دانشگاه علوم پزشکی هوشمند
Smart University of Medical Sciences
JLHS
Journal of Law & Health Studies

مقاله پژوهشی | مجله مطالعات حقوق و سلامت ۱۴۰۴, ۱, ۱۷۳-۱۵۷

مجله مطالعات حقوق و سلامت | شاپا:۶۵۴۸-۳۰۹۲

مطالعه تطبیقی الزامات کیفری پرونده‌های سلامت الکترونیکی در کشورهای پیشرو و ایران

بابک ثابت [۱*]، مهدی سعیدیان [۲]، پردیس قنواتی [۳]

۱- گروه جراحی، دانشکده پزشکی، دانشگاه علوم پزشکی شهید بهشتی، تهران، ایران
۲- گروه حقوق عمومی، دانشگاه آزاد اسلامی، واحد علوم و تحقیقات، تهران، ایران
۳- دانش آموخته کارشناسی ارشد حقوق بین الملل، دانشگاه شهید بهشتی، تهران، ایران

چکیده

زمینه و هدف: امروزه با پیشرفت گسترده فناوری اطلاعات، نقش آن بیش از پیش در بخش سلامت حائز اهمیت می‌باشد. با این حال، این کاربردها چالش جدیدی را برای حفاظت از حریم خصوصی به‌وجود می‌آورند و در نتیجه، دولت‌ها درصدد اتخاذ تدابیر مختلف، از جمله تصویب قوانین کیفری با هدف مقابله با این چالش هستند.

روش‌ها: این مقاله با مقایسه الزامات کیفری پرونده‌های سلامت الکترونیک در کشورهای پیشرو و ایران، براساس بررسی قوانین اطلاعات الکترونیک و نحوه اجرای آن در مجامع بین‌المللی و قوانین تجارت الکترونیک ایران تهیه شده است و با ارائه یک مدل استراتژیک در خصوص قوانین و الزامات کیفری پرونده‌های سلامت الکترونیک پیشنهاداتی برای بهبود امنیت و محرمانگی پرونده‌های سلامت الکترونیک مطرح شده است.

یافته‌ها: پرونده‌های سلامت الکترونیک و به‌طور خاص موضوع محرمانگی در کشورهای عضو اتحادیه اروپا، آمریکا و ایران از رویکرد حقوق کیفری بررسی شده است. به‌دلیل عدم وجود قانون جامع مختص به سلامت الکترونیک و رویه‌های قضایی این حوزه در ایران، به قوانین مرتبط نظیر مجازات اسلامی، تجارت الکترونیک، جرائم رایانه‌ای و نیز قوانین حمایت از نظام جامع اطلاعات سلامت پرداخته می‌شود.

نتیجه‌گیری: رویکردهای متفاوتی به موضوع حفاظت از داده‌های شخصی سلامت در کشورهای مختلف وجود دارد. کشورهای عضو اتحادیه اروپا بیشتر بر حق‌ها و آزادی‌های فردی تاکید دارند. ایالات متحده آمریکا به‌دنبال تصویب تشدید مجازات‌ها برای مقابله با این‌گونه جرائم است. ایران نیز با هدف بهره‌گیری از الگوهای کشورهای پیشرفته و استفاده از اصول مذهبی و زمینه‌های فرهنگی، در قالب یک برنامه ده ساله، تلاش دارد حریم خصوصی و اطلاعات شخصی سلامت را به حداکثر حفاظت برساند. با توجه به گستردگی و رشد سریع حوزه سلامت الکترونیک، اتخاذ رویکردی جهت قانونگذاری تخصصی در این حیطه ضروری می‌باشد.

کلید واژه‌ها: حریم خصوصی، اطلاعات سلامت، حفاظت از داده ها، تجارت الکترونیک، جرائم رایانه‌ای.

اطلاعات مقاله

10.22034/jlhs.01.01.157

تاریخچه مقاله:
تاریخ دریافت: ۱۴۰۴/۰۵/۰۵
تاریخ پذیرش: ۱۴۰۴/۰۶/۱۶
انتشار آنلاین: ۱۴۰۴/۰۶/۲۴

دسترسی سریع به مقاله الکترونیکی

اطلاعات نویسنده مسئول:
بابک ثابت
گروه جراحی ، دانشکده پزشکی، دانشگاه علوم پزشکی شهید بهشتی، تهران، ایران.
ایمیل: sabetdivshali@gmail.com

حیطه موضوعی:
حقوق و سلامت دیجیتال

نحوه ارجاع دهی:

ثابت، بابک.، سعیدیان، مهدی.، قنواتی، پردیس. مطالعه تطبیقی الزامات کیفری پرونده‌های سلامت الکترونیکی در کشورهای پیشرو و ایران. مجله مطالعات حقوق و سلامت. ۱۴۰۴;۱(۱):۱۷۳-۱۵۷.

JLHS

Journal of Law and Health Studies | ISSN: 3092-6548

Original Article | JLHS, 2025, 1, 157-173

Criminal Requirements for Electronic Health Records in Developed Countries and Iran: A Comparative Study

Babak Sabet[*1], Mahdi Saidian[2], Pardis Ghanavati[3]

1. Department of Surgery, School of Medicine, Shahid Beheshti University of Medical Sciences, Tehran, Iran
2. Department of Public Law, Islamic Azad University, Science and Research Branch, Tehran, Iran
3. Master of International Laws, Shahid Beheshti University, Tehran, Iran

Abstract

Background and Objective: Today, with the extensive advancement of information technology, its role in the health sector is more important than ever. However, these applications pose new challenges to the protection of privacy, and as a result, governments are seeking to adopt various measures, including the adoption of criminal laws, to address this challenge.

Methods: This article compares the criminal requirements for electronic health records in leading countries and Iran, based on a review of electronic information laws and their implementation in international forums and Iran's Electronic Commerce Law. By presenting a strategic model regarding the criminal laws and obligations for electronic health records, suggestions are made to improve the security and confidentiality of electronic health records.

Findings: E-health cases, and specifically the issue of confidentiality, have been examined in the member states of the European Union, the United States, and Iran from a criminal law perspective. Due to the lack of a comprehensive law specifically dedicated to e-health and the judicial procedures in this area in Iran, relevant laws such as the Islamic Penal Code, e-commerce, computer crimes, and laws protecting the comprehensive health information system are addressed.

Conclusion: There are different approaches to the issue of protecting personal health data in different countries. The member states of the European Union emphasize more on individual rights and freedoms. The United States of America is seeking to enact stricter punishments to combat such crimes. Iran, with the aim of utilizing the models of advanced countries and using religious principles and cultural foundations, is striving to maximize the protection of privacy and personal health information within the framework of a ten-year program. Given the vastness and rapid growth of the e-health field, it is necessary to adopt an approach to specialized legislation in this area.

Keywords: Privacy, Health Information, Data Protection, Electronic Commerce, Cybercrimes.

Article Info

10.22034/jlhs.01.01.157

Received: 27 July 2025
Accepted: 07 September 2025
Published: 15 September 2025

Scan QR code and read the article online

Corresponding author:

Babak Sabet
Department of Surgery, School of Medicine, Shahid Beheshti University of Medical Sciences, Tehran, Iran
E-mail: sabetdivshali@gmail.com

Scope:

Digital Law and Health

How to Cite This Article

Sabet, B., Saidian, M., Ghanavati, P. Criminal Requirements for Electronic Health Records in Developed Countries and Iran: A Comparative Study. Journal of Law and Health Studies. 2025;1(1):157-173.

۱- مقدمه

پیشرفت فناوری اطلاعات و ارتباطات در دو دهه اخیر سبب تحول عظیمی در علوم، صنایع و خدمات مختلف شده است. تاثیر این فناوری بر علوم و کسب و کارها موجب ظهور حیطه‌های جدیدی مانند دولت الکترونیک، آموزش الکترونیک، سلامت الکترونیک و غیره شده است. یکی از مقوله‌هایی که به واسطه ذینفعان و ذیربطان (آحاد ملت) حجم زیادی از اطلاعات را شامل می‌شود، بخش سلامت، بهداشت و درمان است. فناوری اطلاعات سلامت به معنای بهره‌برداری از فرآیندهای سخت‌افزاری و نرم‌افزاری به منظور حفظ و نگهداری، بازیابی، به اشتراک‌گذاری و استفاده از داده‌های سلامت، جهت تبادل اطلاعات و تصمیم‌گیری می باشد. فناوری اطلاعات سلامت، چهارچوب جامعی را برای مدیریت اطلاعات سلامت و تبادل ایمن اطلاعات میان کاربران و ارائه‌دهندگان خدمات، نهادهای دولتی و بیمه‌گزاران بخش سلامت فراهم نموده است.[۱] هم‌زمان با گسترش استفاده از رایانه و تلفن همراه، جرائم گوناگونی در حوزه‌های مختلف اقتصادی و اجتماعی با استفاده از این ابزارها در حال وقوع است که به جرائم رایانه‌ای معروف هستند. با توجه به ماهیت جرائم رایانه‌ای، ارتکاب این جرائم، کم‌هزینه، اما آثار سوء آن بسیار زیاد و پرهزینه است. یکی از پیشرفت‌های مهم حوزه فناوری اطلاعات سلامت به پرونده‌های سلامت الکترونیک مربوط می‌شود که در بسیاری از بخش‌های بهداشتی-درمانی موجب تحول در زمینه حفاظت، دسترسی به اطلاعات سلامت و ارتقای کیفیت خدمات بهداشت و درمان، کاهش خطا و حتی کاهش هزینه-ها شده است.[۲]

