



A Reflection on the Privacy and Confidentiality of Electronic Health Records in U.S. and Iranian Law

Abbas Mirshekari

Associate Professor, Faculty of Law and Political Science, University of Tehran, Tehran, Iran

mirshekariabbas1@ut.ac.ir

Shobeir Azadbakht

Ph.D. Candidate of Private Law, Faculty of Law and Political Science, Allame Tabataba'i University, Tehran, Iran

shobeir_azadbakht95@atu.ac.ir

Abstract

Modern technologies have significantly penetrated various aspects of human life, to the extent that the adoption of technology-driven innovations in different societies and systems has become inevitable. One of these areas is the healthcare system, which has been moving toward the implementation of Electronic Health Records (EHRs). In this regard, several fundamental questions arise: first, what are the advantages and disadvantages of using electronic health records? Second, what protective measures exist to safeguard these records? Third, how are issues of privacy and confidentiality of health record information reflected in the legal systems of the United States and Iran? The conducted studies indicate that despite the significant and considerable benefits of implementing electronic health records, the main challenge lies in issues related to privacy and the confidentiality of the information contained in them. Nevertheless, Western scholars, as well as the U.S. legal system, have adopted measures to protect these records, including administrative or managerial safeguards, technical safeguards, and finally physical safeguards. Despite this, the Iranian legal system remains largely silent regarding security and protective policies governing electronic health records. More precisely, there is no specific framework addressing this issue. Therefore, the aim of this paper is to answer the aforementioned questions, through an analytical-descriptive method and with a comparative perspective drawing on the achievements of U.S. law.

Keywords:

Health Information, Electronic Medical Record (EMR), Personal Health Record (PHR), Technology, Security

How To Cite:

Mirshekari, A., & Azadbakht, S. (2026). A reflection on the privacy and confidentiality of electronic health records in U.S. and Iranian law. *Health Law and Policy*, 1(1), pp. 113-145.

Received: 18/06/2026

Received in revised form: 12/08/2026

Accepted: 26/08/2026

Published online:



تأملی در حریم خصوصی و محرمانگی پرونده الکترونیک سلامت در حقوق امریکا و ایران

دریافت: ۱۴۰۵/۰۳/۲۸
بازنگری: ۱۴۰۵/۰۵/۲۱
پذیرش: ۱۴۰۵/۰۵/۲۵
انتشار برخط:

■ mirshekariabbas1@ut.ac.ir

■ shobeir_azadbakht95@atu.ac.ir

✉ عباس میرشکاری

شیر آزادبخت

فناوری‌های نوین به عرصه‌های مختلف زندگی بشر به طور جدی نفوذ کرده‌اند؛ تا آنجا که پذیرش نوآوری‌های فناورمحور در جوامع و نظامات مختلف اجتناب‌ناپذیر شده است. یکی از این عرصه‌ها نظام سلامت است که به سمت استقرار پرونده‌های الکترونیک سلامت سوق پیدا کرده است. در این خصوص چند سؤال اساسی قابل طرح است: ۱. مزایا و معایب بهره‌گیری از پرونده الکترونیک سلامت چیست؟ ۲. تدابیر حفاظتی برای صیانت از این پرونده‌ها کدام‌اند؟ ۳. مباحث حریم خصوصی و محرمانگی اطلاعات پرونده‌های سلامت به چه صورت در نظام حقوقی امریکا و ایران منعکس شده است؟ بررسی‌های صورت‌پذیرفته مؤید آن بود که با وجود مزایای جدی و قابل توجه به کارگیری پرونده‌های الکترونیک سلامت چالش اصلی در مباحث مربوط به حریم خصوصی و محرمانگی اطلاعات مندرج در آن‌ها نهفته است. البته، اندیشمندان غربی و همچنین نظام حقوقی امریکا تدابیری را برای صیانت از این پرونده‌ها به کار گرفته‌اند که عبارت‌اند از حفاظت‌های مدیریتی یا اداری و فنی و در آخر فیزیکی. با وجود این، نظام حقوقی ایران در زمینه سیاست‌های امنیتی و حفاظتی ناظر بر پرونده‌های الکترونیک سلامت ساکت است. به عبارت دقیق‌تر، چارچوب خاصی برای این موضوع وجود ندارد. از این رو، رسالت این نوشتار آن است که به شیوه تحلیلی-توصیفی و با نگاهی تطبیقی به دستاوردهای حقوق امریکا تا جای ممکن به پرسش‌های یادشده پاسخ دهد.

واژگان کلیدی:

اطلاعات سلامت، امنیت، پرونده الکترونیک پزشکی، پرونده شخصی سلامت، فناوری.

استناد:

میرشکاری، عباس، و آزادبخت، شیر (۱۴۰۵). تأملی در حریم خصوصی و محرمانگی پرونده الکترونیک سلامت در حقوق امریکا و ایران. *فلسفه و سیاست‌گذاری سلامت*، ۱۱(۱)، صص ۱۱۳-۱۴۵.

۱. دانشیار گروه حقوق خصوصی و اسلامی دانشکده حقوق و علوم سیاسی دانشگاه تهران، تهران، ایران.
۲. دانشجوی دکتری حقوق خصوصی، دانشکده حقوق و علوم سیاسی، دانشگاه علامه طباطبائی (ره)، تهران، ایران.

مقدمه

اشخاص، اعم از زنده یا مرده، دارای اطلاعات پزشکی هستند. ایشان در زمان حیات برای معالجه به پزشک مراجعه می‌کنند و در این صورت، برای طی شدن صحیح فرایند درمان، اطلاعات مربوط به بیماری خود را برای پزشک بازگو می‌کنند. در نتیجه این ارتباط، پزشک اطلاعات پزشکی مربوط به ایشان را جمع‌آوری می‌کند. همچنین، احتمال دارد اطلاعات پزشکی متوفا را کادر درمان گردآوری کند. این گردآوری ممکن است در زمان حیات شخصی باشد که اکنون فوت کرده یا در همان زمان فوت شخص (مثلاً از طریق پزشکی قانونی). در گذشته (حتی در بعضی از کشورها در حال حاضر) این اطلاعات به صورت سنتی و غیر الکترونیکی و در واقع در کاغذ ذخیره می‌شد. امروزه، به دلیل رسوخ روزافزون فناوری در زندگی بشر، نظام سلامت و بهداشت کشورهای مختلف به سمت ذخیره‌سازی و انتقال الکترونیکی اطلاعات پزشکی حرکت کرده است (Carter, 1999, p. 223). به عبارت بهتر، از طریق بهره‌گیری از فناوری‌های نوین، پرونده سلامت که حاوی اطلاعات پزشکی اشخاص است در نظام سلامت کشورهای جهان در حال شکل‌گیری و توسعه است. مثلاً، رئیس‌جمهور وقت ایالات متحده آمریکا (جورج دابلیو بوش) در سال ۲۰۰۴ بیان داشت طی یک برنامه ده‌ساله باید غالب شهروندان آمریکایی پرونده سلامت داشته باشند. در ایران نیز، در بند «ه» ماده ۸۸ قانون چهارم برنامه توسعه اقتصادی، اجتماعی، و فرهنگی (۱۳۸۴ تا ۱۳۸۸) وزارت بهداشت موظف به طراحی و استقرار نظام جامع اطلاعات سلامت ایرانیان شده بود. این دو مثال نشان‌دهنده توجه کشورها به ثبت و ضبط الکترونیکی اطلاعات پزشکی و در واقع استفاده از فناوری‌های جدید در عرصه سلامت و پزشکی است.

این موضوع، یعنی رواج بیش از پیش پرونده الکترونیک سلامت، با وجود منافع بی‌نظیر یا حداقل کم‌نظیر خود، چالش‌هایی را در خصوص حریم خصوصی و محرمانگی اطلاعات پزشکی در نظام‌های حقوقی مختلف ایجاد کرده است. البته، ظهور این چالش‌ها طبیعی است. در حقیقت، قاعدتاً حفاظت و صیانت از اطلاعات پزشکی در شیوه سنتی (کاغذی) بسیار ساده‌تر از شیوه الکترونیکی آن است. دیگر آن روزها که پرونده و سوابق پزشکی صرفاً در اختیار بیماران بود و هنگام مراجعه به پزشک خود بیمار آن را برای پزشک آشکار می‌کرد گذشته است. این اطلاعات در دنیای مغروق در تکنولوژی امروز منحصرراً در اختیار بیماران نیست و با توجه به اینکه اطلاعات پزشکی در یک سیستم مرکزی مربوط به پرونده‌های پزشکی جمع‌آوری می‌شود به راحتی توسط اپراتورهای این سیستم‌ها یا حتی در مواردی توسط کادر درمان قابل مشاهده و استخراج است. بنابراین، دسترسی به سوابق پزشکی بسیار ساده‌تر از زمان‌های گذشته شده و این دسترسی سهل‌تر مشکلات عدیده‌ای را به لحاظ حفاظت از اطلاعات پزشکی ایجاد کرده است. با این اوصاف، مذاقه در حریم خصوصی و محرمانگی اطلاعات پزشکی، اعم از سنتی و الکترونیکی، نامعقول نیست؛ بلکه یک نیاز و الزام ضروری است.^۱

۱. اهمیت دیگر بررسی این موضوع را می‌توان در زیان ناشی از نقض حریم خصوصی و محرمانگی جست‌وجو کرد. در حقیقت «زیان‌های ناشی از نقض محرمانگی سوابق پزشکی ماهیت متفاوت دارند. پرونده‌های پزشکی مشتمل بر اطلاعاتی مانند بیماری‌های قلبی، بیماری‌های لاعلاج، خشونت‌های خانگی، ... درمان روان‌پزشکی، ... بیماری‌های مقاربتی و حتی

بر این بنیاد، چند پرسش اساسی قابل طرح است: ۱. پرونده الکترونیک سلامت چیست و انواع آن کدام است؟؛ ۲. مزایا و محاسن به کارگیری این پرونده در نظام سلامت به چه ترتیب است؟؛ ۳. راهکارهای صیانت از پرونده الکترونیک سلامت چیست؟؛ ۴. نظام‌های حقوقی امریکا و ایران برای صیانت از حریم خصوصی بیماران و محرمانگی پرونده الکترونیک سلامت چه اقداماتی را انجام داده‌اند؟ و ۵. آیا وجود پرونده الکترونیک سلامت در نظام‌های حقوقی امریکا و ایران الزامی است؟ رسالت این نوشتار آن است که به شیوه تحلیلی-توصیفی و البته تطبیقی به سؤالات یادشده پاسخ دهد.

