایران با توجه به قوانین GDPR و HIPAA، باید چندین جنبه کلیدی را در نظر گرفت. این پیشنهادات باید بر مبنای الزامات قانونی و نیازهای بومی کشور تنظیم شوند تا علاوه بر تأمین امنیت داده‌ها، به بهبود کیفیت خدمات سلامت الکترونیک نیز کمک کنند. در ادامه، به بررسی این راهکارها و تطابق آن‌ها با زیرساخت‌های فعلی ایران می‌پردازیم.

۴-۱. ایجاد چهارچوب قانونی جامع برای حفاظت از داده‌های سلامت: تردیدی نیست که ایران نیازمند یک چهارچوب قانونی مشخص مشابه GDPR و HIPAA است. مستندی که به صورت جامع به حفاظت از داده‌های شخصی و به ویژه داده‌های سلامت بپردازد و اصولی مانند اصل رضایت صریح بیمار یا حق دسترسی، اصلاح و حذف دادها در آن به دقت مورد بررسی قرار گیرد. این چهارچوب می‌تواند با استفاده از تجربیات موفق سایر کشورها توسعه یابد (۱۸).

۴-۲. پیاده‌سازی استانداردهای امنیتی و فنی: یکی دیگر از پیشنهادات، به کارگیری تدابیر فنی و پروتکل‌های امنیتی است. برای مثال استفاده از روش‌هایی مانند رمزنگاری داده‌ها (Encryption)، احراز هویت دومرحله‌ای (Two-Factor Authentication) و کنترل دسترسی‌های مبتنی بر نقش (Role-Based Access Control) می‌تواند به طور قابل توجهی سطح امنیت سیستم‌های سلامت الکترونیک را ارتقا دهد، کمااینکه در این خصوص مشاهده می‌کنیم به ترتیب مواد ۳۲ قانون GDPR و ماده 164.31245 § CFR قانون HIPAA سازمان‌ها را موظف به اتخاذ تدابیر فنی مناسب برای حفاظت از داده‌ها می‌کنند (۱۷).

۴-۳. آموزش و توانمندسازی کارکنان حوزه سلامت: تجربه نشان داده بسیاری از نقض‌های امنیتی ناشی از خطاهای انسانی هستند. بنابراین آموزش دقیق، رایگان و مستمر کارکنان حوزه سلامت در مورد حفاظت از داده‌ها و آگاهی از تهدیدات امنیتی امری ضروری است. این دوره‌ها می‌تواند با تمرکز بر نحوه مدیریت داده‌های حساس باشد. امری که می‌تواند در دراز مدت ضمن حفاظت از داده‌ها، هزینه فعالیت در این حوزه را کاهش دهد. طبق ماده § CFR 164.30845 در HIPAA سازمان موظف به ارائه آموزش‌های منظم به کارکنان خود هستند.

۴-۴. استفاده از ارزیابی‌های امنیتی و ممیزی منظم: باید توجه داشت که انجام ارزیابی‌های ریسک و ممیزی‌های دوره‌ای برای شناسایی و کاهش آسیب‌پذیری‌های احتمالی ضروری است. طبق ماده ۲۴ GDPR سازمان‌ها موظف به

انجام ارزیابی‌های امنیتی و پیاده‌سازی تدابیر پیشگیرانه هستند. در این خصوص پیشنهاد می‌شود از خدمات شرکت‌های متخصص در زمینه امنیت سایبری برای انجام Penetration Testing و ارزیابی‌های امنیتی استفاده شود.

۴-۵. ایجاد سیستم‌های گزارش‌دهی نقض داده‌ها: ایجاد مکانیزم‌های سریع و کارآمد برای گزارش‌دهی نقض داده‌ها به مراجع ذی‌صلاح و اطلاع‌رسانی به بیماران از دیگر پیشنهاداتی است که در این زمینه مطرح می‌گردد. همانطور که پیش از این گفته شد، بر اساس ماده ۳۳ قانون GDPR سازمان‌ها ظرف ۷۲ ساعت ملزم به اطلاع رسانی نقض داده به بیمار هستند. در کشور ما این امر می‌تواند از طریق طراحی پورتالی خاص برای گزارش‌دهی آن لاین یا پیگیری نقض داده‌ها ورود نماید.