۲- پیشینه پژوهش

سلامت الکترونیک، به کاربرد ایمن و مقرون به صرفه فناوری‌های اطلاعات و ارتباطات در حمایت از سلامت و زمینه‌های مربوط به آن از جمله خدمات مراقبت سلامت، خدمات نظارتی، آموزشی و پژوهشی و مطالعه در زمینه سلامت اطلاق می‌شود.[۳] به‌طور کلی سلامت الکترونیکی در قالب یا عنوان سلامت از راه دور موضوعیت دارد. در واقع سلامت از راه دور، به استفاده از فناوری مخابراتی و اطلاعاتی برای حمایت از دسترسی به اطلاعات سلامت، توسط متخصصان سلامت و عموم مردم، خدمات مراقبت، سلامت عمومی و مدیریت سلامت اطلاق می‌شود. سلامت از راه دور می‌تواند به سادگی یک تماس تلفنی میان دو متخصص سلامت در مورد یک پرونده و یا به‌کارگیری ابزارهای پیشرفته‌ای نظیر کنفرانس ویدئویی میان ارائه‌دهندگان خدمات سلامت در دو منطقه دور از یکدیگر باشد. از این‌رو، سلامت از راه دور عموماً به‌عنوان یک مفهوم کلی به‌تمام انواع خدمات مراقبت سلامت با استفاده از ارتباطات الکترونیک و فناوری اطلاعات تعریف می‌شود و نه تنها توسط پزشکان، بلکه توسط کلیه متخصصان امر سلامت که از فناوری‌های راه دور بهره می‌برند مورد استفاده قرار می‌گیرد.[۴] در این راستا واژه جرائم الکترونیکی، مطرح می‌شود که بیانگر استفاده از رایانه و سایر سیستم‌های ارتباطات الکترونیکی برای تسهیل ارتکاب اعمال مجرمانه می‌باشد. در عصر ظهور فناوری اطلاعات سلامت، هرگونه پیشرفت در این حوزه می‌تواند یک چالش جدید برای حریم خصوصی بیماران پدید آورد. اطلاعات موجود در پرونده‌های سلامت الکترونیک ممکن است شامل مواردی از جمله تاریخچه پزشکی، نحوه زندگی، امور خصوصی، داروهای مورد استفاده، نتایج آزمایشات، اطلاعات ژنتیکی، اطلاعات مربوط به پرداخت‌های مالی و بسیاری از اطلاعات مهم دیگر باشد. بنا به اهمیت این موضوع، پزشکان، بیمارستان‌ها، بیمه‌گزاران، شرکت‌های حقوقی مرتبط با سلامت و دست‌اندرکاران فناوری اطلاعات با هدف مقابله با تهدیدات مربوط به پرونده‌های سلامت الکترونیک، باید از آمادگی لازم برخوردار باشند، اما حقیقت این است که بسیاری از آن‌ها هنوز به آمادگی لازم نرسیده‌اند.[۵] وزارت سلامت و خدمات انسانی آمریکا در سال‌های اخیر تأکید ویژه‌ای بر ارتقای سیستم فناوری اطلاعات، شامل نرم‌افزارها و شبکه‌های اینترنتی مورد استفاده، به‌ویژه از نظر امنیت داده‌ها در مراکز و موسسات مرتبط با سلامت، را دارد.[۶] مصوبه اخیر دولت فدرال آمریکا درخصوص قانون هیپا در بیش از ۴۳ ایالت آمریکا اجرا می‌شود و نیویورک فعال‌ترین ایالت در تشویق موسسات بهداشتی به بهبود وضعیت سیستم فناوری اطلاعات و ملزم ساختن آن‌ها به پیروی از قوانین جدید، جهت بالابردن سطح امنیت پرونده‌ها می باشد؛ به‌طوری که درنظر دارد طی یک برنامه ده ساله حداقل ۷۵ درصد ارائه‌دهندگان خدمات سلامت به سیستم پیشرفته تجهیز شوند. به‌طورکلی مطالعه قوانین حقوقی کشورهای خارجی به‌طور مجزا و مقایسه

مقررات و اصول آن‌ها با یکدیگر و با کشور خود که تحت عنوان مطالعه تطبیقی شناخته می‌شود.[۷] فرصت مناسبی را برای شناخت تفاوت‌ها بین آن‌ها از نظر مسائل حقوقی، فراهم آورده و زمینه را برای ترسیم یک الگوی جدید متناسب با شرایط کشور مهیا می‌سازد.[۸]

۳- توصیف و بررسی

در کشورهای پیشرو مانند ایالات متحده، استرالیا، کانادا، و کشورهای اروپایی، الزامات کیفری مرتبط با پرونده‌های سلامت الکترونیک (EHR) عمدتاً براساس قوانین حفظ حریم خصوصی و امنیت اطلاعات نظارت می‌شوند. به‌عنوان مثال، در ایالات متحده، قانون سلامت و مسئولیت‌پذیری بیمه (HIPAA) الزامات سخت‌گیرانه‌ای برای حفاظت از اطلاعات سلامت شخصی (PHI) تعیین کرده است. این الزامات شامل تضمین محرمانگی، یکپارچگی، و دسترس‌پذیری اطلاعات سلامت است.[۹] در ایران، استفاده از پرونده‌های سلامت الکترونیک نیز تحت نظارت قوانین خاصی قرار دارد. بر اساس قانون شماره ۲۶۹ وزارت بهداشت، درمان و آموزش پزشکی، پرونده‌های پزشکی می‌توانند به صورت الکترونیکی تهیه شوند. با این حال، هنوز قوانین خاصی برای مدیریت و حفاظت از این اطلاعات وجود ندارد. مسئولیت کیفری در صورت سوءاستفاده از این اطلاعات بر عهده کارکنان پزشکی و بیمارستان‌ها است.[۱۰] در کشورهای پیشرو، استفاده از سیستم‌های اطلاعاتی پیشرفته و نرم‌افزارهای متن‌باز برای مدیریت پرونده‌های سلامت الکترونیک رایج است. این سیستم‌ها به بهبود کیفیت و کارایی خدمات بهداشتی کمک می‌کنند و از بروز خطاهای پزشکی جلوگیری می‌کنند.[۱۱]

۳-۱- پرونده‌های سلامت الکترونیک و حفاظت از داده‌ها

پرونده‌های سلامت الکترونیک به‌علت مزایای فوق‌العاده‌ای که دارند مورد توجه سیاست‌گذاران و ارائه‌دهندگان خدمات بخش سلامت قرار گرفته‌اند. هرچند پرونده‌های سلامت الکترونیک از مزایای متعددی از قبیل ارتقای سطح کیفی خدمات، کاهش خطاهای پزشکی، ارتقای امنیت اطلاعات دسترسی آسان، کاهش زمان دسترسی و انتقال اطلاعات، ارتقای سطح تصمیم‌گیری برخوردار می‌باشد، به‌دلیل ساختار و عملکرد خاص خود، به‌طور جدی درمعرض مخاطرات ناشی از کاربرد فناوری رایانه‌ای نظیر ویروس‌ها، خطاهای برنامه‌نویسی، عدم دسترسی به اطلاعات به‌علت نقص رایانه‌ای، دسترسی غیرمجاز، دخل و تصرف و سرقت اطلاعات توسط هکرها قرار دارند.[۱۲] جرائم مربوط به پرونده‌های سلامت الکترونیک، از طریق دسترسی غیرمجاز، تخریب، تغییر، سرقت و افشای اطلاعات محرمانه شخصی، می‌تواند امنیت، سلامت و حتی جان و حیثیت افراد جامعه را با مخاطرات جدی مواجه کند. علاوه براین، جعل، کلاهبرداری و قصور در ثبت اطلاعات به‌ویژه در مواردی می‌تواند منجر به آسیب جدی یا حتی مرگ دیگران شود، لذا باید با موارد نقض قانون از جانب مراجع قضایی، برخورد جدی کیفری صورت گیرد. با اعمالی نظیر جرائم فوق، معمولاً با مجازات‌هایی مانند جزای نقدی بسیار سنگین و یا حبس مقابله می‌شود و هدف از آن صرفاً پرداخت غرامت اصلاح و برگرداندن شرایط به قبل از وقوع جرم نیست بلکه متنبه کردن فرد مجرم و آینه عبرت نمودن او برای سایرین نیز مدنظر می‌باشد. این جرائم در گروه جرائم کیفری دسته‌بندی می‌شوند.[۱۳]

۳-۲- قوانین حفاظت از داده‌های شخصی

فقدان قوانین، مقررات و استانداردهای موثر به‌منظور حفظ حریم خصوصی و امنیت داده‌های شخصی در سیستم قضایی برخی کشورها به‌همراه نبود هماهنگی و همکاری بین‌المللی در زمینه مصادیق فرامرزی جرائم مزبور، موجب نگرانی‌های بسیاری شده است و مسئولان و سیاست‌گذاران برخی کشورها را به اندیشه مبارزه کیفری با این جرائم سوق داده است. مشکلات فوق نقش اساسی در ایجاد چالش‌های پیش روی سلامت الکترونیک بازی می‌کنند. متاسفانه، اقدامات صورت گرفته در خصوص تدوین استانداردها یا دستورالعمل‌های لازم توسط انجمن‌های حرفه‌ای و موسسات حقوقی نیز با پیشرفت‌های فناوری در عرصه سلامت همگام نبوده‌اند.[۱۴] به‌منظور مقابله با تهدیدات فوق، دو رویکرد اساسی وجود دارد؛ ۱- پیشگیری از طریق ارتقاء کیفی ساختار فنی سیستم و ایجاد موانع جهت جلوگیری از دسترسی غیرمجاز و سوءاستفاده از داده‌ها و ۲- مجازات متخلفان، همچون اخراج، تعهد قانونی، پیگیری کیفری، جزای نقدی، حبس و غیره را شامل شود.[۱۵] اگر بپذیریم که

قوانین مربوط به حفظ حریم خصوصی باید سازنده و پیشگیرانه باشند و نه انفعالی، به‌کارگیری تدابیر پیشگیرانه نظیر توجه به امور فنی سیستم و آگاه‌سازی کاربران جهت اجتناب از خطا، بر مجازات آن‌ها به‌دلیل تخلفات احتمالی، ارجحیت خواهد داشت؛ به‌خصوص اینکه در بسیاری از این موارد ارتکاب تخلف به‌طور ناآگاهانه صورت می‌پذیرد. البته، هرگز نمی‌توان اهمیت رویکرد دوم را نادیده گرفت و حقیقت این است که این رویکرد در کنار رویکرد اول، می‌تواند جنبه بازدارنده یا پیشگیرانه نیز داشته باشد.[۱۶]

۳-۲-۱- قوانین اروپایی

کشورهای عضو اتحادیه اروپا و به‌ویژه فرانسه (به‌عنوان مهد قانون)، نه‌تنها در خصوص حقوق مربوط به حفاظت از حریم خصوصی و محرمانگی داده‌های شخصی، قوانین ویژه‌ای وضع کرده‌اند؛ بلکه با احترام خاصی که برای حقوق و آزادی‌های فردی قائل هستند، هرگونه بی‌توجهی به این حقوق را در امور جمع‌آوری، پردازش، انتقال و انتشار داده‌ها، خلاف قانون می‌دانند. در بند ۱ ماده ۸ آیین‌نامه EC/۴۶/۹۵ اتحادیه اروپا، غیرقانونی بودن پردازش داده‌های شخصی مربوط به ریشه‌های قومی ـ نژادی، اعتقادات سیاسی، دینی، فلسفی، داده‌های مربوط به سلامت و مسائل جنسی در کشورهای عضو این اتحادیه به‌صراحت بیان شده است. داده‌های مربوط به سلامت که در گروه داده‌های حساس طبقه‌بندی می‌شوند، در اکثر کشورهای جهان و به‌ویژه در کشورهای عضو اتحادیه اروپا بیش از سایر داده‌ها مورد حفاظت قرار دارند. طبق بند فوق، پردازش داده‌های شخصی مربوط به سلامت، بدون اجازه قانونی یا جز در مواردی که قانون به صراحت اجازه آن را صادر کرده، جرم محسوب می‌شود و مجرم با محکومیت‌های سنگین قانونی مواجه خواهد شد. به‌موجب Principle 10.1 آیین‌نامه Recommendation R(97)5 شورای اروپا (که اغلب با مقررات اتحادیه اروپا همخوانی دارد)، فرد یا نهادی که داده‌های شخصی مذکور را در اختیار دارد موظف است اقدامات فنی و سازمانی مناسب برای حفاظت از داده‌های شخصی در برابر تخریب، حذف، دسترسی، تغییر، انتقال، انتشار و هر نوع پردازش غیرمجاز را به‌عمل آورد. در آیین‌نامه R(97)5 شورای اروپا، در ارتباط با حفاظت از داده‌های سلامت، بر احترام به حقوق و آزادی‌های فردی در امور جمع‌آوری و پردازش داده‌ها تأکید شده است. براساس آیین‌نامه مذکور، داده‌های پزشکی باید به‌صورت عادلانه و قانونی و تنها برای اهداف مشخص شده، جمع‌آوری و پردازش شوند. آیین‌نامه فوق در موارد زیر نیز بر کسب رضایت بیمار تأکید دارد: (۱) چنانچه لازم باشد، بیمار رضایت خود را اعلام کند، این رضایت باید آزادانه، صریح و آگاهانه باشد. (۲) آزمایش‌های ژنتیکی باید در محدوده اهداف مشاوره، تشخیص یا درمان پزشکی که رضایت فرد در ارتباط با آن کسب شده انجام شوند. طبق Principle 5.1 این آیین‌نامه، بیمار باید حداکثر در زمان جمع‌آوری داده، از موارد زیر اطلاع پیدا کند:[۱۷،۱۸،۱۹]