پژوهشگران حقوقی امریکا حدوداً از سه دهه پیش شروع کردند به عرضه نتیجه مطالعات خود در زمینه حریم خصوصی و محرمانگی اطلاعات پزشکی که در بستر فناوری‌های نوین جمع‌آوری شده‌اند (Shenoy & Appel, 2017; Glenn, 2000; Bomash, 2008; Terry, 2012; Bayer et al., 2015; 29-30). برعکس، در حقوق ایران صرفاً به محرمانگی اطلاعات پزشکی و حریم خصوصی بیماران از منظر روابط پزشک-بیمار پرداخته شده است، نه اینکه اثر فناوری در این زمینه‌ها بررسی شود (نوری یوشانلوئی و آزادبخت، ۱۴۰۱؛ میرشکاری و آزادبخت، ۱۴۰۱، صص. ۲۷۸-۲۷۹؛ آسمانی و ابراهیمی، ۱۳۹۲؛ پرویز و احتشام، ۱۳۹۷).^۱ بنابراین، وجه تمایز این نوشتار با مباحث پیشین را می‌توان در چند مورد خلاصه کرد: اول آنکه مزایا و معایب به کارگیری فناوری در خصوص اطلاعات پزشکی در مباحث حقوقی ایران مطالعه نشده است که در این مقاله به آن پرداخته می‌شود؛ دوم اینکه راهکارهای صیانت از پرونده الکترونیک پزشکی به نحو مختصر بیان می‌شود؛ سوم اینکه رویکرد نظام‌های حقوقی به لحاظ اجباری یا اختیاری بودن پرونده الکترونیک سلامت معرفی می‌شود؛ و در آخر، موضوع از منظر حقوق امریکا به صورت تطبیقی بررسی می‌شود.

بنا بر مطالب یادشده، در گام نخست به تشریح برخی مفاهیم، مانند پرونده الکترونیک سلامت، پرداخته می‌شود. در گام بعد، محاسن و معایب به کارگیری پرونده‌های الکترونیک سلامت معرفی می‌شود. سپس، در خصوص شیوه‌های حفاظت از پرونده‌های الکترونیک سلامت توضیحاتی ارائه می‌شود. و در آخر، موضع نظام حقوقی امریکا و ایران در خصوص حریم خصوصی و محرمانگی اطلاعات پزشکی مندرج در پرونده الکترونیک سلامت بررسی می‌شود.

۱. مفاهیم

شناخت و احاطه دقیق بر هر موضوعی مستلزم فهم دقیق مفاهیم به کاررفته در آن موضوع است. هنگامی که از پرونده الکترونیک سلامت و مباحث حریم خصوصی و محرمانگی اطلاعات پزشکی صحبت می‌شود،

تجاوز و ... هستند. افشای این اطلاعات می‌تواند شغل، روابط دوستی، و حتی روابط زناشویی ما را تحت تأثیر قرار دهد» (Terry, 2014, p. 65). بنابراین، برای جلوگیری از افشای اطلاعات و نقض بی‌مورد حریم خصوصی بیماران، که ضررهایی با ماهیت متفاوت و آثار دامنگیر ایجاد می‌کنند، مطالعه حریم خصوصی بیماران و محرمانگی اطلاعات پزشکی اهمیت دارد (همچنین ن. ک.: Miller, 2008, p. 353).

۱. برای مطالعه بیشتر در خصوص مالیت و مالکیت پرونده‌های الکترونیک سلامت ر. ک.: میرشکاری و همکاران، ۱۴۰۳.

باید ابتدا این مفاهیم را تعریف و سپس چالش مربوط به حریم خصوصی بیماران و محرمانگی اطلاعات پزشکی در پرونده‌های الکترونیک سلامت را بررسی کرد. بدین منظور، ابتدا مفهوم پرونده الکترونیک سلامت و تمایز آن با برخی مفاهیم مشابه و اقسام آن معرفی و در قسمت بعد منظور از حریم خصوصی بیماران و مرز میان این مفهوم با محرمانگی اطلاعات پزشکی بیان می‌شود.

۱-۱. پرونده الکترونیک سلامت و اقسام آن

بر اساس تعریف مراکز خدمات پزشکی و پرداخت هزینه‌های پزشکی^۱ (زیرمجموعه وزارت بهداشت و خدمات انسانی^۲ ایالات متحده آمریکا) پرونده الکترونیک سلامت^۳ عبارت است از «یک نسخه الکترونیکی از سوابق پزشکی بیمار که ارائه‌دهنده خدمات پزشکی در طول زمان نگهداری می‌کند و ممکن است شامل همه داده‌های اداری و بالینی کلیدی (از جمله اطلاعات جمعیتی، یادداشت‌های پیشرفت، مشکلات، داروها، نشانه‌های حیاتی، سوابق پزشکی گذشته، ایمن‌سازی، داده‌های آزمایشگاهی، گزارش‌های رادیولوژی) مربوط به مراقبت از آن فرد زیر نظر یک ارائه‌دهنده به خصوص باشد» (Centers for Medicare & Medicaid Services, Electronic Health Records, 2023). بنا بر این تعریف، همه اطلاعات مربوط به سلامت افراد که برخی از ارائه‌دهندگان خدمات پزشکی، مانند بیمارستان‌ها، به صورت الکترونیکی ذخیره می‌کنند در قلمرو مفهومی پرونده الکترونیک سلامت قرار می‌گیرد. این اطلاعات، همان‌طور که در تعریف نیز آمده، منحصر به موارد یادشده نیست و به طور تمثیلی بیان شده است. افزون بر اطلاعات اختصاصی پزشکی، مواردی مانند مشخصات هویتی افراد (مانند کد ملی و ...) نیز در این سوابق درج می‌شود (Turk, 2015, p. 565). در تعریف دیگری گفته‌اند پرونده الکترونیک سلامت «مجموعه‌ای از اطلاعات الکترونیک سلامت است که در طول زمان درباره بیماران گردآوری شده است.» (Kruser, 2007, p. 317). در تعریف دیگری، وزارت بهداشت، درمان، و آموزش پزشکی ایران بیان داشته: «پرونده الکترونیک سلامت مجموعه اطلاعات مرتبط با رویدادهای سلامت شهروندان، از پیش از تولد تا پس از مرگ، است که به صورت مداوم و با گذشت زمان به شکل الکترونیکی ذخیره می‌گردد. این اطلاعات منحصراً در اختیار و مالکیت صاحب پرونده و تنها در صورت اجازه فرد و با رعایت قواعد محرمانگی و حریم خصوصی در اختیار افراد مجاز قرار خواهد گرفت» (وزارت بهداشت، درمان، و آموزش پزشکی ایران، ۱۳۹۸-۱۴۰۰، ص. ۳۴).

با عنایت به این تعاریف، هدف از ایجاد پرونده‌های الکترونیک سلامت ذخیره‌سازی و انتقال الکترونیکی «اطلاعات مربوط به سلامت»^۴ اشخاص است. منظور از اطلاعات مربوط به سلامت «هر اطلاعاتی است که به وضعیت پزشکی اشخاص مربوط می‌شود و شخصی است؛ یعنی همه واقعیات، ارتباطات، یا نظرات که به فرد مربوط می‌شود و معقول است که او درباره آن‌ها حساس باشد و در نتیجه بخواهد که جمع‌آوری،

1. Centers for Medicare and Medicaid Services (CMS)

2. Department of Health & Human Services (HHS)

3. Electronic Health Record (EHR)

4. Health Information (HI)

استفاده، یا انتشار آن‌ها را منع یا محدود کند» (Sperling, 2008, p. 187). همچنین، داده‌های مربوط به سلامت در بند ۱۵ ماده ۴ مقررۀ عمومی حفاظت از داده‌های اتحادیه اروپا (مصوب ۲۰۱۶) چنین تعریف شده است: «به داده‌های شخصی مرتبط با سلامت جسمی یا روانی یک شخص حقیقی اطلاق می‌شود که شامل داده‌های مربوط به ارائه خدمات مراقبت‌های بهداشتی و بیانگر اطلاعاتی درباره وضعیت سلامت اوست»^۱.

با این حال، اصطلاحات دیگری مانند «پروندۀ الکترونیک پزشکی»^۲ و «پروندۀ شخصی سلامت»^۳ در این عرصه مطرح شده است که نباید پروندۀ الکترونیک سلامت را با این موارد خلط کرد. پروندۀ الکترونیک سلامت و پروندۀ الکترونیک پزشکی^۴ به لحاظ بستر ایجاد (فضای الکترونیکی) یکسان‌اند؛ اما، از حیث دامنه اطلاعات و نحوه دسترسی به داده‌ها با یکدیگر تفاوت دارند. پروندۀ الکترونیک پزشکی به نسخه دیجیتالی سوابق درمانی بیمار در یک مرکز یا نزد یک ارائه‌دهندۀ خدمات سلامت خاص اطلاق می‌شود که معمولاً در همان مرکز ایجاد و نگهداری شده و عمدتاً برای استفاده همان ارائه‌دهندۀ طراحی شده است. از این رو، اطلاعات موجود در این نوع پرونده غالباً محدود به خدمات ارائه‌شده در همان مرکز است و امکان تبادل گسترده آن با سایر مراکز درمانی به صورت نظام‌مند وجود ندارد. در مقابل، در پروندۀ الکترونیک سلامت، قابلیت «همکاری و هماهنگی»^۵ وجود دارد. این اصطلاح در حوزه فناوری اطلاعات به معنی توانایی سیستم‌ها و برنامه‌های کاربردی مختلف برای تبادل داده‌ها و اطلاعات با یکدیگر و به‌کارگیری آن‌ها در کنار هم، بدون مشکل و دردسر، است. به عبارت دیگر، در پروندۀ الکترونیک سلامت قابلیت همکاری بین سامانه‌ها و برنامه‌ها و دستگاه‌های مختلف به منظور انتقال و تبادل اطلاعات و داده‌ها در سیستم‌های مختلف و در شبکه‌های مختلف است (Bauer, 2009, p. 47). همچنین، تفاوت میان پروندۀ الکترونیک سلامت با پروندۀ شخصی سلامت در کنترل‌کنندۀ اطلاعات سلامت است؛ بدین توضیح که در پروندۀ شخصی سلامت خود بیمار اطلاعات سلامت خود را به صورت الکترونیکی مدیریت می‌کند و در واقع مسئول این اطلاعات خود اوست (Terry & Francis, 2007, p. 681). بیمار است که تصمیم می‌گیرد چه اطلاعاتی در پرونده وارد شود، باقی بماند، تغییر کند، اصلاح شود، یا خارج شود. این در حالی است که در پروندۀ الکترونیک سلامت ارائه‌دهندگان خدمات سلامت یا اشخاصی که قانون معین می‌کند متولی و عهده‌دار سامانه‌های ذخیره‌سازی پرونده‌های الکترونیک می‌شوند؛ یعنی مسئول نگهداری شخصی غیر از بیمار است. بدیهی است حریم خصوصی و محرمانگی اطلاعات پزشکی در این مدل از پرونده‌های سلامت بیشتر از پرونده‌های الکترونیک سلامتی است که سایر اشخاص (از جمله کادر درمان و به طور کلی

1. General Data Protection Regulation (Gdpr): 'Data Concerning Health' Means Personal Data Related to the Physical or Mental Health of a Natural Person, Including the Provision of Health Care Services, Which Reveal Information About His or Her Health Status.

2. Electronic Medical Record (EMR)

3. Personal Health Record (PHR)

4. See: Bomash, 2008, p. 119.

5. Interoperability

6. Also See: Francis, 2011, pp. 173-174.

ارائه دهندگان خدمات پزشکی) به آن دسترسی دارند.