۴-۶. حفظ حریم خصوصی در پلتفرم‌های سلامت‌محور: به نظر می‌رسد بسیاری از پلتفرم‌های سلامت‌محور در ایران نیاز به بازنگری و ارتقای تدابیر امنیتی دارند و باید اطمینان از Privacy by Design و Privacy by Default در توسعه نرم‌افزارها باید به عنوان یک اولویت برای ایشان در نظر گرفته شود. در این خصوص، به نظر می‌رسد همکاری نزدیک بین توسعه‌دهندگان نرم‌افزار و متخصصان حقوقی برای طراحی سیستمی که از ابتدا با اصول حریم خصوصی مطابقت داشته باشد، می‌تواند پاسخگو باشد.

در انتها و پس از اشاره به آخرین پیشنهاد باید گفت در خصوص ظرفیت حقوقی پیاده‌سازی ابزارهای فوق در سیستم داخلی کشور، مسیر، خالی و تهی از دستاورد و روشنایی نیست. چنانچه علاوه بر وجود سیستم‌های تنبیهی، مانند ماده ۶۴۸ قانون مجازات اسلامی که دربردارنده مسئولیت کیفری خاطیان و همچنین ماده ۴ آیین‌نامه انتظامی رسیدگی به تخلفات صنفی و حرفه‌ای شاغلین حرفه‌های پزشکی در سازمان نظام پزشکی جمهوری اسلامی ایران موضوع ماده ۲ و مواد ۲۴ و ۴۳ قانون سازمان نظام پزشکی مصوب ۱۳۸۳ که با رویکرد تنبیهی حاوی مسئولیت انتظامی ناقضان حریم اطلاعات است (۲۴)، می‌توان به سیاست‌های کشور برای دیجیتالی‌سازی خدمات سلامت را در برنامه‌های پنجم و ششم توسعه اشاره نمود. ماده ۷۴ قانون برنامه ششم در این مورد به طور خاص به توسعه سیستم‌های سلامت الکترونیک اشاره می‌کند (۲۲). این ماده دولت را ملزم می‌نماید طی یک دوره دو ساله سیستم پرونده الکترونیک سلامت را برای تمامی شهروندان ایجاد و آن را با سیستم‌های بیمه سلامت ادغام کند. همچنین مشاهده می‌شود که در بخشنامه‌ها و تصمیمات متعدد مانند مصوبات هیأت وزیران و جلسات شورای عالی سلامت و امنیت غذایی، بر ضرورت توسعه زیرساخت‌های الکترونیک در نظام سلامت تأکید شده است. به عنوان مثال، مصوبه شماره ۱۲۱۷۶/ت۵۵۲۸۵هـ مورخ ۹ اردیبهشت ۱۳۹۷ هیأت وزیران که در زمینه تقویت زیرساخت‌های سامانه‌های الکترونیکی مرتبط با معاملات دولتی است و سلامت الکترونیک را به عنوان یکی از پروژه‌های اولویت‌دار دولت در نظر گرفته است (۲۳). از سوی دیگر قانون حمایت از حقوق مصرف‌کننده و قانون جرایم رایانه‌ای به عنوان دو قانون موجود در سیستم حقوقی کشور جوابگوی برخی از نیازها در این زمینه هستند. همچنین مشاهده می‌شود با توجه به استفاده گسترده از سیستم‌های سلامت الکترونیک (EHR)، پلتفرم‌های مختلفی در ایران شروع به توسعه زیرساخت‌های دیجیتال و اقدامات امنیتی کرده‌اند، از جمله این اقدامات می‌توان به سامانه‌های ملی مانند سامانه سپاس (سامانه پرونده الکترونیک سلامت) و نسخه‌نویسی الکترونیکی اشاره کرد که در راستای ایجاد پرونده‌های الکترونیک سلامت و تجمیع داده‌های بیماران فعالیت می‌کنند. علاوه بر آن برخی پلتفرم‌های ایرانی مانند دکترنکست و اسنپ دکتر نیز سعی کرده‌اند با ارائه خدمات سلامت آنلاین، اطلاعات بیماران را به شکل امن‌تری مدیریت کنند. این پلتفرم‌ها از پروتکل‌های امنیتی برای حفاظت از داده‌های کاربران بهره می‌برند. از سوی دیگر در بستر تحلیل حقوقی و استمداد از اصول و مبانی برای استنباط حکم، چهارچوب‌هایی مانند مال‌انگاشتن داده‌ها و ورود از درگاه حقوق اموال، بحث الزامات قراردادی و قاعده «اذن در شئ اذن در لوازم آن» و همچنین تعارض قانون اهم و مهم از