محتوای پرونده حاوی داده‌های پزشکی خود و نوع داده‌ها.
هدف یا اهداف حفاظت از داده‌ها.
افراد یا نهاد جمع‌آوری‌کننده داده‌ها (در صورت امکان).
افراد یا نهادی که داده‌ها به آن‌ها منتقل می‌شوند و دلایل این انتقال.
امکان بازپس‌گیری رضایت در هر زمان برای شخص بیمار.
هویت کنترل‌کننده و نماینده او و همچنین شرایط صدور مجوز برای حق دسترسی.

نادیده گرفتن هریک از حقوق فردی فوق، تخلف از قانون تلقی می‌شود و با مجرم برخورد قانونی خواهد شد. این قوانین بیانگر توجه خاص اتحادیه اروپا به حق آزادی و استقلال فردی است.[۲۰] قوانین دولت فدرال و دولت‌های ایالتی درخصوص حفاظت از داده مشخص را باید جداگانه مورد مطالعه قرار داد.

۳-۲-۲- قوانین آمریکا

در ایالات متحده آمریکا، قانون حمل‌پذیری و مسئولیت‌پذیری بیمه سلامت (HIPAA) که در سال ۱۹۹۶ تصویب شد، استانداردهای ملی برای حفاظت از اطلاعات پزشکی فردی و سایر اطلاعات شناسایی‌کننده سلامت (PHI) برقرار می‌کند. این قانون، که توسط وزارت بهداشت و خدمات انسانی (HHS) اجرا می‌شود، بر محرمانگی داده‌های شخصی تأکید دارد و تنها اجازه استفاده، پردازش یا افشای این داده‌ها را در موارد مجاز مانند درمان، پرداخت یا عملیات مراقبت‌های بهداشتی، یا با رضایت صریح فرد، می‌دهد. نقض قاعده حفظ حریم خصوصی HIPAA، مانند دسترسی غیرمجاز یا افشای داده‌ها، می‌تواند منجر به جریمه‌های سنگین مالی (تا ۵۰،۰۰۰ دلار برای هر تخلف) و حتی مجازات کیفری شود،

و نهادهای پوششی مانند ارائه‌دهندگان مراقبت‌های بهداشتی، طرح‌های بیمه و مراکز تسویه حساب‌ها موظف به اجرای اقدامات امنیتی مناسب برای جلوگیری از چنین تخلفاتی هستند.[۲۱]

۳-۲-۲-۱- قوانین فدرال آمریکا

ایالات متحده آمریکا، از نظر نرخ وقوع جرائم الکترونیکی مقام نخست جهان را دراختیار دارد. بین سال‌های ۲۰۰۰ تا ۲۰۰۷ میلادی، در این کشور حدود ۴۰ درصد حوادث امنیتی شناخته شده در سازمان‌های بهداشت و درمان، درگروه دسترسی غیرمجاز به داده‌ها قرار گرفتند و تنها در سال ۲۰۰۵ میلادی، حدود ۲۵۰۰۰۰ نفر قربانی سرقت اطلاعات پزشکی شدند، لذا این کشور با تصویب قانون انتقال‌پذیری و مسئولیت‌پذیری بیمه سلامت (هیپا) (HIPAA: Health Insurance Probability and Accountability Act) درصدد اعمال قوانین کیفری و مبارزه جدی با این جرائم برآمده است.[۲۲] از آن‌جا که مقررات کیفری خاصی در این قانون برای مقابله با نقض حریم اطلاعات و امنیت داده‌های شخصی گنجانده شده است، در این بخش یک مرور اجمالی بر این قانون خواهد شد. براساس بند ۱۱۷۶ این قانون، هر فردی که امنیت یا تمامیت داده‌های شخصی حساس، نظیر داده‌های سلامت را به مخاطره اندازد، برای هر بار تخلف، به پرداخت حداقل ۱۰۰ دلار جریمه نقدی محکوم می‌شود، که مبلغ کل جریمه برای تمامی موارد نقض این قانون طی یک سال، نباید از ۲۵۰۰۰ دلار فراتر رود. البته، در مواردی که فرد مسئول، از تخلف و نقض مواد قانونی بی‌اطلاع باشد و یا به دلایل موجه مرتکب آن شود و حداکثر ظرف سی روز از آگاهی به تخلف، آن را اصلاح کند، مجازاتی در مورد وی اعمال نخواهد شد. بالعکس، سنگین‌ترین مجازات‌ها برای استفاده غیرقانونی از اطلاعات به‌منظور کسب سود برای خود و یا زیان رساندن به دیگری درنظر گرفته شده است. این رویکرد دو وجهی قانون، بیانگر اهمیت قصد و نیت افراد در تعیین مجازات است.[۲۳] در این قانون همچنین تصریح شده است؛ فردی که عامدانه از شناسه سلامت دیگری استفاده کند، اطلاعات شخصی قابل شناسایی دیگری را به‌دست آورد یا آن را برای سایرین افشا کند، به حداکثر ۵۰۰۰۰ دلار جریمه نقدی یا یک سال حبس یا هر دو مورد محکوم خواهد شد. شایان ذکر است که اگر این جرائم تحت دلایل کذب صورت گیرند، ممکن است مجازات‌های قانونی تا ۱۰۰۰۰۰ دلار یا حبس تا پنج سال یا هر دو مورد را برای مجرم در پی داشته است. در صورتی که جرم مذکور با قصد فروش، انتقال، کاربرد تجاری، منفعت شخصی و با سوء نیت انجام شود، ۲۵۰۰۰۰ دلار جریمه نقدی یا حبس تا ده سال و یا هر دو مورد برای آن در نظر گرفته می‌شود. براساس قانون جدیدی که در فوریه ۲۰۰۹ به تصویب دولت فدرال آمریکا رسیده است و تحت عنوان بسته تشویقی شناخته می‌شود، اعتبار مالی قابل‌توجهی به‌منظورگسترش سرمایه گذاری در توسعه پرونده‌های الکترونیک سلامت اختصاص یافته است. هدف این قانون اعمال اصلاحاتی در قانون هیپا می‌باشد که براساس آن، علاوه بر تشویق مراکز و دست‌اندرکاران سلامت، به دیجیتالی کردن پرونده‌های تمامی شهروندان تا سال ۲۰۱۴، الزامات و مجازات مربوط به آن، تشدید گردیده است.[۲۴،۲۵] از جمله این الزامات می‌توان به اجبار موسسات مربوط، به صدور گزارش هرگونه تخلف درخصوص اطلاعات محرمانه افراد، تسهیل امکان دسترسی افراد به پرونده‌های شخصی خود و همچنین تشدید مجازات‌ها درخصوص تخلفات عمدی و غیرعمد، نظیر جزای نقدی و حبس اشاره کرد.[۲۶]

۳-۲-۲-۲- قوانین ایالتی آمریکا

ایالت‌هایی نظیر مینسوتا و کالیفرنیا در ایالات متحده آمریکا، درخصوص حفاظت از اطلاعات یا داده‌های پرونده‌های سلامت، قوانین مستقل و جداگانه‌ای نیز وضع کرده‌اند؛ که این امر بیانگر اهمیت این اطلاعات برای قانون‌گذاران ایالت‌های مزبور می‌باشد. به‌عنوان مثال طبق بندهای ۱۴۴/۲۹۱ تا ۱۴۴/۲۹۸ قانون پرونده‌های سلامت ایالت مینسوتا، هر فرد یا سازمانی که:

(۱) عمداً یا سهواً درخواست افشای غیرقانونی اطلاعات یک پرونده سلامت را مطرح کند یا اقدام به این کار نماید.

(۲) اقدام به جعل امضا روی فرم رضایت‌نامه بیمار نماید یا فرم رضایت‌نامه را بدون جلب رضایت وی تغییر دهد.

(۳) تحت دلایل کذب، اقدام به جمع‌آوری فرم رضایت یا پرونده‌های پزشکی شخص دیگر کند.

علاوه بر جبران خسارات وارده در اثر افشا و جعل، باید هزینه و دستمزد وکیل را نیز تقبل نماید.[۲۷] به تازگی، ایالت کالیفرنیا با تصویب اصلاحیه قانون سلامت و ایمنی، موضع تندتری نسبت به این جرائم اتخاذ کرده است و با متخلفان

برخورد کیفری می‌نماید. طبق این اصلاحیه که از سال ۲۰۰۹ میلادی به اجرا درآمده، نه تنها برای استفاده غیرقانونی از اطلاعات پرونده‌های پزشکی، بلکه برای دسترسی غیرمجاز به این اطلاعات نیز، مجازات سنگینی درنظر گرفته شده است که شامل حداکثر ۵۰۰۰۰ دلار برای اولین بار، ۷۵۰۰۰ دلار برای دومین بار، و ۱۰۰۰۰۰ دلار برای سومین بار و بیشتر می‌باشد. براساس قانون SB -541، ارائه‌دهندگان خدمات سلامت باید تمام موارد دسترسی غیرقانونی به اطلاعات را حداکثر ظرف پنج روز پس از محرز شدن، به اطلاع بیماران برسانند. در غیر این صورت، در ازای هر روز دیرکرد به ۱۰۰ دلار جریمه نقدی محکوم می‌شوند. که البته این جریمه نباید از ۲۵۰۰۰۰ دلار در سال فراتر رود.[۲۸] قانون هیپا به‌همراه قوانین ایالتی و مربوط به حریم خصوصی و نقض امنیت اطلاعات، همگی درصدد حفاظت از داده‌های افراد از افشا شدن و سوءاستفاده قرار گرفتن می‌باشند. هرچند وجود این قوانین الزاماً حفاظت کامل از داده‌ها را تضمین نمی‌کند و همچنان موارد بسیاری از تخلف در زمینه حریم خصوصی ناشی از دسترسی افراد غیرمجاز به داده‌های شرکت‌های دارویی و شرکت‌ها و مراکز ارائه‌دهنده خدمات سلامت رخ می‌دهد.