اندیشمندان پرونده‌های الکترونیک سلامت را حداقل به دو دسته تقسیم کرده‌اند: «نسخه ابری»^۱ یا «مبتنی بر وب»^۲ و «نسخه محلی»^۳ یا «سرور مشتری»^۴. در نسخه ابری یا مبتنی بر وب اطلاعات موجود در پرونده سلامت از طریق مرورگرهای وب، به صورت برخط، قابل دسترسی است و نیازی به نصب نرم‌افزار خاص برای دسترسی به پرونده‌های سلامت نیست. برعکس، در نسخه محلی یا سرور مشتری باید نرم‌افزار مربوط به ذخیره‌سازی و انتقال اطلاعات سلامت خریداری و در سیستم رایانه‌ای مشتری نصب شود. نسخه محلی گران‌تر از نرم‌افزارهای مبتنی بر ابر هستند. چون مراکزی که سرورهای محلی را اجرا می‌کنند کل هزینه راه‌نگام خرید نرم‌افزار پرداخت می‌کنند، به استثنای هزینه‌های سالیانه نگهداری؛ درحالی‌که در نرم‌افزار مبتنی بر ابر هزینه نگهداری در هزینه ماهیانه منظور می‌شود و مبلغ کمتری اخذ می‌شود (Turk, 2015, pp. 573-574).

۲-۱. تمایز حریم خصوصی از محرمانگی اطلاعات پزشکی

مفهوم حریم خصوصی^۵ و محرمانگی (در معنای خاص) به حدی به یک‌دیگر شباهت دارند که در برخی نوشته‌ها به اشتباه این دو را یکسان در نظر می‌گیرند و به جای هم استفاده می‌کنند (Gostin, 1997, p. 688)؛^۶ گویی مقصود از دو عبارت یک موضوع است و رابطه این‌همانی (تساوی) میان دو اصطلاح وجود دارد. با وجود این شباهت‌ها، این تصور را باید از ذهن زدود. در توضیح این تمایز، اشاره به حقوق انگلیس ضروری به نظر می‌رسد. در حقوق انگلیس ارکان مفهوم محرمانگی اطلاعات در دعوی کوکو (Coco v. AN Clarke (Engineers) Ltd, 1968)) بیان شده است. بر این بنیاد، در دعوی مسئولیت مدنی ناشی از نقض محرمانگی باید سه شرط وجود داشته باشد: ۱. اطلاعات مورد افشا ماهیت محرمانه داشته باشد؛ ۲. این اطلاعات در شرایطی ردوبدل شده باشد که نوعی تعهد به رازداری را تحمیل کند (یعنی یک رابطه قبلی مبنی بر اعتماد و اطمینان میان طرفین وجود داشته باشد، مانند اطلاعات بیمار که به پزشک داده می‌شود)؛ و ۳. اطلاعات یادشده بدون مجوز و به ضرر شخص صاحب اطلاعات استفاده شده باشد (Cooke, 2007, p. 437).

با این اوصاف می‌توان گفت بنیان مفهوم محرمانگی اطلاعات بر مبنای یک رابطه مبتنی بر اعتماد و اطمینان است. به عبارت بهتر، زمانی یک اطلاعات محرمانه تلقی می‌شود که شخصی، به دلیل یک رابطه مبتنی بر اعتماد، اطلاعاتی را در اختیار شخص دیگر قرار دهد و بنای صریح یا ضمنی طرفین آن باشد که این اطلاعات بدون رضایت اطلاعات‌دهنده در اختیار اشخاصی خارج از این رابطه قرار نگیرد. بنابراین، در صورتی که این رابطه میان طرفین وجود نداشته باشد، دیگر نمی‌توان از محرمانه بودن اطلاعات و تکلیف به رازداری صحبت کرد. وانگهی، حوزه بحث از محرمانگی اطلاعات هنگام افشای اطلاعات است

1. Cloud-Based
2. Web-Based
3. On-Premise
4. Client Server

۵. برای مطالعه مفهوم حریم خصوصی ر.ک.: سلمانلو، ۱۳۹۸، صص. ۵۷-۶۶.

۶. ر.ک.: محسنی، ۱۳۹۴، ص. ۴۲۱.

نه جمع‌آوری آن. برخلاف این توضیحات، حریم خصوصی صرفاً به معنای قدرت شخص بر عدم افشای اطلاعات از پیش انتقال یافته نیست؛ بدین معنا که حریم خصوصی هم در زمان جمع‌آوری اطلاعات اشخاص هم در زمینه افشای این اطلاعات حاکم است، منتها در این موقعیت دیگر رابطه‌ای که مبتنی بر اعتماد و اطمینان باشد میان طرفین وجود ندارد.^۱ بیان مثالی می‌تواند موضوع را روشن‌تر کند. در زمان مراجعه بیمار به پزشک، بیمار ناچار با هدف درمان باید اطلاعات مربوط به بیماری خود را برای پزشک بازگو کند. این مرحله که بیمار این اطلاعات را مطرح می‌کند یا اجازه کسب اطلاعات را به پزشک از طریق معاینه می‌دهد، به معنای آن است که بیمار از حریم خصوصی خودش صرف‌نظر کرده است؛ یعنی، در این مرحله قواعد حریم خصوصی حاکم است. پس از جمع‌آوری اطلاعات توسط پزشک و به دست آوردن اطلاعات محرمانه مربوط به بیمار، افشا یا عدم افشای این اطلاعات تحت شمول مفهوم محرمانگی قرار می‌گیرد. به عبارت دیگر، حریم خصوصی حاکم بر مرحله کسب اولیه اطلاعات (زیرا هنوز رابطه مبتنی بر اعتماد شکل نگرفته است) و محرمانگی حاکم بر بازنشر اطلاعات (زیرا رابطه مبتنی بر اعتماد در این زمان شکل می‌گیرد) از پیش جمع‌آوری شده است (Rothstein, 2007, p. 489; Bauer, 2009, p. 50). برخی اندیشمندان تفاوت این دو مفهوم را بدین شکل به تصویر کشیده‌اند: «فقط در صورتی حق محرمانگی یک فرد نقض می‌شود که شخص یا نهادی که اطلاعات به صورت محرمانه به آن‌ها اعلام شده نتواند این اطلاعات را محافظت کند یا آن‌ها را بدون موافقت طرف اول، عمداً، برای شخص دیگری افشا کند. در مقابل، فردی که بدون اجازه وارد اتاق سوابق بیمارستان یا پایگاه داده کامپیوتری می‌شود حقوق حریم خصوصی را نقض می‌کند؛ اما حقوق مرتبط با محرمانگی را نقض نمی‌کند. فقط شخص یا نهادی که در یک رابطه محرمانه اطلاعات را دریافت کرده است می‌تواند متهم به نقض حقوق محرمانگی [اطلاعات] شود» (Terry, 2017, p. 151).

البته، تفاوت میان این دو مفهوم به گواه دیگر محققان منحصر در این موارد نیست. در حقیقت، شخص زیان‌دیده از نقض حریم خصوصی در صورتی می‌تواند علیه ناقض اقامه دعوا کند که اثبات کند افشای اطلاعات مربوط به او در نظر یک انسان معقول و متعارف (معیار نوعی) توهین‌آمیز بوده است و این در حالی است که در دعوای نقض محرمانگی اطلاعات صرف افشای اطلاعات، صرف نظر از اینکه تا چه حد توهین‌آمیز باشد، برای ناقض موجد مسئولیت است (انصاری، ۱۴۰۰، صص. ۹۱-۹۲). افزون بر این، معیاری که در این دعوا به کار گرفته می‌شود شخصی است؛ یعنی همین که خواهان دچار تألمات روحی-روانی شود و از افشای اطلاعات پزشکی‌اش احساس شرمندگی کند، با وجود اینکه در نظر انسان معقول افشای اطلاعات وی شرم‌آور نباشد، او می‌تواند علیه خوانده به دلیل نقض محرمانگی اقامه دعوا کند (Winn, 2001, p. 617).

۲. محاسن و معایب استفاده از پرونده الکترونیک سلامت

بهره‌گیری از پرونده‌های الکترونیک سلامت، مانند هر فناوری نوظهور دیگر، دارای محاسن و معایبی است

۱. مانند اینکه اطلاعات پزشکی شخص را کسی در خیابان پیدا کند. در این مثال، مفهوم حریم خصوصی حاکم است؛ بدین معنا که در صورت افشای این اطلاعات، نقض حریم خصوصی رخ داده است، نه نقض محرمانگی اطلاعات پزشکی.

که باید پیش از استقرار گسترده آن بررسی شود. از این رو، نخست مزایای به کارگیری پرونده الکترونیک سلامت، سپس معایب آن، و در پایان تحلیل این ادله عرضه خواهد شد.

۱-۲. محاسن

استفاده از پرونده الکترونیک سلامت منجر به کارآمدی هر چه بیشتر در نظام سلامت می شود. پزشکان و به طور کلی کادر درمان مرتبط با معالجه بیماری یک شخص، با توجه به عدم محدودیت مکانی، به اطلاعات سلامت مراجعه کنندگان دسترسی آبی و بدون دردسر دارند. این اشخاص به راحتی می توانند آزمایش ها، نسخه ها، اظهارات گذشته خود بیمار، نظریات و دیدگاه های سایر پزشکان را مشاهده کنند و با توجه به مجموعه این مستندات و مدارک به معالجه بیماری شخص اقدام کنند. از سوی دیگر، در سیستم سنتی ذخیره سازی اطلاعات سلامت ممکن است، با توجه به انباشت کاغذهای مربوط به اطلاعات سلامت، برخی مستندات به هر دلیلی مفقود شود. این وضعیت باعث می شود خطاهای پزشکی بیشتر و همچنین فرایند درمان طولانی شود. به بیان روشن تر «سیستم کاغذی اغلب منجر به اطلاعات نادرست، ناقص، نابهنگام، پراکنده، و تکراری شده است. سهولت جمع آوری، سازمان دهی، نگهداری، و تبادل اطلاعات شخصی، که به وسیله یک سیستم ذخیره سازی الکترونیک اطلاعات مراقبت های بهداشتی امکان پذیر شده، ممکن است ناکارآمدی و عدم دقت سیستم سنتی ذخیره سازی کاغذی را از بین ببرد» (Steward, 2005, p. 497). یکی دیگر از آثار استقرار پرونده های الکترونیک صرفه جویی است. این صرفه جویی دو بعد زمانی و مالی دارد (Carter, 1999, pp. 232-233). دسترسی به اطلاعات پزشکی اشخاص صرفاً با وارد کردن مشخصات آنها در سامانه ممکن است. بنابراین، هنگامی که با این سرعت بتوان به اطلاعات پزشکی بیماران دسترسی داشت، طبیعی است در زمان صرفه جویی می شود. روی دیگر سکه صرفه جویی در هزینه هاست. مثلاً، لازم نیست بیمار برای نشان دادن آزمایش های خود به پزشک حتماً به مطب وی مراجعه کند؛ می تواند با دادن مشخصات خود، برای ورود به پرونده الکترونیک سلامت، پزشک را از آزمایش های ذخیره شده آگاه کند یا هنگامی که خطای پزشکی از طریق کاربرد پرونده الکترونیک کاهش یابد بدیهی است هزینه های رفع آن خطا نیز کاهش می یابد. وانگهی، یکی از هزینه های سرسام آور در این زمینه رونوشت گرفتن از مستندات مربوط به سلامت برای ارائه به پزشک ها یا بیمارستان های متفاوت است. کاهش هزینه ها منحصر در مثال های بیان شده نیست؛ در بسیاری دیگر از موارد می توان این کاهش هزینه ها و مخارج را مشاهده کرد.