سوی نویسندگان مطرح شده که می‌تواند پاسخی بومی برای خلأهای قانونی موجود باشد (۲۷)، لذا در مجموع تلاش‌های متعددی برای حرکت در ریل سلامت الکترونیک صورت گرفته است و قطعاً مشاهده و بهره‌گیری از تجارب جهانی می‌تواند در این زمینه بسیار کمک‌کننده و تسریع‌بخش باشد.

نتیجه‌گیری

با توجه به تحلیل‌های انجام‌شده پیرامون امنیت داده‌ها در حوزه سلامت الکترونیک و مقایسه قوانین HIPAA و GDPR، می‌توان نتیجه گرفت که این دو قانون به عنوان استانداردهای بین‌المللی در زمینه حفاظت از داده‌های سلامت، چهارچوب‌های جامع و مؤثری را برای تضمین امنیت اطلاعات بیماران ارائه می‌دهند. HIPAA به طور ویژه بر حفاظت از اطلاعات پزشکی در سیستم بهداشت و درمان ایالات متحده تمرکز دارد و از طریق مقرراتی نظیر Privacy Rule (45 CFR § 164.500) و Security Rule (45 CFR § 164.302) تلاش می‌کند تا محرمانگی، یکپارچگی و در دسترس‌بودن اطلاعات سلامت را تضمین کند. از سوی دیگر، GDPR در اتحادیه اروپا رویکردی جامع‌تر دارد که نه‌تنها به داده‌های حوزه سلامت، بلکه به کلیه داده‌های شخصی افراد نیز می‌پردازد. مقررات کلیدی مانند ماده ۳۲ (امنیت پردازش) و ماده ۹ (پردازش داده‌های حساس) اصول پیشرفته‌ای نظیر Privacy by Design و Data Minimization را معرفی کرده‌اند که نه‌تنها محدود به بخش سلامت نیستند، بلکه در تمامی بخش‌های اقتصادی و اجتماعی کاربرد دارند. با وجود اینکه ایران در سال‌های اخیر تلاش‌های مثبتی برای تقویت امنیت داده‌ها در بستر سلامت الکترونیک داشته، همچنان نیاز به توسعه قوانین جامع‌تری در این زمینه احساس می‌شود. تصویب‌نامه شماره ۱۲۱۷۶/ت۵۵۲۸۵هـ مورخ ۹ اردیبهشت ۱۳۹۷ هیأت وزیران تلاش کرده است تا زیرساخت‌های الکترونیکی و شفافیت در فرآیندها را بهبود بخشد یا طرح حمایت و حفاظت از داده‌های شخصی که در سال ۱۴۰۰ به مجلس تقدیم گردیده و در همین مرحله تحت نگاه تیزبین اساتید حقوق قرار گرفته (۳۰) و خلأهای آن مورد شناسایی قرار گرفته، همه و همه تأیید می‌کند نیاز به تقنین در این حوزه مورد شناسایی و تأیید قرار گرفته که این خود نقطه روشن و امیدبخشی است، اما هنوز خلأهایی در حوزه حفاظت از داده‌های سلامت وجود دارد که می‌توان با عزمی ملی در جهت رفع آن‌ها قدم برداشت. در این راستا، پیشنهاد می‌شود:

۱ـ یک چهارچوب قانونی مشابه HIPAA برای ایجاد الزامات قانونی جامع در جهت حفاظت از اطلاعات سلامت تدوین شود. این چهارچوب می‌تواند شامل الزاماتی برای تمامی ارائه‌دهندگان خدمات بهداشتی باشد که اطلاعات بیماران را پردازش می‌کنند.