۳-۲-۳-کنوانسیون اروپایی جرائم سایبری

کنوانسیون جرائم سایبری در ۸ نوامبر ۲۰۰۱، توسط شورای وزیران اروپا در بوداپست به‌تصویب رسید و در ۲۳ نوامبر ۲۰۰۱ امضاء شد. لازم‌الاجرا شدن مصوبات این کنوانسیون، مستلزم اخذ سه امضا از پنج امضا اعضاء شورا بود. کنوانسیون جرائم سایبری اولین سند حقوقی معاهده بین‌المللی الزام‌آور است که به‌طور خاص برای مبارزه با جرائم مؤثر برسیستم‌ها، شبکه‌ها و داده‌های رایانه‌ای ایجاد شده است. فعالیت‌های جعل، کلاهبرداری رایانه‌ای، پورنوگرافی کودکان و همچنین نقض حق چاپ و حقوق مرتبط با این معاهده یک چهارچوب قانونی برای مبارزه با جرائم سایبری فراهم می‌کند و تبادل اطلاعات بین کشورهای امضاکننده را ترویج می‌کند. این کنوانسیون توسط ۴۶ کشور به امضا رسیده است. در میان کشورهای دنیا، چین، چندین کشور آمریکای لاتین و روسیه که به‌عنوان اولین کشورهای تولیدکننده بدافزار شناخته می‌شوند، آن را امضا نکرده‌اند.[۲۹]

۳-۲-۳-۱- قانون ۱۵ نوامبر ۲۰۰۱

ظهور اقدامات و حملات تروریستی در آغاز قرن، تحولات قانونی در مورد شبکه‌های دیجیتال و اینترنت را تسریع کرد. قانون ۱۵ نوامبر ۲۰۰۱، اصل حفظ اطلاعات اتصال مشترکین را برای مدت یک سال، توسط اپراتورهای تلفن ثابت، سیار و ارائه‌دهندگان خدمات اینترنتی برای اهداف کیفری تعیین کرد. این قانون به مقامات قضایی، امکان دسترسی به برخی اطلاعات محرمانه را می‌دهد تا تحت عنوان دفاع ملی، رمزگشایی داده‌ها صورت گیرد. همچنین تحت این قانون، مصوبات ایجاد یک رصدخانه امنیتی، برای رسیدگی به مسائل مرتبط با جعل کارت‌های بانکی صورت گرفته است.[۳۰]

۳-۲-۳-۲- قانون ۲۱ ژوئن ۲۰۰۴ در خصوص اعتماد به اقتصاد دیجیتال

با قانون اعتماد در اقتصاد دیجیتال، اینترنت اکنون از جایگاه قانونی برخوردار است. این قانون مسئولیت ارائه‌دهندگان خدمات را در عین اجرای حفاظت مؤثر از کاربران اینترنت تعریف می‌کند. ارائه‌دهندگان خدمات فنی و ارائه‌دهندگان سرویس‌های اینترنت طبق شرایط ماده ۶ قانون، تعهدی کلی برای نظارت و جستجوی فعالیت‌های غیرقانونی به‌ویژه در مورد محتوایی که میزبانی، حمل و نقل یا ذخیره می‌کنند، ندارند. بنابراین، این قانون از بی‌مسئولیتی تقریباً کامل میزبان ناشی می‌شود. با این حال، آن‌ها موظفند در مبارزه با جنایات علیه بشریت، تحریک به نفرت، پورنوگرافی کودکان، تحریک به خشونت و حمله به کرامت انسانی مشارکت کنند. آن‌ها باید ضمن محکوم کردن این انحرافات، زمینه لازم را برای مقابله عملی فراهم نمایند. این قانون چهارچوبی را برای اقتصاد دیجیتال ایجاد می‌کند و به تجارت الکترونیک، مسئولیت فروشندگان و تجار اینترنتی آنلاین و چهارچوب قانونی ابزارهای تجارت الکترونیکی، صورت حقوقی می دهد.[۳۱]

۳-۲-۳-۳- قانون ۲۳ ژانویه ۲۰۰۶ در خصوص مبارزه با تروریسم

با این قانون، الزام نگهداری و ارسال اطلاعات فنی به دادگاه‌ها، کافه‌های سایبری و پایانه‌های وای‌فای نیز کشیده

شده است که اپراتورهای ارتباطات الکترونیکی نیز مورد نظر می‌باشند. با این حال، در عمل، فقدان تعهد برای شناسایی مشتریانی که از این خدمات استفاده می‌کنند، محدودیتی واقعی برای استفاده بهینه از این خدمات می‌باشد.[۳۲]

۳-۲-۳-۴- قانون اول اوت ۲۰۰۶ در خصوص کپی رایت و حق‌های وابسته

هدف این قانون حفظ حق‌های پدیدآورندگان است. ناشران و توزیع‌کنندگان نرم‌افزارهایی که بدون رعایت حق‌های مربوط به تولیدکننده، استفاده می‌شوند، در معرض ارتکاب جرم هستند. به‌همین دلیل، مصادره درآمد حاصل از بهره‌برداری از نرم‌افزارهای کپی شده، ممنوعیت از انجام فعالیت انتشار یا توزیع نرم‌افزار و اعلام عمومی حکم مجرمان، به‌عنوان ابزارهای مقابله می‌باشد. در نهایت، این قانون دارای عوامل تشدیدکننده مجازات نیز می‌باشد؛ مانند استفاده از نام و یا کرونولوژی رسانه‌ای، به معنای ارائه اثر، قبل از انتشار رسمی آن.[۳۳]

۳-۳- قوانین ایران

۳-۳-۱- قوانین کیفری حفاظت از داده‌های شخصی در جمهوری اسلامی ایران

در حالی که ۱۰ تا ۱۵ درصد تولید ناخالص کشورهای پیشرفته به بخش سلامت اختصاص می‌یابد و ۵ تا ۱۰ درصد این میزان، در برنامه‌های سلامت الکترونیک هزینه می‌شود، اعتبار مربوط به نظام سلامت الکترونیک ایران، حدود یک درصد کشورهای پیشرفته است که این امر خود نمایانگر مسیر طولانی پیش روی کشور جهت توسعه این حوزه فعالیت می‌باشد.[۳۴] در حوزه حقوقی سلامت الکترونیک و مقررات مربوط به حفاظت از داده‌های شخصی نیز تاکنون قوانین صریحی وضع نشده است. البته، قوانینی در کشور وجود دارد که می‌تواند به‌طور غیرمستقیم در ارتباط با جرائم حوزه سلامت الکترونیک مورد استفاده قرار گیرند و یا در تدوین قوانین مربوط (به‌عنوان مبنا و الگو) به‌کارگرفته شوند. در ادامه به برخی از این قوانین پرداخته می‌شود.

۳-۳-۲- قانون مجازات اسلامی

درخصوص حفاظت از داده‌های شخصی می‌توان گفت که تا قبل از تصویب قانون تجارت الکترونیک، حفاظت داده‌ها در دستورکار قانون‌گذاران ایران نبوده است و تنها در موارد محدودی به‌تدوین قانون اقدام گردیده که مبنای آن بیشتر قانون مجازات اسلامی می‌باشد. به‌عنوان مثال، به‌موجب ماده ۶۴۸ قانون مجازات اسلامی، پزشکان، جراحان، ماماها، داروسازان و تمامی کسانی که به‌واسطه شغل یا حرفه خود حافظ اسرار مردم می‌باشند، هرگاه در غیر از موارد قانونی، اسرار مردم را فاش کنند، به سه ماه و یک روز تا یک سال حبس و یا به یک میلیون و پانصد هزار تا شش میلیون ریال جزای نقدی محکوم می‌شوند؛ که این مبلغ هر سه سال با توجه به نرخ تورم افزایش می‌یابد.[۳۵]

۳-۳-۳- قانون تجارت الکترونیک

شاید بتوان قانون تجارت الکترونیک را اولین قانون ایرانی دانست که حفاظت از داده‌های شخصی را مورد توجه قرارداده است، لذا لازم است در این بخش، مروری کوتاه به برخی موارد کیفری این قانون شود. به‌موجب ماده ۷۱ قانون مذکور، هر فردی که در بستر مبادلات الکترونیکی، بدون اخذ رضایت صریح، اقدام به ذخیره‌سازی، پردازش یا توزیع داده‌های شخصی، بیانگر ریشه‌های قومی-نژادی (به‌عنوان مثال، اطلاعات ژنتیک)، دیدگاه‌های عقیدتی، مذهبی، خصوصیات اخلاقی و نیز داده‌های مربوط به وضعیت جسمانی، روانی و جنسی اشخاص نماید، به حبس از یک تا سه سال محکوم خواهد شد. براساس ماده ۷۲ این قانون، اگر مجرم به موسسات ارائه‌دهنده خدمات مزبور یا سازمان‌های مسئول متعهد باشد، حداکثر مجازات فوق برای وی درنظرگرفته می‌شود. طبق ماده ۷۳ همین قانون، چنانچه جرم فوق براثر سهل‌انگاری و قصور ارائه‌دهندگان خدمات رخ دهد، متخلف به سه ماه تا یک سال زندان محکوم خواهد شد. با توجه به تشابه قانون تجارت الکترونیک و سلامت الکترونیک و زمینه لازم برای تصویب قوانین کیفری مناسب با استفاده از متون فقهی (احکام شرعی)، قانون‌گذار ایرانی می‌بایست، قانون حفاظت از داده‌های شخصی حساس سلامت الکترونیک را به‌طور مجزا مطرح می‌نماید تا از این نوع داده‌ها نیز به‌صراحت حمایت قانونی به‌عمل می‌آید.[۳۶]

۳-۳-۴- قانون جرائم رایانه‌ای

بالاخره پس از سال‌ها انتظار در دی ماه ۱۳۸۷، قانون جرائم رایانه‌ای به‌تصویب رسید و یک خلاء مهم قانونی کشور برطرف گردید تا قضات بتوانند جرائم رایانه‌ای یا الکترونیکی را براساس قوانین مرتبط، مورد بررسی قرار داده و حکم