مزیت دیگر ایجاد یک منبع مناسب و گسترده به جهت انجام دادن تحقیقات برای پژوهشگران این عرصه است (Ries & Moysa, 2005, p. 19). از طریق انبوه اطلاعاتی که در پرونده های الکترونیک سلامت وجود دارد، پژوهشگران می توانند اطلاعات سلامت را به راحتی و به سرعت با یک دیگر مقایسه و علل به وجود آمدن برخی بیماری ها را در یک منطقه جغرافیایی کشف کنند و از این طریق به جامعه کمک کنند (Menachemi & Collum, 2011, p. 51). افزون بر این، با توجه به افزایش کیفیت اطلاعات

به دست آمده، نتایجی که محققان به آن می‌رسند دقیق‌تر و صحیح‌تر است. همچنین، دولت‌ها می‌توانند از مسیر پرونده‌های الکترونیک سلامت در زمینه سلامت سیاست‌گذاری کنند. آری، دولت نمی‌تواند در همه موارد سلامت افراد جامعه را تضمین کند، اما با استفاده از منابع اطلاعاتی که در دسترس دارد می‌تواند تا حد امکان از شیوع برخی بیماری‌ها جلوگیری کند یا برخی اقدامات تأمینی را جهت حفاظت از شهروندان انجام دهد (Gostin, 1997, p. 686). مثلاً، اگر در یک منطقه نوع خاصی از بیماری عفونی وجود داشته باشد یا در یک کشور فرضاً بیماری دیابت شایع باشد، دولت می‌تواند با دسترسی سریع به اطلاعات پزشکی افراد آن منطقه یا کل جامعه زمینه شیوع بیشتر بیماری را از بین ببرد یا حداقل آن را کنترل کند. بنابراین، هر مقدار که این منابع اطلاعاتی دقیق‌تر، شفاف‌تر، و راحت‌تر باشد تصمیم اتخاذشده توسط حکمرانان یک مملکت نیز به صواب نزدیک‌تر است.

۲-۲. معایب

دلایل مخالفت با استفاده از پرونده‌های الکترونیک به طور کلی از دو زاویه فردی و اجتماعی قابل تحلیل است. گزاف نیست اگر ادعا شود عمده‌ترین دلیل مخالفت با استقرار پرونده الکترونیک سلامت، از بعد فردی، مسائل مربوط به حریم خصوصی بیمار و محرمانگی اطلاعات پزشکی اوست (Keshta & Odeh, 2021, p. 178)؛ تا جایی که برخی حتی عنوان پژوهش خود را «پرونده‌های الکترونیک سلامت به مثابه تهدیدی برای حریم خصوصی» نام نهاده‌اند (Griener, 2005). اصولاً مسیر نقض حریم خصوصی و محرمانگی در پرونده‌های الکترونیک سلامت برای افراد خاطی بازتر است؛ به تعبیری، هرچند رسوخ فناوری در نظام سلامت و تحولات ناشی از کاربرد آن در اطلاعات پزشکی منجر به انتقال سریع اطلاعات مربوط به بیماران میان کادر درمان و بیمارستان‌های مختلف در مکان‌های متفاوت می‌شود، از منظر دیگر «افشای اطلاعات [اشخاص] صرفاً مستلزم فشردن یک دکمه است» (Steward, 2005, p. 498). به علاوه، نظر به اینکه تعداد افرادی که به پرونده الکترونیک سلامت اشخاص دسترسی دارند زیاد است، همین موضوع احتمال نقض حریم خصوصی و محرمانگی اطلاعات را بیش از پیش افزایش می‌دهد (Winn, 2001, p. 639). مثلاً، در گزارش منتشرشده در روزنامه لس آنجلس تایمز این‌گونه آمده است که به طور تقریبی در هر مورد بستری شدن حدوداً صد و پنجاه نفر به بخشی از اطلاعات پزشکی اشخاص، که در پرونده الکترونیک ثبت و ضبط شده، دسترسی دارند (Kruser, 2007, pp. 320-321).^۱ ایراد نشود که نقض محرمانگی اطلاعات و حریم خصوصی بیمار با توجه به نبود منفعت در افشای این اطلاعات از طریق کادر درمان به ندرت ممکن است اتفاق افتد. زیرا، مجموعه اطلاعات پزشکی اشخاص مختلف برای اشخاص دیگر می‌تواند با ارزش باشد و این آمادگی را داشته باشند که در ازای در اختیار گرفتن آن اطلاعات مابه‌ازایی ارزشمند به افشاکننده پرداخت کنند. بنابراین، با توجه به گردش مالی بالای افشای اطلاعات، تصور نقض محرمانگی

۱. برخی حتی احتمال سوءاستفاده دولت‌ها، که ایجادکننده بستر پرونده الکترونیک سلامت هستند، را از اطلاعات پزشکی ذخیره‌شده در سامانه‌های مرتبط بعید ندانسته‌اند (Miller, 2008, pp. 365-366).

و واگذاری و انتقال این اطلاعات به دیگران دور از ذهن نیست. فقط اشخاصی که به پرونده الکترونیک سلامت دسترسی دارند به افشای اطلاعات دست نمی‌زنند؛ همواره امکان هک سیستم‌های الکترونیکی استفاده‌شده برای ذخیره‌سازی و انتقال اطلاعات پزشکی نیز وجود دارد (Pasquale & Ragone, 2013, p. 621).

از بعد اجتماعی نیز پرونده الکترونیک سلامت از عیب مصون نیست. در حقیقت، هنگامی که جمع‌آوری داده‌های سلامت اشخاص به میزان قابل توجهی افزایش یابد به حدی که بتوان عنوان «بانک اطلاعات» بدان داد، دغدغه حقوق دانان در زمینه موضوع محرمانگی و به طور کلی حساسیت‌های فردی فراتر می‌رود و رویکرد اجتماعی به خود می‌گیرد. این دغدغه ریشه در این واقعیت دارد که اطلاعات مربوط به سلامت افراد جامعه می‌تواند از داده‌های حساس یک کشور محسوب شود که دولت‌ها تمایلی به ارائه آمار دقیق در این زمینه ندارند و یگانه دلیل توجیه‌کننده جمع‌آوری آن‌ها مسائل مربوط به سیاست‌گذاری در عرصه سلامت است. بر این اساس، افشای این اطلاعات و کوتاهی در حفظ امنیت آن‌ها می‌تواند بر امنیت و آسایش عمومی اثر بگذارد (کریمی و همکاران، ۱۳۸۹، صص. ۵۷-۵۸).

قانون مدیریت داده‌ها و اطلاعات ملی، مصوب ۱۴۰۱/۰۸/۱۰، نیز به این دو دغدغه اصلی در این خصوص به خوبی توجه داشته است. ماده ۴ این قانون بیان می‌کند: «داده‌ها و اطلاعات ملی با لحاظ مسائل امنیتی و با رعایت محرمانگی اطلاعات اشخاص در اختیار دولت جمهوری اسلامی ایران است».

در کنار دو دغدغه اصلی مربوط به حفظ محرمانگی اطلاعات (بعد فردی) و صیانت از امنیت آن (بعد اجتماعی)، معایب دیگری نیز در خصوص بهره‌گیری از این سیستم قابل بیان است: ۱. برخلاف ادعای طرفداران استفاده از پرونده‌های الکترونیک سلامت، هزینه استفاده از این سیستم بسیار بالاست. همچنین، هزینه‌های این نوع از پرونده‌های سلامت صرفاً محدود به زمان استقرار این سیستم نیست. هزینه نگهداری و حتی توسعه و به‌روزرسانی زیرساخت‌های پرونده الکترونیک سلامت نیز زیاد است (Menachemi & Collum, 2011, pp. 51-52)؛ ۲. موضوع دیگر عدم آشنایی و آموزش کارکنان و کادر درمان، که با این نوع از پرونده‌ها سروکار دارند، است. در حقیقت، پزشکی که در طول سالیان متمادی به شیوه سنتی امور مربوط به معالجه بیماران را انجام داده نمی‌تواند به سرعت با این نوع از سیستم‌های نوین خو بگیرد (Alpert, 2016, p. 49).

۳-۲. تحلیل ادله

مداقه در دیدگاه‌های بیان‌شده مؤید آن است که هر دو نظریه تا حد زیادی رنگی از حقیقت دارند. آری، بی‌تردید نقض حریم خصوصی بیمار و محرمانگی اطلاعات پزشکی، هزینه‌های بالای استقرار، نگهداری، پشتیبانی و توسعه و در نهایت آموزش و خو گرفتن کادر درمان و حتی مردم عادی با پرونده الکترونیک سلامت از چالش‌های مهم بهره‌گیری گسترده از پرونده‌های الکترونیک سلامت است. اما، همان‌طور که برخی ادعا کرده‌اند، تثبیت پرونده‌های الکترونیک سلامت در کشورهای مختلف اجتناب‌ناپذیر است



و ناچار نظام سلامت در کشورهای مدرن به این سمت حرکت خواهد کرد (See: Murdoch & Detsky, 2013, pp. 1351-1352). چون «سنت‌ها با همه نیرو و سنگینی که با خود دارند، سرانجام، مغلوب نیازها و ضرورت‌ها می‌شوند. این قانون حرکت تاریخ است» (کاتوزیان، ۱۳۹۵، ص. ۹۵).

بر این اساس، نظام سلامت، با توجه به افزایش جمعیت و همچنین افزایش مراجعه‌کنندگان، نیازمند استفاده از فناوری‌های نوین در جهت تسریع انتقال اطلاعات است. در واقع، با توجه به تنوع امراض، لازم است نسخه‌ای از مدارک پزشکی در اختیار پزشکان مختلف با تخصص‌های متنوع قرار گیرد. حال، امکان دارد متخصصان مرتبط با بیماری یک شخص در مکان واحدی نباشند. بنابراین، قابل انکار نیست که وجود پرونده الکترونیک سلامت می‌تواند بررسی اطلاعات پزشکی بیماران را تسهیل کند. البته، طبیعی است که تجهیز نظام سلامت به پرونده الکترونیک سلامت، مانند سایر اقدامات فناورمحور، هزینه‌بر است. اما این هزینه در مقابل منفعی که دارد قابل چشم‌پوشی است.

به علاوه، اصولاً انسان به هر چه عادت کند دل‌کنند از آن برای او سخت است. اما اگر بر این اخلاق آدمی زیاد تکیه شود، هیچ پیشرفتی در جهان رخ نخواهد داد. بنابراین، در مواردی چاره‌ای جز تحمیل اجباری وجود ندارد. پس، اگر کادر درمان به دلیل سختی کار با پرونده الکترونیک از استفاده از آن امتناع می‌کنند و همچنین مطابق با سیستم قدیمی عمل می‌کنند، می‌توان با اتخاذ سیاست‌هایی (از جمله ضمانت اجرای انتظامی) این رویه را تغییر داد. وانگهی، مسئله مربوط به حریم خصوصی و محرمانگی نیز تا حدی قابل حل است. امروزه، می‌توان از خود فناوری برای حفاظت از پرونده‌های الکترونیک سلامت استفاده کرد. بنابراین، حفاظت در مقابل هک کردن سامانه‌ها امری عادی تلقی می‌شود؛ هرچند نفوذ به این سامانه‌ها نیز غیر عادی به نظر نمی‌رسد. در سیستم سنتی کاغذی هم امکان داشت حریم خصوصی بیماران و محرمانگی اطلاعات پزشکی نقض شود. پس، نمی‌توان این استدلال که امکان نقض حریم خصوصی در پرونده‌های الکترونیک سلامت وجود دارد را مستمسکی برای نفی کلی این نوع از پرونده‌های سلامت دانست. بالاتر از این، اگر پروتکل‌های امنیتی به نحو دقیق و کامل در پرونده‌های الکترونیک سلامت رعایت شوند، این پرونده‌ها از پرونده‌های کاغذی امن‌تر هستند (Barrows & Clayton, 1996, p. 146). به هر روی، به نظر می‌رسد باید ضمن پذیرش پرونده الکترونیک سلامت دغدغه‌های مخالفان استقرار و توسعه نظام نوین ذخیره‌سازی و انتقال اطلاعات پزشکی را نیز مد نظر قرار داد و تا جای ممکن چالش‌های پیش روی پرونده‌های الکترونیک سلامت، از لحاظ حریم خصوصی و محرمانگی، را برطرف کرد.