۲ـ اصول GDPR به خصوص در زمینه Privacy by Design و Data Protection Impact Assessments (DPIAs) مورد انطباق قرار گیرد. پیاده‌سازی این اصول می‌تواند به بهبود امنیت داده‌ها و افزایش اعتماد عمومی کمک کند.

۳ـ از تخصص و تحلیل متخصصان داخلی برای شناسایی کمبودهای قانونی، طراحی ابزارهای حقوقی، استخراج چالش‌های انفورماتیک و تنظیم سیاست‌های بومی سلامت‌محور استفاده کنیم.

۴ـ همکاری‌های بین‌المللی برای بهره‌گیری از تجربیات کشورهای پیشرو در زمینه امنیت داده‌های سلامت توسعه یابد. این همکاری‌ها می‌تواند شامل تبادل دانش فنی و به کارگیری بهترین شیوه‌های قانونی و فناورانه باشد.

۵ـ به آموزش و آگاهی‌بخشی به سازمان‌ها و مؤسسات بهداشتی درباره اهمیت امنیت داده‌ها و راهکارهای قانونی و فنی مرتبط توجه و اهتمام ویژه شود. این امر می‌تواند به افزایش سطح امنیت و کاهش خطرات ناشی از نشت اطلاعات منجر شود.

در نهایت به طور کلی، با توجه به رشد سریع فناوری‌های سلامت‌محور و افزایش تبادل داده‌های الکترونیکی، به‌روزرسانی و تقویت قوانین ملی در این حوزه امری ضروری است. اتخاذ رویکردی جامع که همزمان از مزایای HIPAA و GDPR بهره گیرد، می‌تواند به بهبود سیستم سلامت الکترونیک در ایران کمک شایانی نماید و باعث ارتقای سطح حفاظت از حقوق بیماران و داده‌های سلامت شود.

مشارکت نویسندگان

داود سلطانیان: طراحی ایده، جمع‌آوری داده‌ها، تجزیه تحلیل و بازبینی متن، نگارش متن.

ابولفضل قهاری: جمع‌آوری داده‌ها، تجزیه و تحلیل.

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. Shah W. Preserving privacy and security: A comparative study of health data regulations - GDPR vs HIPAA. Int J Res Appl Sci Eng Technol. 2023; 11: 2189-2199.

2. Olawunmi I. Safeguarding health data in a digital era: A comparative study of the GDPR and HIPAA. [Published Online]; 2023.

3. Granmar CG. Global applicability of the GDPR in context. Int Data Privacy Law. 2021; 11(3): 225-244.

4. Said A, Yahyaoui A, Abdellatif T. HIPAA and GDPR compliance in IoT healthcare systems. In Book: Advances in Model and Data Engineering in the Digitalization Era. 2024. p.198-209.

5. Friedewald M, Schiering I, Martin N, Hallinan D. Data protection impact assessments in practice. In Book: Computer Security. ESORICS 2021 International Workshops, CyberICPS, SECPRE, ADIoT, SPOSE, CPS4CIP and CDT & SECOMANE. 2022. p.424-443.

6. Institute of Medicine, Board on Health Care Services, Board on Health Sciences Policy, Committee on Health Research and the Privacy of Health Information: The HIPAA Privacy Rule. Beyond the HIPAA Privacy Rule: Enhancing Privacy, Improving Health Through Research. Washington, D.C.: National Academies Press; 2009. p.334.

7. Eftekhari MH, Parsapour A, Ahmadi A, Larijani B, Yavari N, Shamsi Gooshki E. Policy Brief for Management and Prevention of Defensive Medicine in the Iranian Health System. IJMEHM. 2023; 16(S1): 1-10. [Persian]

8. Vinson DD. No more paper tiger: Promise and peril as HIPAA goes HITECH. J Healthc Risk Manag. 2011; 30(3): 28-37.

9. Nicholson S, Smith CA. Using lessons from health care to protect the privacy of library users: Guidelines for the de-identification of library data based on HIPAA. Proc Am Soc Inf Sci Technol. 2006; 42(1): 1-14.