مقتضی را صادر نمایند. همان‌طور که از مفاد این قانون برمی‌آید، جمهوری اسلامی ایران با توجه به اهمیت مقابله با این جرائم و به‌ویژه اهمیت صیانت از آبرو و حیثیت افراد جامعه، درصدد اعمال قوانین کیفری متناسب با فرهنگ اسلامی برآمده است. به‌موجب ماده اول قانون یاد شده، دسترسی غیرمجاز به سیستم‌های رایانه‌ای یا مخابراتی که با تدابیر امنیتی حفاظت می‌گردند، منجر به مجازات سه ماه و یک روز تا یک سال حبس و یا پنج تا بیست میلیون ریال جزای نقدی و یا هر دو مورد می‌گردد. براساس ماده دوم، دسترسی غیرمجاز به محتوای در حال انتقال سیستم‌های رایانه‌ای، مخابراتی، امواج الکترومغناطیسی یا نوری منجر به مجازات شش ماه تا دو سال حبس یا ده تا چهل میلیون ریال جزای نقدی و یا هر دو مورد می‌گردد. طبق ماده سوم قانون مذکور، الف) دسترسی، تحصیل یا شنود داده‌های مذکور مشمول مجازات حبس از یک تا سه سال یا جزای نقدی از بیست تا شصت میلیون ریال و یا هر دو مورد می‌شود. ب) در دسترس قرار دادن داده‌های مذکور برای افراد فاقد صلاحیت، دو تا ده سال حبس را به‌دنبال دارد. نکته قابل‌توجه این که در فصل هشتم این قانون، برای مجرمین مسئول در ادارات و سازمان‌های دولتی یا وابسته به دولت، متصدیان شبکه‌های ارتباطی، افرادی که به‌صورت سازمان‌یافته و یا با برنامه‌ریزی قبلی و یا در سطح گسترده به این اعمال مجرمانه اقدام می‌کنند، بیش از دو سوم حداکثر مجازات درنظر گرفته شده است.[۳۷] برای جرائم علیه صحت و تمامیت داده‌ها و سیستم‌های رایانه‌ای و مخابراتی، جعل، تخریب و اخلال در داده‌ها یا سیستم‌ها، سرقت و کلاهبرداری، مجازات‌هایی در بندها و مواد قانونی مستقل و جداگانه به‌شکل کیفری و درقالب جریمه نقدی سنگین و یا حبس درنظر گرفته شده است که در این مقاله به این موضوعات پرداخته نمی شود.

۳-۵- قوانین حامی نظام جامع اطلاعات سلامت

معاونت تحقیق و توسعه مرکز مدیریت آمار و فناوری اطلاعات وابسته به وزارت بهداشت، درمان و آموزش پزشکی جمهوری اسلامی ایران، براساس دو قانون زیر طرح جامعی را با چشم‌انداز برخورداری تمامی شهروندان از پرونده‌های الکترونیکی آغاز کرده است:

۱- به‌موجب ماده ۸۸ قانون برنامه چهارم توسعه اقتصادی، اجتماعی و فرهنگی جمهوری اسلامی ایران (۱۳۸۸-۱۳۸۴هش.)، وزارت بهداشت، درمان و آموزش پزشکی موظف است به‌منظور ارتقاء مستمر کیفیت خدمات سلامت و بهبود عملکرد خدمات بالینی، افزایش بهره‌وری و استفاده بهینه از امکانات بهداشتی و درمانی کشور نسبت به طراحی و استقرار نظام جامع اطلاعات سلامت شهروندان ایرانی اقدام کند.

۲- طبق مصوبه شورای عالی سلامت، مورخ دوم مهرماه سال ۱۳۸۷، وزارت بهداشت، درمان و آموزش پزشکی با همکاری سایر نهادهای مرتبط موظف است پرونده الکترونیکی سلامت را توسعه دهد؛ تا در یک دوره ده ساله، بستر اطلاعاتی مناسب برای ارائه خدمات نوین به شهروندان فراهم گردد.

براساس این طرح، ضمن گسترش دامنه به‌کارگیری فناوری ارتباطات و اطلاعات در حوزه پرونده‌های سلامت الکترونیک، مقرراتی نیز درخصوص نقض قوانین و مجازات‌های مربوط تدوین خواهد گردید. در این فرآیند از تعدادی از کارشناسان خبره با تخصص‌های مختلف ازجمله فناوری اطلاعات، حقوق، پزشکی، فقه و... بهره گرفته می‌شود، تا ضمن انجام مطالعات تطبیقی و الگوبرداری از سیستم‌های حقوقی در حوزه مذکور، یک قانون جامع و مستقل برای کشور تدوین و معرفی نمایند.[۳۸] به‌نظر می‌رسد که بررسی قوانین حقوقی کشورها و استفاده از تجارب آن‌ها به‌همراه مدنظر قراردادن زمینه‌های مذهبی و فرهنگی رایج درکشور، می‌تواند منجر به تنظیم قوانینی متناسب با شرایط کشور شود.[۳۹] البته، درکشورهایی نظیر ایران که از ارزش‌های فرهنگی و مذهبی خاصی برخوردار هستند، مسئولین امر بهتر است امکانات مناسبی فراهم آورند تا حقوقدانان، متخصصین امور پزشکی، صاحب‌نظران فرهنگی و علمای مذهبی با به‌کارگیری تجارب سایر کشورها استنباط و الهام از قوانین دین مبین اسلام و نیز زمینه‌های فرهنگی، قوانینی تنظیم نمایند که منطبق با اصول اعتقادی و فرهنگی مردم باشد.[۴۰]

۳-۶- تفاوت‌های الزامات کیفری پرونده‌های سلامت الکترونیک در ایران و کشورهای پیشرو

تفاوت‌های الزامات کیفری مربوط به پرونده‌های سلامت در سه سطح قوانین و مقررات، مسئولیت کیفری و استانداردها و زیرساخت‌ها نمایان می‌شود. در کشورهای پیشرو، مسئولیت کیفری عمدتاً بر عهده پزشکان و مراکز درمانی است که در صورت نقض قوانین، با جریمه‌های

سنگین و حتی حبس مواجه می‌شوند.[۴۱] در ایران با اینکه مسئولیت کیفری همچنان بر عهده پزشکان و مراکز درمانی است، اما قوانین و مقررات خاصی برای مدیریت و حفاظت از اطلاعات سلامت الکترونیک هنوز به طور کامل تدوین نشده است.[۴۲] کشورهای پیشرو از استانداردهای بین‌المللی مانند ISO13606 برای تبادل اطلاعات سلامت استفاده می‌کنند.[۴۳] در ایران، پروژه SEPAS در مراحل اولیه اجرا قرار داشته و نیاز به توسعه زیرساخت‌های ملی اطلاعات سلامت دارد.[۴۴] در جدول ۱ قوانین کیفری در پرونده‌های سلامت الکترونیک در چند کشور پیشرو و ایران مقایسه شده است.

۳-۷- بهبود امنیت پرونده‌های سلامت الکترونیک در ایران

برای بهبود امنیت پرونده‌های سلامت الکترونیک (EHR) در ایران، می‌توان از چندین راهکار استفاده کرد:

- استفاده از فناوری بلاک‌چین: بلاک‌چین می‌تواند امنیت، اصالت و مدیریت زمان داده‌ها را بهبود بخشد. این فناوری با استفاده از قراردادهای هوشمند و سیستم‌های غیرمتمرکز، دسترسی غیرمجاز به داده‌ها را محدود می‌کند و از تغییرات غیرمجاز جلوگیری می‌کند.[۴۵]

- توسعه و به‌روزرسانی مجموعه داده‌های حداقلی (MDS): بازنگری و به‌روزرسانی مجموعه داده‌های حداقلی ملی می‌تواند کیفیت و کارایی اطلاعات را بهبود بخشد و از تکرار داده‌های غیرضروری جلوگیری کند.[۴۶]

- استفاده از تکنیک‌های یادگیری ماشین: تکنیک‌های یادگیری ماشین می‌تواند برای تحلیل و شناسایی مشکلات امنیتی بالقوه قبل از وقوع آن ها استفاده شود. این تکنیک‌ها می‌توانند فعالیت‌های مخرب یا نفوذهای احتمالی را شناسایی کرده و به سازمان‌ها کمک کنند تا به تهدیدات امنیتی به سرعت پاسخ دهند.[۴۷]

اجرای پروتکل‌های امنیتی و احراز هویت: استفاده از پروتکل‌های امنیتی مانند رمزنگاری نامتقارن و متقارن برای تضمین محرمانگی، یکپارچگی، احراز هویت و مجوزدهی اطلاعات سلامت الکترونیک ضروری است. این پروتکل‌ها می‌توانند از تغییرات غیرمجاز و دسترسی‌های غیرمجاز جلوگیری کنند.[۴۸]

- چهارچوب امنیتی برای سیستم‌های مبتنی برابر: استفاده از چارچوب‌های امنیتی که تهدیدات را مدل‌سازی کرده و میزان ریسک را محاسبه می‌کنند، می‌تواند به بهبود امنیت سیستم‌های EHR کمک کند. این چهارچوب‌ها باید بر اساس استانداردهای امنیتی طراحی شوند.[۴۹]

جدول ۱. مقایسه قوانین کیفری در پرونده‌های سلامت الکترونیک در چند کشور پیشرو و ایران

کشور	قوانین و مقررات	مسئولیت کیفری	نکات کلیدی
ایالات متحده	HIPAA (Health Insurance Portability and Accountability Act)	پزشکان و مراکز درمانی	حفاظت از اطلاعات سلامت شخصی (PHI) با استثنائات خاص برای گزارش‌دهی به مقامات قانونی[۳۷]
آلمان	قانون کیفری آلمان(Strafgesetzbuch)	پزشکان و مراکز درمانی	سیستم مبتنی بر کد با تأثیر زیاد نوشته‌های آکادمیک[۵۰]
کانادا	Personal Information Protection and Electronic Documents Act (PIPEDA)	پزشکان و مراکز درمانی	حفاظت از اطلاعات شخصی با تأکید بر رضایت بیمار[۵۱]
استرالیا	Privacy Act 1988	پزشکان و مراکز درمانی	حفاظت از اطلاعات سلامت با تأکید بر شفافیت و دسترسی بیمار[۵۲]
ایران	قانون شماره ۲۶۹ وزارت بهداشت	پزشکان و مراکز درمانی	مسئولیت کیفری در صورت سوءاستفاده از اطلاعات سلامت الکترونیک[۱۰]

۳-۸- چالش‌های اجرای کامل پروژه SEPAS در ایران

پروژه SEPAS (سامانه پرونده الکترونیک سلامت) در ایران با چالش‌های متعددی مواجه است که می‌توان آنها را به چند دسته اصلی تقسیم کرد:

۱-۳-۸- چالش‌های فنی و تکنولوژیکی:

عدم وجود استانداردهای یکپارچه: نبود استانداردهای یکپارچه برای تبادل داده‌ها و هماهنگی بین سیستم‌های مختلف اطلاعاتی بیمارستان‌ها.[۵۳]

مشکلات امنیتی: نگرانی‌های امنیتی و محرمانگی داده‌ها که می‌تواند مانع از پذیرش گسترده سیستم‌های EHR شود.[۴۶]

۲-۳-۸- چالش‌های قانونی و سازمانی:

مسائل قانونی: نبود قوانین و مقررات جامع و به‌روز برای حفاظت از اطلاعات سلامت الکترونیک و مدیریت دسترسی به آن‌ها.[۴۶]

مقاومت در برابر تغییر: مقاومت کارکنان بهداشتی و پزشکان در برابر تغییرات و استفاده از سیستم‌های جدید EHR.[۴۶]