۳. راهکارهای صیانت از پرونده الکترونیک سلامت

از پرونده الکترونیک سلامت، مانند هر پدیده دیگری که در بستر فناوری‌های نوین ایفای نقش می‌کند، می‌توان از راه‌های متفاوت حفاظت کرد.^۱ به منظور تحقق این هدف، اندیشمندان شیوه‌های متعددی

۱. بخش زیادی از جنبه‌های مربوط به صیانت از پرونده‌های الکترونیک سلامت فنی و تخصصی است که از حوزه مباحث این نوشتار خارج است.

را پیشنهاد کرده‌اند.^۱ مثلاً، برخی نویسندگان سه نوع تدبیر امنیتی برای صیانت هر چه بیشتر از پرونده الکترونیک سلامت نام برده‌اند (Keshta & Odeh, 2021, p. 180): ۱. حفاظت‌های مدیریتی یا اداری: «شامل تکنیک‌های مرتبط مانند بازرسی، استخدام یک مسئول برای امنیت اطلاعات، و تدوین طرح‌های اضطراری است...»؛ ۲. حفاظت‌های فیزیکی: «بر حفاظت از اطلاعات پزشکی به شکل فیزیکی تمرکز دارد تا نرم‌افزارها یا سخت‌افزارهای آن‌ها قابل دسترس برای افراد غیر مجاز یا کسانی که ممکن است از آن‌ها سوءاستفاده کنند نباشد...»؛ ۳. حفاظت فنی: «حفاظت از کل سیستم اطلاعاتی موجود در شبکه یک سازمان سلامتی را انجام می‌دهد... این دسته دارای تکنیک‌های امنیتی، مانند استفاده از فایروال و رمزگذاری و بررسی ویروس و اقدامات مورد استفاده در احراز هویت اطلاعات، است». علاوه بر این موارد، تدبیر امنیتی دیگر استفاده از «ناشناس‌سازی»^۲ و «مستعارسازی»^۳ است.^۴ در حقیقت، حفظ محرمانگی

1. Kruse et al., 2017, p. 132:

ردیف	شیوه‌های تأمین امنیت و حفاظت از پرونده الکترونیک سلامت	مصادیق
۱	اداری	● تحلیل ریسک و مدیریت ● افسر ارشد امنیت اطلاعات ● ارزیابی امنیت سیستم ● پیشامدهای احتمالی، استمرار فعالیت، راه کارهای حل بحران
۲	فیزیکی	● تعیین مسئول امنیت ● کنترل دسترسی‌های فیزیکی ● تأمین امنیت محل کار ● دستگاه شناسایی فرکانس رادیویی
۳	فنی	● کنترل دسترسی ● احراز هویت ● رمزگذاری داده‌ها ● محافظت از طریق فایروال (Firewall) ● حسابرسی دنباله‌ها (Audit trail) ● نرم‌افزارهای ضد ویروس

2. Anonymization

3. Pseudonymization

۴. بر اساس بند ۲۶ مقررات عمومی حفاظت از اطلاعات اتحادیه اروپا (GDPR)، اطلاعات ناشناس عبارت است از اطلاعاتی «که به یک شخص حقیقی شناسایی شده یا قابل شناسایی یا به داده‌های شخصی که به گونه‌ای ناشناس ارائه شده‌اند مربوط نمی‌شود؛ به گونه‌ای که موضوع داده‌ها قابل شناسایی نباشد یا دیگر قابل شناسایی نباشد». همچنین، بند ۵ ماده ۴ مقررات عمومی حفاظت از اطلاعات مقرر داشته است: «مستعارسازی، یعنی پردازش داده‌های شخصی به گونه‌ای که دیگر نمی‌توان داده‌های شخصی را بدون استفاده از اطلاعات اضافی به یک موضوع خاص نسبت داد، مشروط بر اینکه این اطلاعات اضافی جداگانه نگهداری شوند و مشمول اقدامات فنی و سازمانی باشند تا اطمینان حاصل شود که داده‌های شخصی به شخص حقیقی شناسایی شده یا قابل شناسایی نسبت داده نمی‌شود». در تفاوت مستعارسازی و ناشناس‌سازی باید گفت در اولی، همان‌طور که در تعریف مقرر یاد شده آمد، با اضافه کردن اطلاعات امکان تشخیص فردی که اطلاعات به او مرتبط است وجود دارد، اما، در ناشناس‌سازی ارتباطی بین دارنده اطلاعات و اطلاعات منتشر شده وجود ندارد. به همین



اطلاعات و حق حریم خصوصی بیماران در زمینه حفظ اطلاعات پزشکی شان، که در پرونده الکترونیک سلامت ذخیره شده، مطلق نیست (میرشکاری و آزادبخت، ۱۴۰۱، صص. ۲۸۰-۲۸۲). مصالح مختلفی نظیر سلامت عمومی جامعه، پیشرفت های پزشکی، ضرورت جلوگیری از سرایت بیماری های عفونی و مسری، و ... می تواند افشای اطلاعات پزشکی بیماران را توجیه کند. به بیان روشن تر، منظور از محرمانگی اطلاعات پزشکی و حق بر حریم خصوصی بیماران حفظ حداکثری (و نه مطلق) محرمانگی و حریم خصوصی است. در واقع، اصولاً اطلاعات پزشکی نباید قابل دسترسی باشد یا افشا شود. اما، در موارد استثنا، اگر قرار بر دسترسی یا افشای اطلاعات پزشکی باشد، می توان از روش هایی مانند ناشناس سازی یا مستعارسازی استفاده کرد تا بیمار و به تبع آن خانواده اش قابل شناسایی نباشند. با این حال، با وجود نسبی بودن حق بیماران بر اطلاعات پزشکی، باید تا جای ممکن هویت ایشان فاش نشود. بدین منظور، لازم است در مواردی که انتقال اطلاعات بیماران میان ارگان های مختلف دولتی، پژوهشگران، و ... ضرورت می یابد از تکنیک های مربوط به ناشناس سازی و مستعارسازی در خصوص هویت بیماران استفاده شود.

شیوه دیگر «کنترل دسترسی»^۱ است (Oh et al., 2021, p. 9). این راهکار را می توان در پرتو اصل «حداقل سازی داده ها»^۲ نیز تحلیل کرد؛ اصلی که بر اساس آن گردآوری و دسترسی به داده های شخصی باید صرفاً به میزانی محدود شود که برای تحقق هدف مشخص و مشروع ضروری است. در حوزه داده های سلامت، رعایت این اصل اقتضا می کند اشخاص مختلف فقط به آن بخش از اطلاعات پزشکی دسترسی داشته باشند که برای انجام دادن وظیفه حرفه ای آنان لازم است و از دسترسی گسترده و غیر ضروری به سایر داده های سلامت جلوگیری شود. بر همین اساس، در اجازه دادن برای دسترسی به پرونده پزشکی بیماران نباید گشاده دستی کرد. در واقع، برای درمان هر بیماری خاص لزومی ندارد پزشک معالج یا اعضای دیگر کادر درمان به پرونده الکترونیک فرد به طور کلی دسترسی داشته باشند. چون ممکن است اطلاعاتی را مشاهده کنند که هیچ ارتباطی با بیماری مربوطه نداشته باشند. افزون بر این، اگر یک پزشک به صورت الکترونیک نسخه ای تجویز کند که بیمار آن را از داروخانه دریافت کند، ضرورتی ندارد داروخانه با وارد کردن مشخصات هویتی فرد، ضمن دسترسی به نسخه مورد نظر، به سایر اطلاعات پرونده دسترسی پیدا کند. بر این بنیاد، لازم است، با استفاده از فناوری های نوین، دسترسی هر شخص به همان عملکرد و کارکردی که از وی انتظار می رود محدود شود. به علاوه، در جهت تحقق این هدف می توان برای ورود به پرونده الکترونیک سلامت افراد محدودیت هایی ایجاد کرد؛ بدین توضیح که به صرف وارد کردن مشخصات هویتی (مانند کد ملی) امکان ورود به این پرونده فراهم نباشد، بلکه از رمز عبور و سازکارهای مشابه برای احراز هویت استفاده شود. وانگهی، اطلاعات پرونده الکترونیک سلامت را نیز می توان بر حسب میزان حساسیت و اهمیت داده ها دسته بندی کرد. در حقیقت، لزومی ندارد که یک پزشک عمومی به اطلاعات بسیار حساس پزشکی فرد، مثلاً

دلیل است که روش ناشناس سازی اصل محرمانگی را در خصوص اطلاعات پزشکی بهتر تأمین می کند و روش مطمئن تری است (Riedl et al., 2007, p. 319). در حقوق انگلیس این موضوع تأیید شده است که در استفاده از اطلاعاتی که در آن ناشناس سازی صورت گرفته هیچ گونه عدولی از محرمانگی اطلاعات پزشکی محقق نمی شود (Lachmann, 2003, p. 2).

1. Access Control
2. Data Minimization



اطلاعات مربوط به ابتلا به نوع خاصی از سرطان، دسترسی داشته باشد. همچنین، می‌توان سیستمی طراحی کرد که مشخص کند در هر بار ورود به پرونده چه شخصی وارد شده و پس از ورود دقیقاً چه اقداماتی انجام داده است.^۱

تدبیر بعد استفاده از سیستم «رمزنگاری»^۲ است (Barrows & Clayton, 1996, p. 144). رمزنگاری روشی است که با استفاده از الگوریتم‌ها و تکنیک‌های ریاضی اطلاعات و ارتباطات را ایمن می‌کند. رمزنگاری فرایند تبدیل داده‌های متن ساده به داده‌های رمزنگاری شده با استفاده از یک الگوریتم ریاضی و یک کلید مخفی است. داده‌های رمزنگاری شده فقط توسط کسی به داده‌های متن ساده بازگشت داده می‌شود که به همان کلید مخفی دسترسی دارد. بنابراین، از این طریق می‌توان به طور نسبی اطمینان یافت که اطلاعات مندرج در پرونده الکترونیک سلامت توسط اشخاصی که به آن کلید مخفی دسترسی ندارند قابل دستیابی نخواهد بود.