10. Bradley University. HIPAA privacy rule vs. HIPAA security rule. [Internet]. Available at: https://www.onlinedegrees.bradley.edu/blog/hipaa-privacy-rule-vs-hipaa-security-rule.

11. Xiang D, Cai W. Privacy protection and secondary use of health data: Strategies and methods. [Institutional Report]. 2021.

12. Comply Assistant. The complexities of data compliance: HIPAA vs GDPR explained. [Internet]. Available at: https://www.complyassistant.com/resources/tips/the-complexities-of-data-compliance-hipaa-vs-gdpr-explained.

13. Custers B, Heijne AS. The Right of Access in Automated Decision-Making: The Scope of Article 15(1)(h) GDPR in theory and practice. Computer Law and Security Review. 2022; 17: 1-17.

14. The GDPR Challenge: Privacy, Technology and Compliance in an Age of Accelerating Change. Boca Raton, Florida: CRC Press; 2021. p.240.

15. Vrabec HU. Data Subject Rights under the GDPR. Oxford: Oxford University Press; 2021. p.288.

16. Li H, Yu L, He W. The impact of GDPR on global technology development. J Glob Inf Technol Manag. 2019; 22(1): 1-6.

17. U.S. Department of Health and Human Services. HIPAA for professionals: Privacy. [Internet]. Available at: https://www.hhs.gov/hipaa/for-professionals/privacy/index.html.

18. European Parliament and Council. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). [Internet]. Available at: https://www.eur-lex.europa.eu/eli/reg/2016/679/oj.

19. Digital Health Central. GDPR vs HIPAA: Key Differences. [Internet]. Available at: https://www.digitalhealthcentral.com/gdpr-vs-hipaa/.

20. Yigzaw KY, Olabarriaga S, Michalas A, Marco-Ruiz L, Hillen C, Verginadis Y, et al. Health data security and privacy: Challenges and solutions for the future. In Book: Health Data Security and Privacy. Amsterdam: Elsevier; 2022. p.335-362.

21. Voigt P, von dem Bussche A. The EU General Data Protection Regulation (GDPR): A Practical Guide. 1st ed. Cham: Springer International Publishing; 2017 p.383.

22. Islamic Republic of Iran's Law on Electronic Commerce. Available at: https://www.rc.majlis.ir/fa/law/show/1014547.

23. Islamic Republic of Iran's Cybercrime Law. Available at: https://www.rc.majlis.ir/fa/law/show/1062426.

24. Meghdadi MM, Delavari MH. The civil liability due to revealing medical secrets in Iran's law and common law. MLJ. 2014; 8(30): 99-145. [Persian]

25. Farhamandian V, Farhamandian M, Mehrabanfar E, Afkhami M. The role of information technology in

contemporary health management in Iran in regard with a future outlook. Intelligent Business Management Studies. 2014; 3(10): 21-38. [Persian]

26. Ghanad F, Sharif E. Comprehensive study of personal data protection in Iran's legal system and European General Data Protection Regulations. New Technologies Law Journal. 2021; 2(4): 1-22. [Persian]

27. Latifzadeh M, Ghobouli Darafshan SMM. How to transfer personal data internationally: A comparative study of European Union law and Iranian legal system. Comparative Law Research Journal. 2022;9(B):221. [Persian]

28. Hosseini SA. Artificial intelligence and the challenges of personal data protection rules with a control approach; Alternative legal regime. Journal of State and Law. 2024; 5(1): 99-122. [Persian]

29. Moghaddasi H, Ghaemi MM. A comparative study of three standards of data security in health systems. JHBMI. 2015; 2(3): 184-194. [Persian]

30. Farahmand F. The bill of data protection and GDPR 2018: A comparative study. New Technologies Law Journal. 2024; 5(9): 17-25. [Persian]