- چالش‌های مالی و اقتصادی:

هزینه‌های بالا: هزینه‌های بالای پیاده‌سازی و نگهداری سیستم‌های EHR و نیاز به سرمایه‌گذاری‌های بزرگ[۴۶]

کمبود منابع مالی: کمبود منابع مالی برای توسعه و به‌روزرسانی سیستم‌های EHR [۵۴]

۳-۳-۸- چالش‌های آموزشی و آگاهی‌بخشی:

کمبود آموزش: کمبود برنامه‌های آموزشی مناسب برای کارکنان بهداشتی و پزشکان در مورد استفاده از سیستم‌های HER.[۴۶]

نگرش منفی: نگرش منفی برخی از پزشکان و بیماران نسبت به استفاده از نرم‌افزارهای سلامت الکترونیک[۴۶]

۴-۳-۸- چالش‌های مدیریتی و اجرایی:

مدیریت ناکارآمد: مدیریت ناکارآمد و عدم هماهنگی بین بخش‌های مختلف بهداشتی و درمانی.[۴۶]

زمان‌بر بودن پیاده‌سازی: زمان‌بر بودن فرآیند پیاده‌سازی سیستم‌های EHR و مشکلات فنی ناشی از تنوع پلتفرم‌ها.[۴۶]

۹-۳- یافته ها

نتایج مطالعات مختلف نشان می‌دهد که دولت ها به این نتیجه رسیده‌اند که منافع کشور در حوزه سلامت در گرو استقرار نظام سلامت الکترونیک است و برای رسیدن به این هدف رویکردهای مختلفی در پیش گرفته‌اند. برای گسترش سلامت الکترونیک در اکثر کشورها، مشوق‌هایی برای مردم، پزشکان، بیمارستان‌ها و شرکت‌های بیمه در نظر گرفته شده است. همچنین، برخی از کشورها برای حفظ امنیت پرونده الکترونیک سلامت و نیز تسهیل روند اجرای سلامت الکترونیک قوانینی وضع کرده‌اند. اتحادیه اروپا نیز طی این دو دهه اخیر از فعالیت‌های تحقیقاتی فناوری اطلاعات حمایت کرده است. در نتیجه این نوع از حمایت‌ها، اتحادیه اروپا پیشرفت‌های قابل توجهی در استفاده از شبکه‌های محلی، پرونده‌های الکترونیک سلامت و توسعه کارت‌های سلامت داشته باشد. در کشور ایران از سال ۱۳۸۰ موضوع سلامت الکترونیک و پرونده الکترونیک سلامت مورد توجه قرار گرفته است. دستاوردهای بدست آمده بیشتر مربوط به وزارت بهداشت، درمان و آموزش پزشکی و سازمان تامین اجتماعی بوده است که با سطح مورد انتظار فاصله زیادی دارد. به علت فقدان قوانین مقایسه‌ای درخصوص سلامت الکترونیک در ایران، برخی از قوانین مرتبط با این حوزه نظیر قانون تجارت الکترونیک، قانون مجازات اسلامی و قانون جرائم رایانه‌ای می‌تواند جهت مقابله با جرائم مدنظر قرار گیرند.

مدل استراتژیک برای قوانین و الزامات کیفری پرونده‌های سلامت الکترونیک و به‌طور خاص موضوع محرمانگی در ایران

برای بهبود امنیت و محرمانگی پرونده‌های سلامت الکترونیک (EHR) در ایران، می‌توان از یک مدل استراتژیک یکپارچه حفاظت از داده‌های سلامت الکترونیک در ایران (ISPDEH-IR) استفاده کرد که شامل چندین محور کلیدی است (جدول ۲ و شکل ۱). این مدل شامل پنج محور کلیدی است که به صورت چرخه‌ای عمل می‌کنند: هر محور بر دیگری تأثیر می‌گذارد و نظارت مداوم را تضمین می‌کند. محورها بر اساس شرایط ایران تنظیم شده‌اند، مانند ادغام با سیستم SIB، توجه به مسائل فرهنگی (مانند تأکید بر رضایت آگاهانه بیماران در جوامع سنتی) و چالش‌های فنی (مانند زیرساخت‌های ضعیف سایبری در بیمارستان‌های دولتی).

- چهارچوب قانونی و مقرراتی: تمرکز بر تدوین قوانین محلی مبتنی بر تجربیات جهانی (مانند GDPR) اما تطبیق‌یافته با قوانین ایران، مانند گسترش قانون حفاظت از داده‌های شخصی (که هنوز ناقص است) برای پوشش

جرایم کیفری در نقض داده‌های سلامت. این محور شامل الزامات کیفری برای نقض حریم خصوصی می‌شود.[۵۵]

- مدل‌های کنترل دسترسی: استفاده از مدل‌های نقش‌محور (RBAC) و ویژگی‌محور (ABAC) برای کنترل دسترسی، با تمرکز بر سطوح مختلف کاربران در ایران (مانند پزشکان، پرستاران و مدیران سیستم SIB). این محور شامل ادغام با استانداردهای ASTM برای دسترسی امن است.[۵۶]

- تکنولوژی‌های امنیتی: پیاده‌سازی رمزنگاری، بلاکچین برای ردیابی داده‌ها، و ابزارهای تشخیص نفوذ، با توجه به تهدیدهای سایبری رایج در ایران (مانند حملات خارجی). این محور بر استانداردهای ISO 18308 برای امنیت داده تأکید دارد.[۵۶]

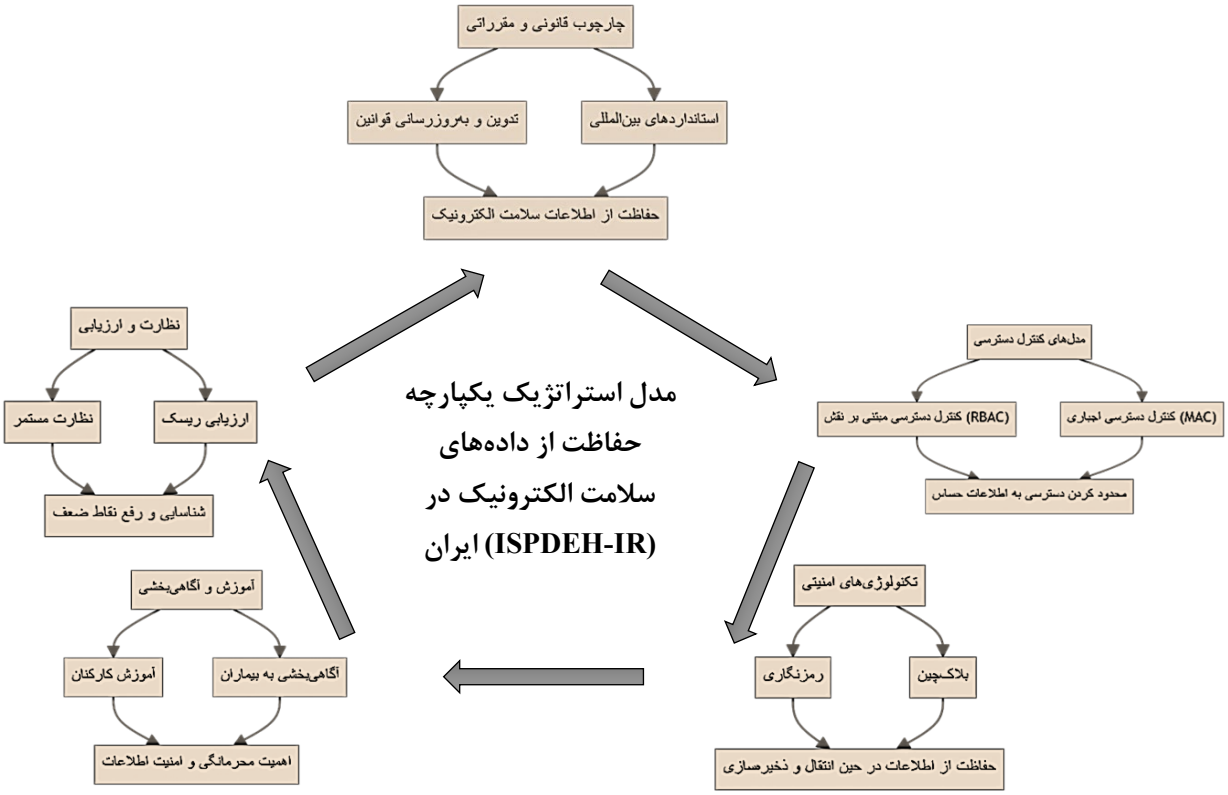
- آموزش و آگاهی‌بخشی: برنامه‌های آموزشی برای کادر پزشکی و بیماران، با تمرکز بر فرهنگ ایران (مانند کارگاه‌های محلی برای افزایش آگاهی در مناطق روستایی). این محور شامل کمپین‌های عمومی برای ترویج فرهنگ حفاظت داده است.[۵۷]

- نظارت و ارزیابی: مکانیسم‌های مداوم مانند بررسی سالانه و ارزیابی ریسک، با تشکیل شورای ملی اطلاعات سلامت در وزارت بهداشت ایران برای نظارت بر سیستم SIB.[۵۷]

مدل استراتژیک یکپارچه حفاظت از داده‌های سلامت الکترونیک در ایران (ISPDEH-IR) با پنج محور کلیدی طراحی شده است که هر یک خروجی‌های مشخصی را برای بهبود امنیت و حریم خصوصی در سیستم سلامت الکترونیک ایران به دنبال دارد. انتظار می‌رود چهارچوب قانونی و مقرراتی با تدوین قوانین کیفری متناسب با قانون جرایم رایانه‌ای ۱۳۸۸، جرایم سایبری در سیستم یکپارچه سلامت (SIB) را کاهش دهد. مدل‌های کنترل دسترسی مبتنی بر RBAC/ABAC از دسترسی غیرمجاز در بیمارستان‌های دولتی جلوگیری می‌کنند. استفاده از تکنولوژی‌های امنیتی مانند رمزنگاری و بلاکچین، حفاظت داده‌ها در برابر حملات سایبری را در زیرساخت‌های ضعیف ایران تقویت می‌کند. برنامه‌های آموزشی و آگاهی‌بخشی، رعایت قوانین حفاظت داده را در میان کادر پزشکی و بیماران، به‌ویژه در مناطق روستایی، ارتقا می‌دهند. در نهایت، نظارت و ارزیابی مستمر با تشکیل شورای ملی در وزارت بهداشت، بهبود مداوم امنیت سیستم SIB را تضمین می‌کند. این خروجی‌ها در مجموع به تقویت حریم خصوصی و کاهش نقض داده‌ها در ایران کمک می‌کنند.