۴. رویکرد نظام‌های حقوقی آمریکا و ایران

پس از تجزیه و تحلیل محاسن و معایب پرونده الکترونیک سلامت و شیوه‌های صیانت از آن، اکنون وقت آن است که موضع نظام حقوقی آمریکا و ایران در زمینه پرونده الکترونیک سلامت از منظر حریم خصوصی بیمار و محرمانگی اطلاعات معین شود. پیش از بررسی دو نظام حقوقی ایران و آمریکا، بیان یک نکته در خصوص تقسیم‌بندی نظام‌های حقوقی از منظر الزامی یا اختیاری بودن پرونده الکترونیک سلامت ضروری به نظر می‌رسد. به طور کلی، دو سیستم در خصوص الزامی یا اختیاری بودن پرونده الکترونیک سلامت وجود دارد (Mikhail & Olga, 2020, p. 104): ۱. opt-in: در این سیستم، برای داشتن پرونده الکترونیک سلامت ابتدا رضایت بیمار اخذ می‌شود؛ یعنی ورود به سیستم پرونده الکترونیک سلامت اختیاری است (کشورهایی مثل فرانسه و تا سال ۲۰۱۶ استرالیا)؛ ۲. opt-out: در این سیستم ورود به سیستم پرونده الکترونیک سلامت اختیاری نیست. اما به بیمار حق داده می‌شود که از داشتن پرونده الکترونیک سلامت انصراف دهد (کشورهایی مثل انگلیس، سنگاپور، استرالیا پس از سال ۲۰۱۶).

در ادامه، نخست رویکرد نظام حقوقی آمریکا و در گام بعد رویکرد نظام حقوقی ایران بررسی می‌شود.

۴-۱. آمریکا

توسعه اولیه پرونده الکترونیک سلامت در دهه ۱۹۶۰ و ۱۹۷۰ در ایالات متحده آمریکا آغاز شد. ابتدا، سیستم‌های پرونده الکترونیک سلامت سیستم‌های اطلاعات بالینی شناخته می‌شدند. در دهه ۱۹۸۰، مؤسسه پزشکی تلاش‌های بی‌وقفه‌ای برای افزایش استفاده از پرونده الکترونیک سلامت انجام داد. در سال

۱. این سیستم شبیه فعال کردن گزینه ترک چنج در فایل ورد است که تغییرات بعدی را نمایش می‌دهد.

2. Cryptography

۲۰۰۴، با ایجاد دفتر هماهنگ‌کننده ملی اطلاعات سلامت، اهمیت پرونده الکترونیک سلامت در سراسر کشور شناخته شد (Purvi Nema & Riya Sinha, 2021, p. 4). پیش از بیان قانون قابل استناد در خصوص مباحث حریم خصوصی بیماران و محرمانگی اطلاعات پزشکی، باید موضع نظام حقوقی امریکا در خصوص الزامی یا اختیاری بودن پرونده الکترونیک سلامت برای بیماران معین شود. در حقوق امریکا، داشتن پرونده الکترونیک سلامت الزامی است؛ بدین توضیح که بیماران در انتخاب اینکه اطلاعات پزشکی شان به صورت الکترونیکی ذخیره نشود مختار نیستند. قوانین فدرالی مربوط به حفظ محرمانگی اطلاعات پزشکی نیز منحصرأ به مبحث انتشار اطلاعات پزشکی پرداخته‌اند؛ یعنی مرحله جمع‌آوری اطلاعات از بیماران را مفروض انگاشته‌اند (Hiller et al., 2011, p. 31).^۱ با وجود این، بیماران می‌توانند از داشتن پرونده الکترونیک سلامت انصراف دهند و در واقع از این سیستم خارج شوند (Mikhail & Olga, 2020, p. 105). وانگهی، ارائه‌دهندگان خدمات پزشکی می‌توانند مانع دسترسی هر شخصی به پرونده‌های پزشکی بشوند، غیر از خود بیمار. بیمار می‌تواند از پرونده پزشکی رونوشت بخواهد، اطلاعات مندرج در پرونده پزشکی را بازبینی و بررسی کند، و درخواست کند برخی اطلاعات اصلاح شوند (Hall, 2009, p. 649).

در حقوق امریکا، حمایت از حریم خصوصی بیماران و محرمانگی اطلاعات در پرونده‌های الکترونیک سلامت در دو سطح فدرال و ایالات قابل بررسی است. پس، برای تعیین موضع ایالات باید به قوانین و مقررات هر ایالت به طور جداگانه مراجعه کرد که این موضوع محل بحث در این نوشتار نیست. بخش فدرال نیز به دو قسم قابل تقسیم است. برخی قوانین، مانند قانون حریم خصوصی (۱۹۷۴)^۲، به صورت عام به حمایت از حریم خصوصی پرداخته‌اند. اما این قوانین نیز حمایت عمیق و به خصوصی در مورد حریم خصوصی بیماران و محرمانگی اطلاعات در پرونده‌های الکترونیک سلامت نکرده‌اند (Carter, 1999, pp. 241-245)؛ بنابراین، باید به دنبال قوانینی بود که به طور خاص بدین موضوع پرداخته‌اند. در این زمینه، قانون قابلیت انتقال و پاسخگویی بیمه سلامت (۱۹۹۶)^۳ قابل اشاره است. در این قانون به کنگره سه سال فرصت داده شده بود که قواعد مربوط به حریم خصوصی اطلاعات پزشکی را به تصویب برساند و در صورت عدم اقدام در این مدت وزارت بهداشت و خدمات انسانی امریکا متولی امر می‌شد. با توجه به عدم اقدام کنگره در این زمینه، وزارت بهداشت و خدمات انسانی ایالات متحده استانداردهای حریم خصوصی اطلاعات بهداشتی قابل شناسایی فردی (اصطلاحاً قانون حفظ حریم خصوصی)^۴ را برای اولین بار، در سال ۲۰۰۰، با هدف اینکه مجموعه‌ای از استانداردهای ملی را برای حفاظت از اطلاعات بهداشتی ایجاد کند، تصویب کرد. به علاوه، قواعد مربوط به امنیت^۵ قانون بیمه سلامت قابل انتقال و مسئولیت‌پذیری نیز در سال ۲۰۰۳ به تصویب رسید.

۱. موضع اتحادیه اروپا دقیقاً برعکس است. بر اساس قواعد حاکم بر این اتحادیه، اساساً داشتن پرونده الکترونیک سلامت نیازمند رضایت بیماران است (Hiller et al., 2011, p. 31). در کانادا (غیر از برخی ایالات) رضایت بیمار برای جمع‌آوری و استفاده و انتشار اطلاعات لازم است (Ries, 2005, p. 693).

2. The Privacy Act, 1974

3. The Health Insurance Portability and Accountability Act (HIPAA), 1996

4. The Standards for Privacy of Individually Identifiable Health Information, Also Known as the Hipaa Privacy Rule

5. Security Rules



قانون دیگری نیز موسوم به فناوری اطلاعات سلامت برای سلامت اقتصادی و بالینی^۱، مصوب ۲۰۰۹، وجود دارد که اصلاحاتی را نسبت به قوانین پیشین اعمال کرده است.^۲

بر اساس قانون بیمه سلامت قابل انتقال و مسئولیت‌پذیری، صرفاً از اطلاعات پزشکی که هویت فرد را معین می‌کند حمایت می‌شود. پس، اطلاعاتی که ناشناس‌سازی شده‌اند تحت شمول این قانون قرار نمی‌گیرند (Terry, 2017, p. 163). این قانون صرفاً به محرمانگی اطلاعات پزشکی پرداخته است. این بدان معناست که شمول قانون یادشده فقط در حوزه مربوط به انتشار و استفاده از اطلاعات پزشکی مندرج در پرونده الکترونیک سلامت اشخاص است و نه حریم خصوصی ایشان که به جمع‌آوری اطلاعات ارتباط پیدا می‌کند. در هر موردی نیز که به حریم خصوصی اشاره شده منظور همان محرمانگی است (Terry & Francis, 2007, p. 701; Terry, 2014, p. 68). همچنین، در این قوانین تأکید شده است که نهادهای ذی‌ربط (ذخیره‌کننده اطلاعات) باید اقدامات احتیاطی و تأمینی را برای حفاظت هر چه بیشتر از اطلاعات پزشکی بیماران انجام دهند. در صورتی که اطلاعات بیماران به صورت غیر موجه افشا شود یا افرادی بدان دسترسی یابند، باید به بیمار اطلاع داده شود.

قاعده کلی در قواعد حریم خصوصی قانون بیمه سلامت آن است که افشای اطلاعات بیماران مجاز نیست، مگر در دو مورد: ۱. قواعد مربوط به حریم خصوصی این اجازه را داده باشد؛ یعنی در یک موقعیت خاص اقتضای افشای اطلاعات را داشته باشد و ۲. خود بیمار یا نماینده وی به صورت کتبی به افشای اطلاعات راضی باشد. در دو فرض، افشای اطلاعات برای نهادهای ذخیره‌کننده الزامی است. فرض اول در صورت درخواست بیماران یا نمایندگان ایشان است؛ یعنی بیمار درخواست کند که به اطلاعات پزشکی خویش دسترسی داشته باشد.^۳ فرض دوم در صورت مطالبه وزارت بهداشت و خدمات انسانی است. گاه، نهاد ذخیره‌کننده می‌تواند، اما، الزام ندارد بدون اجازه گرفتن از بیمار اطلاعات وی را افشا کند: ۱. ممکن است از اطلاعات بهداشتی محافظت شده برای درمان، پرداخت و عملیات مراقبت‌های بهداشتی خود استفاده و آن را افشا کند؛ ۲. در مواردی که فرد اهلیت ندارد، در شرایط اضطراری، یا هنگامی که فرد در دسترس نیست نهادهای تحت پوشش عموماً می‌توانند افشاگری‌هایی انجام دهند، البته در صورتی که در اعمال قضاوت حرفه‌ای خود استفاده یا افشای اطلاعات به نفع فرد تشخیص داده شود؛ ۳. هنگامی که موضوع منافع عمومی و فعالیت‌های سودمند مطرح باشد اجازه افشای اطلاعات بهداشتی محافظت شده بدون مجوز فرد برای دوازده هدف اولویت ملی داده شده است. مثلاً، نهادهای مربوطه ممکن است اطلاعات بهداشتی محافظت شده را در مورد قربانیان سوءاستفاده، غفلت، یا خشونت خانگی برای مقامات دولتی

1. The Health Information Technology for Economic and Clinical Health (HITECH), 2009

۲. در این قانون اصلاحاتی بدین صورت پذیرفته است: افزایش جرایم برای نقض قانون بیمه سلامت قابل انتقال و مسئولیت‌پذیری، گسترش دامنه اشخاصی که ملزم به رعایت قانون هستند، اخطار دادن به بیمار، وزارت بهداشت در صورتی که اطلاعات پزشکی بیماران افشا شده باشد، و مواردی از این دست.

۳. «برای اجتناب از آثار سوء آزادی اطلاعات بر سلامتی افراد، در قوانین آزادی اطلاعات کشورهای مختلف جهان مقرر شده است که چنانچه مؤسسه دارنده اطلاعات تشخیص دهد که افشای اطلاعات درخواستی سلامتی جسمی یا روانی فرد یا افرادی را در معرض تهدید قرار می‌دهد یا به سلامتی عمومی لطمه وارد می‌کند باید از ارائه اطلاعات خودداری کند؛ حتی اگر اطلاعات درخواستی در زمره اطلاعات شخصی متقاضی باشد» (انصاری، ۱۳۹۷، ص. ۲۵۵).

مرتبط افشا کنند. همچنین احتمال دارد اطلاعات مربوط به شخص را برای پزشکی قانونی افشا کنند تا پزشکی قانونی بتواند مثلاً هویت فرد با علت دقیق مرگ را تشخیص دهد. اگر درخواست اطلاعات از طریق دستور دادگاه باشد، نهادهای تحت پوشش ممکن است اطلاعات بهداشتی محافظت شده را در دادرسی افشا کنند. این اطلاعات همچنین ممکن است در پاسخ به احضاریه یا سایر فرایندهای قانونی فاش شود.^۱ به هر شکل، هدف از بیان مختصر قواعد حاکم بر حریم خصوصی بیماران و محرمانگی اطلاعات پزشکی پرونده‌های الکترونیک سلامت در حقوق امریکا آن بود که حرکت این نظام حقوقی به سمت قاعده‌مند کردن هر چه بیشتر این موضوعات نشان داده شود.

۴-۲. ایران

در حقوق ایران، در خصوص پرونده الکترونیک سلامت، قوانین متعددی به تصویب رسیده‌اند. روند تصویب قوانین مرتبط با پرونده الکترونیک سلامت از سال ۱۳۸۴ از طریق بند «ه» ماده ۸۸ قانون برنامه چهارم توسعه اقتصادی، اجتماعی، و فرهنگی آغاز شد. این روند با تصویب بند «الف» و «ب» ماده ۳۵ قانون برنامه پنجم توسعه اقتصادی، اجتماعی، و فرهنگی مصوب ۱۳۹۰ و بند «ح» ماده ۶۸ و بندهای «الف» و «ث» و «ج» ماده ۷۴ قانون برنامه ششم توسعه اقتصادی، اجتماعی، و فرهنگی پیگیری شد. البته، هر سال در قوانین بودجه نیز به پرونده الکترونیک سلامت اشاره می‌شود؛ کما اینکه در بند «ل» (۵) تبصره ۱۷ قانون بودجه ۱۴۰۲ کل کشور مقرر شده است: «... کلیه شرکت‌ها و سازمان‌های بیمه‌گر پایه و تکمیلی درمان، اعم از دولتی و غیر دولتی، مکلف‌اند با همکاری وزارت بهداشت، درمان، و آموزش پزشکی درگاه پرونده الکترونیکی بیمار و پزشک را (مبتنی بر نسخ الکترونیک بیمه‌ای) ظرف سه ماه از ابلاغ این قانون عملیاتی نموده و در اختیار ارائه‌دهندگان خدمت و بیمه‌شدگان قرار دهند». اکنون، به دو پرسش اشاره شده در حقوق امریکا برمی‌گردیم: نخست آنکه آیا در نظام حقوقی ایران داشتن پرونده الکترونیک سلامت الزامی است؟ و دوم آنکه آیا چارچوب مشخص امنیتی برای صیانت از حریم خصوصی و محرمانگی اطلاعات مندرج در پرونده الکترونیک سلامت وجود دارد؟

در پاسخ به پرسش اول باید اذعان داشت که در بند «الف» ماده ۷۴ قانون برنامه ششم توسعه عباراتی دال بر غیر الزامی بودن پرونده الکترونیک برای شهروندان وجود داشت. مطابق این بند از ماده یادشده «وزارت بهداشت، درمان، و آموزش پزشکی با هدف ارائه خدمات الکترونیکی سلامت مکلف است ظرف دو سال اول اجرای قانون برنامه نسبت به استقرار سامانه پرونده الکترونیکی سلامت ایرانیان و سامانه‌های اطلاعاتی مراکز سلامت با هماهنگی پایگاه ملی آمار ایران و سازمان ثبت احوال کشور با حفظ حریم خصوصی و منوط به اذن آن‌ها و محرمانه بودن داده‌ها و با اولویت شروع برنامه پزشک خانواده و نظام ارجاع اقدام نماید». با توجه به این ماده، می‌شد گفت استقرار پرونده الکترونیک سلامت ایرانیان منوط به اذن ایرانیان بوده است. با این حال، به نظر می‌رسد پذیرش اختیاری بودن استفاده از پرونده الکترونیک سلامت قابل پذیرش نباشد. چون اولاً اگر استقرار پرونده سلامت الکترونیک و سامانه‌های اطلاعاتی مراکز سلامت منوط به اذن افراد جامعه باشد، عملاً ممکن است این استقرار به نحو مطلوب و احسن صورت نپذیرد. در حقیقت، اگر اراده



1. See: Summary of the HIPAA Privacy Rule

اشخاص در داشتن یا نداشتن پرونده الکترونیک سلامت دخیل باشد، این طرح و اهداف عالیّه آن سرانجام خوبی نخواهند داشت. چه آنکه ممکن است اشخاص مختلف از اعطای اذن به وزارت بهداشت امتناع کنند. ثانیاً، با توجه به اینکه اذن قابل رجوع است، معنای آن این است که اشخاص جامعه هر زمان مایل باشند می‌توانند از ورود در فرایند حاکم بر پرونده الکترونیک سلامت انصراف دهند؛ موضوعی که نتایج نامطلوب آن مورد پذیرش هیچ‌کس نیست.

شاید با توجه به همین نقدهاست که قانون‌گذار در قانون برنامه هفتم پیشرفت جمهوری اسلامی ایران مسیر دیگری را انتخاب کرد. بند «الف» ماده ۶۹ این قانون وزارت بهداشت، درمان، و آموزش پزشکی را مکلف کرده است، با هدف ایجاد نظام هوشمند اطلاعات سلامت، همه سامانه‌های مراکز ارائه‌دهنده خدمات و کالای سلامت را به یک‌دیگر متصل و داده‌های سلامت تولیدشده را به صورت متمرکز و امن در «پایگاه ملی سلامت» ذخیره کند. همچنین، مطابق جزء ۲ همان بند، همه ارائه‌دهندگان خدمات سلامت، اعم از دولتی و عمومی غیر دولتی و خیریه و خصوصی، مکلف شده‌اند داده‌های سلامت و پزشکی ایرانیان و اتباع غیر ایرانی را به صورت برخط و هم‌زمان با ارائه خدمت به وزارت بهداشت ارسال کنند و حتی تمدید پروانه‌های حرفه‌ای و مجوزهای فعالیت آنان نیز منوط به اجرای این تکلیف شده است. مفاد این مقرر نشان می‌دهد قانون‌گذار در برنامه هفتم اصل تشکیل، تکمیل، و تغذیه مستمر پرونده الکترونیک سلامت را یکی از ارکان نظام سلامت کشور به شمار آورده و آن را در قالب تکالیف الزام‌آور بر ارائه‌دهندگان خدمات سلامت تحمیل کرده است. از این رو، دشوار می‌توان پذیرفت که قانون‌گذار از یک سو شبکه‌ای فراگیر و اجباری برای تولید و انتقال و تجمیع داده‌های سلامت طراحی کرده باشد و از سوی دیگر اصل تشکیل پرونده الکترونیک سلامت را به اراده و رضایت موردی اشخاص واگذار کرده باشد. نکته مهم دیگر آن است که ماده ۶۹ برنامه هفتم، ضمن تأکید بر «صیانت از اطلاعات سلامت شهروندان»، دسترسی به این اطلاعات را صرفاً برای اشخاصی مجاز دانسته است که یا قانوناً حق دسترسی دارند یا بر اساس مجوز دریافت شده از «مالک اصلی اطلاعات (شهروند)» مجاز به استفاده از آن هستند. بنابراین، قانون‌گذار در این ماده، به جای اعطای اختیار به شهروند برای اصل تشکیل پرونده الکترونیک سلامت، بر حقوق او در ارتباط با اطلاعات موجود در پرونده تأکید کرده است. به بیان دیگر، رضایت شهروند در این مقرر ناظر به بهره‌برداری و دسترسی به اطلاعات سلامت است، نه ناظر به اصل ایجاد و نگهداری پرونده الکترونیک سلامت. بر این اساس، به نظر می‌رسد حتی اگر از عبارت «منوط به اذن آن‌ها» در بند «الف» ماده ۷۴ قانون برنامه ششم توسعه برداشتی دال بر لزوم رضایت اشخاص برای پردازش داده‌های سلامت استنباط می‌شد، قانون برنامه هفتم پیشرفت، با تصریح به ایجاد پایگاه ملی سلامت، الزام مراکز درمانی به ارسال برخط داده‌ها، و شناسایی شهروند در مقام مالک اطلاعات سلامت ابهام اشاره‌شده را تا حد زیادی مرتفع ساخته و حکایت از آن دارد که نظام حقوقی ایران در حال حرکت به سمت الگوی تشکیل فراگیر و تقریباً الزامی پرونده الکترونیک سلامت همراه تضمین حقوق و منافع صاحبان داده است.

با لحاظ این الزام قانونی به نظر می‌رسد همه اطلاعات مربوط به سلامت اشخاص جامعه باید در پرونده الکترونیک سلامت ثبت شود و وزارت بهداشت، درمان، و آموزش پزشکی بر اساس ردیف ۱۷ جدول ذیل ماده ۱۰ قانون مدیریت داده‌ها و اطلاعات ملی متولی اداره و به‌روزرسانی پایگاه ملی سلامت خواهد بود.

بنابراین، داده‌های این حوزه به طور کامل (صرف نظر از مالکیت اشخاص موضوع داده) داده و اطلاعات ملی محسوب می‌شود و مطابق ماده ۴ قانون مدیریت داده‌ها و اطلاعات ملی در اختیار دولت جمهوری اسلامی ایران است. در نتیجه، بر اساس ماده ۵ قانون یادشده هر گونه تولید، نگهداری، پردازش، حفظ امنیت و صیانت این داده‌ها وفق سیاست‌ها و نظامات مصوب شورای عالی فضای مجازی و مصوبات کارگروه تعامل‌پذیری دولت الکترونیک خواهد بود و ارائه‌دهندگان خدمات سلامت ذیل تنظیم‌گران بخشی مانند پزشکان، بیمارستان‌ها، داروخانه‌ها، آزمایشگاه‌ها، و... حق اطلاع از پرونده الکترونیک سلامت و داده‌های مندرج در آن را ندارند و وفق تبصره ماده ۴ قانون مدیریت داده‌ها و اطلاعات ملی باید امکان دسترسی و تبادل این دست داده‌ها و اطلاعات را صرفاً بر اساس سطوح دسترسی تعیین شده توسط کارگروه تعامل‌پذیری دولت الکترونیک فراهم کنند.

البته، چند نکته مهم در این زمینه قابل بیان است:

نخست آنکه، هرچند داشتن پرونده الکترونیک سلامت الزامی است، این موضوع به معنای آن نیست که داده‌های سلامت اشخاص، که در این پرونده‌ها ذخیره شده، به طور آزادانه قابل دسترسی هستند؛ بلکه، دسترسی به این داده‌ها باید با رعایت کامل حریم خصوصی بیماران صورت پذیرد. جلوه‌گاه رعایت حریم خصوصی نیز طبیعتاً اخذ اذن از بیماران است (بند ۵ ماده ۳ آیین‌نامه برنامه اجرایی توسعه و استقرار نظام جامع سلامت الکترونیک). گفتنی است، نقض حریم خصوصی و محرمانگی اطلاعات بیماران، از طریق دسترسی با افشای داده‌های سلامت ایشان، ضمانت اجرای (مسئولیت) مدنی و کیفری دارد. از منظر مسئولیت مدنی، «در صورت انتشار اطلاعات واقعی برخلاف مفاد این قانون، اشخاص حقیقی یا حقوقی حق دارند که مطابق قواعد عمومی مسئولیت مدنی جبران خسارت‌های وارد شده را مطالبه نمایند» (قانون انتشار و دسترسی آزاد به اطلاعات، تبصره ماده ۲۱). همچنین، به لحاظ کیفری قانون‌گذار در ماده ۶۴۸ قانون مجازات اسلامی (بخش تعزیرات) اظهار می‌دارد: «اطبا و جراحان و ماماها و داروفروشان و کلیه کسانی که به مناسبت شغل یا حرفه خود محرم اسرار می‌شوند، هرگاه در غیر از موارد قانونی اسرار مردم را افشا 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».^۱ گفتنی است موضوع ماده مربوط به افشای اسرار حرفه‌ای است و افراد عادی جامعه، که اسرار مردم را افشا می‌کنند، مشمول آن قرار نمی‌گیرند.^۲

دوم آنکه در خصوص امکان یا عدم امکان خروج از پرونده الکترونیک سلامت توسط دارندگان این پرونده سخنی به میان نیامده است و مشخص نیست که موضع نظام حقوقی در این موضوع چیست.