جدول ۲. مدل استراتژیک پیشنهادی برای قوانین و الزامات کیفری پرونده‌های سلامت الکترونیک با تمرکز بر محرمانگی در ایران

چارچوب قانونی و مقرراتی	تدوین و به‌روزرسانی قوانین: تدوین قوانین جامع و به‌روزرسانی مداوم آنها برای حفاظت از اطلاعات سلامت الکترونیک ضروری است. این قوانین باید شامل مقررات سخت‌گیرانه برای حفاظت از محرمانگی و امنیت اطلاعات باشند.[۵۸]
	استانداردهای بین‌المللی: استفاده از استانداردهای بین‌المللی مانند ISO 13606 و HL7 برای تضمین یکپارچگی و امنیت اطلاعات[۵۹]
مدل‌های کنترل دسترسی	کنترل دسترسی مبتنی بر نقش (RBAC): استفاده از مدل‌های کنترل دسترسی مبتنی بر نقش برای محدود کردن دسترسی به اطلاعات حساس بر اساس نقش‌های مختلف در سیستم بهداشتی[۶۰]
	کنترل دسترسی اجباری (MAC): استفاده از مدل‌های کنترل دسترسی اجباری برای حفاظت از اطلاعات حساس و جلوگیری از دسترسی غیرمجاز[۶۱]
تکنولوژی‌های امنیتی	رمزنگاری: استفاده از تکنیک‌های رمزنگاری پیشرفته برای حفاظت از اطلاعات در حین انتقال و ذخیره‌سازی[۶۲]
	بلاک‌چین: استفاده از فناوری بلاک‌چین برای تضمین اصالت و یکپارچگی داده‌ها و جلوگیری از تغییرات غیرمجاز[۴۱]
آموزش و آگاهی‌بخشی	آموزش کارکنان: آموزش مداوم کارکنان بهداشتی در مورد اهمیت محرمانگی و امنیت اطلاعات و نحوه استفاده صحیح از سیستم‌هایEHR[۶۳]
	آگاهی‌بخشی به بیماران: اطلاع‌رسانی به بیماران در مورد حقوق آنها و نحوه حفاظت از اطلاعات شخصی‌شان[۶۴]
نظارت و ارزیابی	نظارت مستمر: ایجاد سیستم‌های نظارتی برای ارزیابی مداوم امنیت و محرمانگی اطلاعات و شناسایی و رفع نقاط ضعف[۶۵]
	ارزیابی ریسک: انجام ارزیابی‌های دوره‌ای ریسک برای شناسایی تهدیدات و آسیب‌پذیری‌های جدید و اتخاذ تدابیر مناسب برای مقابله با آن‌ها[۴۳]



شکل ۱. مدل استراتژیک پیشنهادی برای قوانین و الزامات کیفری پرونده‌های سلامت الکترونیک با تمرکز بر محرمانگی در ایران

برخورد می‌کنند، زیرا ماهیت این‌گونه جرائم ایجاب می‌کند که با همکاری بین‌المللی و اتخاذ سیاست‌های هماهنگ با آن‌ها مقابله شود. جمهوری اسلامی ایران با تصویب قانون جرائم رایانه‌ای در آغاز این مسیر قرار گرفته و تا رسیدن به هدف نهایی راه درازی پیش‌رو دارد. با توجه به این که شرع مقدس اسلام، برای حفظ حریم شخصی افراد توجه خاصی قائل شده است، مسئولان و قانون‌گذاران باید ضمن مطالعه قوانین کشورهای پیشگام در این عرصه، قوانین آن‌ها را منطبق با فرهنگ و معیارهای اسلامی حاکم بر کشور، بومی‌سازی کنند تا موانع موثری بر سر راه فرصت‌طلبانی که درصدد سودجویی یا هتک حیثیت افراد هستند، فراهم آید. اگرچه در سال ۱۳۸۷طی مصوبه شورای عالی سلامت، وزارت بهداشت درمان و آموزش پزشکی، موظف شده با همکاری سایر نهادهای مسئول، ظرف یک دوره ده ساله بسترهای اطلاعاتی مناسب را برای ارائه خدمات نوین به شهروندان ایجاد کند، اما برای رسیدن به اهداف فوق، علاوه برتدوین قوانین مستقل و پیوستن به مجامع بین‌المللی مبارزه با این جرایم، بودجه کافی نیز باید به این امر و

۴- نتیجه‌گیری

موضوع امنیت اطلاعات شخصی بیماران از دیرباز مورد توجه پزشکان بوده است که بارزترین نمونه آن سوگندنامه بقراط است. امروزه، با توجه به افزایش گسترده دسترسی به این اطلاعات که به‌ویژه با ایجاد پرونده‌های الکترونیکی سلامت میسر شده، اهمیت این موضوع دوچندان شده است. البته، مسائل دیگری نظیر رضایت، مسئولیت و حفظ حریم خصوصی در شرایط کنونی بسیار پیچیده‌تر از قبل شده و این امر لزوم وجود قوانین فنی و کیفری متناسب با این‌گونه موارد را بیش از پیش نمایان می‌کند. نمونه‌های بارز این مسأله را می‌توان در قوانین کشورهای پیشگام در حوزه سلامت الکترونیک نظیر کشورهای عضو اتحادیه اروپا، امریکا، کانادا، استرالیا، مالزی و غیره مشاهده کرد. کشورهای پیشگام در حوزه سلامت الکترونیک با تدوین سیاست‌ها و قوانین کیفری مناسب و عضویت در توافق‌نامه‌ها وکنوانسیون‌های بین‌المللی، ضمن مبارزه با مصادیق داخلی و خارجی، با این‌گونه جرائم نیز به شدت

جبران ناپذیری برای آن جامعه داشته باشد. مدل استراتژیک یکپارچه حفاظت از داده‌های سلامت الکترونیک در ایران (ISPDEH-IR) با شش محور کلیدی (چارچوب قانونی، رضایت و مالکیت داده‌ها، کنترل دسترسی، تکنولوژی‌های امنیتی، آموزش و آگاهی‌بخشی، و نظارت و ارزیابی) یک رویکرد جامع و بومی‌سازی‌شده برای حفاظت از حریم خصوصی و محرمانگی داده‌های سلامت ارائه می‌دهد. این مدل با تطبیق استانداردهای بین‌المللی مانند GDPR و ISO 18308 با شرایط ایران (مانند سیستم SIB و چالش‌های فرهنگی-قانونی)، به کاهش جرایم سایبری، افزایش اعتماد بیماران و بهبود امنیت پرونده‌های سلامت الکترونیک کمک می‌کند. پیاده‌سازی این مدل نیازمند همکاری بین وزارت بهداشت، قانون‌گذاران و نهادهای فناوری است تا نقض داده‌ها به حداقل برسد و حقوق فردی بیماران تضمین شود.

۵- شفافیت

۵-۱- تشکر و قدردانی

از تمامی افرادی که به‌صورت مستقیم وغیرمستقیم در بازخوانی و ویرایش اثر همیاری و راهنمایی داشتند، تشکر و قدردانی می گردد..

۵-۲- تعارض منافع

هیچ‌گونه تعارض منافع میان تهیه‌کنندگان این مقاله با حق‌های سلامت عمومی و قوانین و مقررات ملی و بین‌المللی مربوطه وجود ندارد.

۵-۳- منابع مالی

این پژوهش بدون تامین مالی خاصی انجام گرفته است.

۶-۴- ملاحظات اخلاقی

ملاحظات اخلاقی مربوط به انجام پژوهش رعایت شده است.

۵-۵- سهم نویسندگان

نویسندگان پژوهش، معیار های استاندارد نویسندگی مجلات نظام سلامت را رعایت نموده اند. همهٔ نویسندگان به‌طور برابر در نوشتن مقاله نقش داشتند.

۵-۶- استفاده از ابزارهای هوش مصنوعی

در تولید محتوای این مقاله از هیچ گونه ابزار هوش مصنوعی استفاده نشده است.

زمینه‌های مربوط به آن اختصاص یابد. هم اکنون که تعدادی از اساتید و کارشناسان خبره، در حال طراحی و تدوین قوانین کیفری مربوط به پرونده سلامت الکترونیک هستند، مطالعات تطبیقی و بهره‌گیری از الگوهای موفق در دنیا می‌تواند بسیار مفید باشد. علاوه بر این، به‌نظر می‌رسد به‌منظور موفقیت بیشتر در این مسیر، اتخاذ تمهیداتی به خصوص در زمینه فرهنگی ضروری می‌باشد. از جمله این موارد می‌توان به اطلاع‌رسانی به عموم مردم به‌منظور فرهنگ‌سازی در خصوص اهمیت موضوع، ارتقاء شیوه‌های امنیتی سیستم‌ها و تشویق آن‌ها به انجام این عمل و همچنین آگاه نمودن آن‌ها از عواقب کیفری تخلفات احتمالی اشاره کرد. ایمنی و حفاظت از اطلاعات پرونده الکترونیک سلامت یکی از ضروریات پیشرفت در استفاده از این فناوری می‌باشد و متاسفانه ایران فاقد الزامات جامعی در این زمینه می‌باشد. با توجه به سیاست‌های وزارت بهداشت، درمان و آموزش پزشکی بر ایجاد و توسعه پرونده الکترونیک سلامت برای هر ایرانی، طراحی و تدوین الزامات ایمنی و حفاظت پرونده الکترونیک سلامت بسیار حائز اهمیت است. بنابراین، استفاده از تجربیات و بهره‌گیری از الگوهای کشورهای پیشرو و موفق در این زمینه برای موفقیت ایران در انجام پروژه مذکور توصیه می‌گردد. استفاده از فناوری‌های نوین مانند هوش مصنوعی (AI) و بلاک‌چین می‌تواند به طور قابل توجهی امنیت و محرمانگی پرونده‌های سلامت الکترونیک (EHR) را بهبود بخشد. این فناوری‌ها با ارائه راهکارهای پیشرفته برای تحلیل داده‌ها، رمزنگاری و مدیریت دسترسی می‌توانند نقاط ضعف موجود در سیستم‌های فعلی را برطرف کنند و به بهبود کارایی و دقت در مدیریت اطلاعات سلامت کمک کنند. به علاوه قانون‌گذار باید مجازات در زمینه خدمات الکترونیک را به گونه‌ای تدوین نماید که مجازات نقدی در کنار مجازات کیفری بازدارندگی کافی را برای ناقضین داشته باشد. همچنین قانون حفاظت از داده‌های سلامت الکترونیک به صورت مجزا و مختص تخلفات حوزه سلامت تدوین گردد، تا مجازات سختگیرانه‌ای در این خصوص ارائه نماید چراکه اطلاعات سلامتی حاوی داده‌های بسیار مهمی از جوامع یک منطقه یا کشور است که دسترسی غیر قانونی و مجرمانه به آن‌ها می‌تواند عواقب سخت و

References

1. Fadahunsi KP, Akinlua JT, O'Connor S, Wark PA, Gallagher J, Carroll C, Majeed A, O'Donoghue J. Protocol for a systematic review and qualitative synthesis of information quality frameworks in eHealth. BMJ Open. 2019 Mar;9(3):e024722. doi: 10.1136/bmjopen-2018-024722.
2. Langabeer JR, Walji MF, Taylor D, Valenza JA. Economic outcomes of a dental electronic patient record. J Dent Educ. 2008;72(10):1189-200.
3. World Health Organization (WHO). e-Health, 2003. Available at: www.openclinical.org/e-Health.html
4. Zolait A, Radhi N, Alhowaishi MM, Sundram VPK, Aldoseri LM. Can Bahraini patients accept e-health systems? Int J Health Care Qual Assur. 2019;32(4):721.
5. Malek AL, Meisel JD. Privacy & information. Bloomberg Law Reports. 2008;1(2).
6. Ropes & Gray. Health care client alert. August 3, 2006. Available at: www.ropesgray.com.
7. Goodson JM. Foreign & comparative law. Research guides. J Michael Goodson Law Library, Duke University School of Law; 2008:1-2. Loi n° 88-19 du 5 janv. 1988 relative à la fraude informatique, JORF 6 janv.
8. The American Journal of Comparative Law. Introduction of Journal. 2009. Available at: http://comparativelaw.netapress.com.
9. Farhadi M, Haddad H, Shahriar H. Static analysis of HIPAA security requirements in electronic health record applications. In: 2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC); 2018 Jul 23; Vol. 2, pp. 474-479. IEEE.
10. Cahyani P, Astutik A. Criminal liability for misuse of electronic medical records in health services. Soepra J Hukum Kesehatan. 2019;5(2):215-23.
11. Aminpour F, Sadoughi F, Ahmadi M. Towards the application of open source software in developing national electronic health records: A narrative review article. Iran J Public Health. 2013 Dec;42(12):1333.
12. Miller N. Telemedicine legalities for physicians in PA. Physician's News Digest. 1999 Jun;3-4.
13. Gibbons JC. Thoughts on Crime and Punishment: MPSA annual national conference. 2008 Apr 3. Available at: www.allacademic.com/meta/p266011-Index.html.
14. Wachter GW. Malpractice and telemedicine liability: The uncharted waters of medical risk. Telemed.org. 2002 Jul. Available at: tie.telmed.org.
15. The National Academies Press. Privacy and security concerns regarding electronic health information. In: Protecting Electronic Health Information. 2009. Available at: www.nap.edu/openbook.php.
16. Lang Michener LLP. Privacy brief. 2008. Available at: www.langmichener.ca.
17. Recommendation R. of the Committee of Ministers to Member States on the protection of medical data.1997
18. Data PO. Directive 95/46/EC of the European parliament and of the council on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal L. 1995;281(23/11):0031-50.
19. Regulation P. Regulation (EU) 2016/679 of the European Parliament and of the Council. Regulation (eu). 2016 May;679(2016):10-3.
20. Council of Europe, Committee of Ministers. Recommendation No. R(97)5 on the protection of medical data. 1997 Feb 13. Available at: www.unmn.edu.
21. Assistance HC. Summary of the hipaa privacy rule. Office for Civil Rights. 2003.
22. Health Insurance Portability and Accountability Act (HIPAA). 29 Dec 2008. Available at: www.cms.hhs.gov/HIPAAAGENInfo/Downloads/HIPAA LAW.pdf.
23. Privacy Standard/Rule (HIPAA). 29 Dec 2008. Available at: www.privacy.med.miami.edu/glossary/xd-privacy-stds-huml
24. King R. Patient privacy. Business Week. 2009 Apr 8. Available at: www.zdentasia.com.
25. The National Law Journal. 2000 Jun 19. Available at: www.mosessinger.com.
26. Baker Donelson Health Law. Advisory. Stimulus package expands the applicability

and penalties of the HIPAA privacy and security regulations. 2009.
27. Minnesota Health Records Act. 29 Dec 2008. Available at: www.health.state.mu.us/e-health/mpsn/healthcordsact2007.
28. California Health Records Act. 1 Dec 2008. Available at: www.amendnews.com.
29. Forest D. Droit des données personnelles. Paris: Gualino, Lextenso; 2011. p. 117. Collection Droit en action. ISBN: 978-2-297-01502-8.
30. Gautrain V, Trudel P. Circulation des renseignements personnels et Web 2.0. Montréal: Université de Montréal, Édition Thémis; 2010. p. 231. ISBN: 978-2-89400-280.
31. Herveg J, Beyleveld D, Duguet AM. La protection des données médicales - The protection of medical data. In: Les défis du XXIe siècle - Challenges of the 21st century. Paris: LGDJ; Louvain-la-Neuve: Anthémis; 2008. p. 217.
32. Lavenue JJ, Beauvais G. La commercialisation des données personnelles, perspectives et prospective: l'exemple des données de santé et du DMP. In: La sécurité de l'individu numérisé. CNRS. Paris: L'Harmattan; 2009. p. 163.
33. Aghroum C. Personal communication. 2010. p. 33.8.
34. Eslamitabar S, Kebriaei A. Rules and regulations of drugs and medicines in Iran. Tehran: Naghsh Iran; 2008. (Persian).
35. Eslamitabar S, Elahimanesh M. Rules and regulations of medicines, drugs and health. 6th ed. Tehran: Majd Scientific and Cultural Association; 2008. (Persian).
36. Electronic Commerce Act. Iranian Islamic Parliament; 2008. (Persian).
37. Computer-Related Crimes. Iranian Islamic Parliament; 2008. (Persian).
38. Riazi H, Mohamadifar A, Moraveji SS. Electronic health records site. Deputy for R&D of Statistics and Information Technology Management, Ministry of Health; 2000. (Persian).
39. Eslamitabar S. Medical Law (4), New Approaches for Treatments and Health Officials' Responsibilities. Teb-Tazkieh. 2005;4(1):160-6. ISSN: 1608-2397.
40. Eslamitabar S. Medical Law (2), Necessity for Revision of Criminal Laws in Health and Related Occupations. Teb-Tazkieh. 2000;1(38):15-21. ISSN: 1608-2397.
41. Spector-Bagdady K, Mello MM. Protecting the privacy of reproductive health information after the fall of Roe v Wade. JAMA Health Forum. 2022 Jun 3;3(6):e222656.
42. Aliabad MB, Sadeghi N, Mokhtari-Payam M, Seddighi S, Ehsanzadehsorati SJ, Beygi FM. Establishment and utilization of electronic health records in Iran: A review of the policy documents of the past four decades. Shiraz E-Medical Journal. 2023 Jul 31;24(7).
43. Winter A, Takabayashi K, Jahn F, Kimura E, Engelbrecht R, Haux R, Honda M, Hübner UH, Inoue S, Kohl CD, Matsumoto T. Quality requirements for electronic health record systems. Methods Inform Med. 2017 Jan;56(S1):e92-104.
44. Asadi F, Moghaddasi H, Rabiei R, Rahimi F, Mirshekarlou SJ. The evaluation of SEPAS national project based on electronic health record system (EHRS) coordinates in Iran. Acta Informatica Medica. 2015 Dec;23(6):369-74.
45. Akhter Md Hasib KT, Chowdhury I, Sakib S, Monirujjaman Khan M, Alsufyani N, Alsufyani A, Bourouis S. [Retracted] Electronic Health Record Monitoring System and Data Security Using Blockchain Technology. Security and Communication Networks. 2022;2022:2366632.
46. Abbasi R, Khajouei R, Mirzaee M. Evaluating the demographic and clinical minimum data sets of Iranian National Electronic Health Record. BMC Health Serv Res. 2019 Dec;19(1):1-9.
47. Saraswat BK, Saxena A, Vashist PC. Machine learning techniques for analysing security practices in electronic health records. In: 2023 3rd International Conference on Technological Advancements in Computational Sciences (ICTACS); 2023 Nov 1; pp. 998-1005. IEEE.
48. Techapanupreed C, Kurutach W. Enhancing transaction security for handling accountability in electronic health records. Security and Communication Networks. 2020;2020:8899409.

49. Ganiga R, Pai RM, Sinha RK. Security framework for cloud-based electronic health record (EHR) system. Int J Electr Comput Eng. 2020 Feb 1;10(1):455-61.
50. Bohlander M. Principles of German Criminal Law. Oxford: Hart Publishing; 2009.
51. Dumortier J, Verhenneman G. Legal regulation of electronic health records: A comparative analysis of Europe and the US. In: eHealth: Legal, Ethical and Governance Challenges. Berlin, Heidelberg: Springer; 2012 Apr 16. p. 25-56.
52. Lee BS, Walker J, Delbanco T, Elmore JG. Transparent electronic health records and lagging laws. Ann Intern Med. 2016 Aug 2;165(3):219-20.
53. Ayat M. E-Health implementation challenges and HIS evaluation in accordance with EMRAM in Iran. Health Technol Assess. 2024 May 19;8(2).
54. Bashiri A, Shirdeli M, Niknam F, Naderi S, Zare S. Evaluating the success of Iran Electronic Health Record System (SEPAS) based on the DeLone and McLean model: A cross-sectional descriptive study. BMC Med Inform Decis Mak. 2023 Jan 17;23(1):10.
55. Soltanian D, Ghahari A. Comparative Study of Health Data Security under GDPR and HIPAA: Challenges and Implementation Opportunities in Iran. Health Law Journal. 2024 Jul 10;2(2):1-4.
56. Seiedfarajollah S; Safdari R; Ghazisaeedi M; Keikha L. Key security and privacy issues from implementing the National Electronic Health Record in the Islamic Republic of Iran. East Mediterr Health J. 2019;25(9):656–659. https://doi.org/10.26719/emhj.19.006
57. Rouzbahani F, Asadi F, Rabiei R, Moghaddasi H, Emami H. Developing a model for national health information governance program in Iran. Journal of Medicine and Life. 2020 Oct;13(4):510.
58. Farzandipour M, Ahmadi M, Sadoughi F, Karimi Irajk I. Adopting confidentiality principles for electronic health records in Iran: A Delphi study. J Med Syst. 2011 Jun;35:333-43.
59. Abbasi S, Ferdosi M. Do electronic health records standards help implement patient bill of rights in hospitals? Acta Informatica Medica. 2013 Mar;21(1):20-4.
60. Gajanayake R, Iannella R, Sahama T. Privacy-oriented access control for electronic health records. Electron J Health Inform. 2014;8(2):Article-number.
61. Alhaqbani B, Fidge C. Access control requirements for processing electronic health records. In: International Conference on Business Process Management; 2007 Sep 24; Berlin, Heidelberg: Springer; 2007. p. 371-82.
62. Terry NP, Francis LP. Ensuring the privacy and confidentiality of electronic health records. U Ill L Rev. 2007:681-702.
63. Shenoy A, Appel JM. Safeguarding confidentiality in electronic health records. Camb Q Healthc Ethics. 2017 Apr;26(2):337-41.
64. Bayer R, Santelli J, Klitzman R. New challenges for electronic health records: Confidentiality and access to sensitive health information about parents and adolescents. JAMA. 2015 Jan 6;313(1):29-30.
65. Keikha L, Farajollah SS, Safdari R, Ghazisaeedi M, Mohammadzadeh N. Development of hospital-based data sets as a vehicle for implementation of a national electronic health record. Perspect Health Inf Manag. 2018;15(Winter):1-9.