سوم آنکه به رغم وجود نصوص متعدد در خصوص اجباری بودن پرونده الکترونیک سلامت، در عمل، اوضاع به گونه دیگری است. در واقع، به گواه گزارش مرکز پژوهش‌های مجلس، هنوز تا اجرای کامل و استقرار نهایی و ملی پرونده الکترونیک سلامت فاصله وجود دارد. زیرا، در حال حاضر بسترهای لازم برای ایجاد یک سامانه ملی نظام الکترونیک سلامت به دلیل «فقدان نقشه و معماری کلان و یکپارچه، عدم تناسب ساختار

۱. برای مطالعه بیشتر در خصوص این ماده، ر.ک.: میرکمالی و صالح احمدی، ۱۴۰۰، صص. ۳۷۲-۳۷۷.

۲. همچنین، ماده ۱ قانون جرایم رایانه‌ای در این زمینه قابل استناد است.

اجرایی با ابعاد و گستردگی طرح و تغییرات مکرر مدیریتی، عدم تأمین اعتبارات کافی، عدم اتصال بخش عمده‌ای از مراکز خدمتی با مرکز تبادل اطلاعات سلامت، و عدم درج بخشی از اقلام پرونده در سامانه مراکز، ناهمسانی کدها، عدم پیش‌بینی سازکارهای تضمین امنیت و محرمانگی اطلاعات، عدم تحقق امضای الکترونیک و ضعف برخی از زیرساخت‌ها» (بختیاری علی‌آباد، ۱۴۰۱، صص. ۱۸-۲۸)، وجود ندارد.

اما در مورد سؤال دوم، همان‌طور که در گزارش مرکز پژوهش‌های مجلس آمده، نظام خاصی برای صیانت از پرونده‌های الکترونیک سلامت وجود ندارد؛ تا آنجا که در مکاتبه سرپرست مرکز مدیریت آمار و فناوری اطلاعات وزارت بهداشت، درمان، و آموزش پزشکی با وزیر بهداشت آمده است: «اقدامات لازم جهت اخذ گواهی ارزیابی امنیتی افتا روی سامانه‌های نسخه الکترونیک انجام نشده است. همچنین، مرکز راهبردی افتا صراحتاً سامانه‌های مذکور را فاقد امنیت لازم اعلام نموده است» (بختیاری علی‌آباد، ۱۴۰۱، صص. ۱۸-۲۸). آری، نصوص متعددی درباره اینکه اطلاعات پزشکی در زمره اطلاعات محرمانه است وجود دارد (مانند بند «ب» از ماده ۱ آیین‌نامه اجرایی قانون انتشار و دسترسی آزاد به اطلاعات و ماده ۶ قانون مدیریت داده‌ها و اطلاعات ملی). اما وجود این نصوص به معنای ایجاد سازکار فنی حفاظت از اطلاعات پزشکی مندرج در پرونده الکترونیک سلامت نیست.

در پایان باید گفت نظام قانون‌گذاری ایران، چنان‌که شایسته و بایسته است، به حقوق اشخاص صاحب پرونده الکترونیک سلامت (بیماران) نپرداخته است. در واقع، با وجود حرکت سایر نظام‌های حقوقی پیشرفته به سمت شناسایی حقوق اشخاص صاحب داده، حقوق ایران اصولاً و منحصرأً اصل پرونده الکترونیک سلامت را به رسمیت شناخته است؛ این در حالی است که صرف شناسایی کفایت نمی‌کند و باید به طور دقیق و با جزئیات روشن به حقوق صاحبان پرونده الکترونیک اشاره شود. بیان این حقوق موضوعی است که سابقاً در حقوق غرب نیز مشاهده شده است. مثلاً، مواد ۱۲ تا ۲۲ مقررات عمومی حفاظت از داده‌های اتحادیه اروپا حقوق اشخاص موضوع داده را به تفصیل بیان کرده است. این حقوق عبارت‌اند از: «حق دریافت اطلاعات از کنترل‌کننده»، «حق دسترسی به داده‌های شخصی»، «حق تصحیح، حق حذف (فراموش شدن)، حق محدودیت پردازش»، «حق انتقال داده»، «حق اعتراض»، و «حق در خصوص عدم ارزیابی با تصمیمات خودکار» (لطیف‌زاده و همکاران، ۱۴۰۲، صص. ۹۸۱-۱۰۰۵). بنابراین، حداقل انتظار از قانون‌گذار آن است که در زمینه این امور نصوصی را اختصاص دهد تا حقوق ایران از ابهامات موجود در این زمینه رهایی یابد.

نتیجه

رسوخ فناوری‌های نوین در نظام سلامت کشورهای مختلف اجتناب‌ناپذیر است. این موضوع، با توجه به مزایای انکارنشدنی استفاده از فناوری در نظام سلامت، منطقی به نظر می‌رسد. البته، وجود مزیت به معنای عدم عیب نیست. به دیگر بیان، همان‌طور که استفاده از فناوری در نظام سلامت مفید است، طبیعتاً معایبی نیز دارد که باید تا جای ممکن برطرف شوند. یکی از این چالش‌ها موضوعات مربوط به حریم



خصوصی و محرمانگی اطلاعات پزشکی مندرج در پرونده‌های الکترونیک سلامت است. دغدغه‌مندان حریم خصوصی و محرمانگی اطلاعات با هدف حفاظت از این دو مورد به طور کلی استفاده از پرونده‌های الکترونیکی سلامت را نفی می‌کنند. اما به نظر می‌رسد، با توجه به پیشرفت‌های روزافزون فناوری‌های جدید، صیانت از اطلاعات پزشکی ناممکن نباشد. البته، بدیهی است که اتخاذ تدابیر امنیتی در سطوح مختلف لزوماً به معنای حفاظت صد درصدی نخواهد بود. در هر حال، ضمن عنایت به این نکته که نظام سلامت ایران به لحاظ نصوص قانونی برای شناسایی اصل پرونده الکترونیک سلامت و اجباری بودن آن تقریباً غنی به نظر می‌رسد، در زمینه تدابیر امنیتی و حفاظت از این اطلاعات هیچ نص قابل اتکایی وجود ندارد. بنابراین، پیشنهاد می‌شود در حقوق ایران نیز قانون‌گذار صرفاً به اصل وجود پرونده الکترونیک سلامت اکتفا نکند؛ بلکه، همانند حقوق آمریکا، سطوح مختلف امنیتی و همچنین اشخاصی که می‌توانند به این اطلاعات دسترسی داشته باشند را به صراحت معین کند. افزون بر این، سازکاری پیش‌بینی شود که هرگونه تغییر و تحول در پرونده الکترونیک سلامت اشخاص به راحتی قابل ردیابی باشد. وانگهی، در خصوص اینکه دارندگان پرونده الکترونیک سلامت تا چه حد می‌توانند در داده‌های مندرج در پرونده الکترونیک سلامت دخل و تصرف کنند ساختار و چارچوب مشخص و روشنی تدوین شود.

توضیحات:

تأمین مالی

این پژوهش از مرکز ملی تحقیقات حقوق سلامت، حمایت مالی دریافت نکرده است.

تعارض منافع

نویسندگان اعلام می‌کنند که هیچ‌گونه تعارض منافی در ارتباط با این پژوهش وجود ندارد.

ملاحظات اخلاقی

این پژوهش بر پایه تحلیل اسناد و منابع کتابخانه‌ای انجام شده و مستلزم اخذ کد اخلاق نبوده است.

مشارکت نویسندگان

تمام مراحل طراحی پژوهش، تحلیل، نگارش و بازنگری مقاله با مشارکت همه نویسندگان انجام شده است.



منابع

الف) فارسی

کتاب‌ها

۱. انصاری، باقر (۱۳۹۷). حق دسترسی به اطلاعات: آزادی اطلاعات. دفتر مطالعات و برنامه‌ریزی رسانه‌ها.
۲. _____ (۱۴۰۰). حقوق حریم خصوصی. سمت.
۳. سلمانلو، مریم (۱۳۹۸). حقوق حریم خصوصی. گنج دانش.
۴. کاتوزیان، ناصر (۱۳۹۵). قواعد عمومی قراردادها: آثار قرارداد (ج ۳). سهامی انتشار.
۵. محسنی، فرید (۱۳۹۴). حریم خصوصی اطلاعات: مطالعه کیفری در حقوق ایران، ایالات متحده آمریکا، و فقه امامیه. دانشگاه امام صادق (ع).
۶. میرکمالی، سید علی رضا، و صالح احمدی، سحر (۱۴۰۰). قانون مجازات اسلامی در نظم حقوقی کنونی (ج ۲). گالوس.

مقالات

۱. آسمانی، امید، و ابراهیمی، صدیقه (۱۳۹۲). رازداری در علوم پزشکی. اخلاق و تاریخ پزشکی ایران، ۶(۶)، ۶۴-۷۶.
۲. پرویز، محسن، و احتشام، فاطمه (۱۳۹۷). سیر تطور رازداری پزشکی از مطلق بودن به نسبی شدن به روایت تاریخ. فرهنگستان علوم پزشکی، ۲(۲)، ۲۴۸-۲۵۷.
۳. کریمی، عباس؛ رحیمی پور، ایمان؛ و حسنی، مهدی (۱۳۸۹). جرایم پزشکی از راه دور ناشی از سلامت الکترونیک. فصلنامه حقوق پزشکی، ۴(۱۴)، ۴۷-۶۹.
۴. مهدوی نژاد، غلام حسین (۱۳۸۷). رازداری و حدود آن در حرفه پزشکی. اخلاق و تاریخ پزشکی، ۴(۱)، ۱۳-۲۰.
۵. لطیف‌زاده، مهدیه؛ قبولی درافشان، سید محمد مهدی؛ محسنی، سعید؛ و عابدی، محمد (۱۴۰۲). حمایت از داده شخصی در حقوق اتحادیه اروپا و امکان سنجی آن در نظام حقوقی ایران. مطالعات حقوق عمومی، ۵۳(۲)، ۹۸۱-۱۰۰۵. DOI: <https://doi.org/10.22059/jpls.2021.324694.2786>
۶. میرشکاری، عباس، و آزادبخت، شبیر (۱۴۰۱). مطالعه تطبیقی محرمانگی اطلاعات پزشکی متوفیان. مطالعات حقوق تطبیقی معاصر، ۱۳(۲۶)، ۲۶۹-۳۰۰. DOI: 10.22034/law.2021.45522.2874
۷. میرشکاری، عباس؛ آزادبخت، شبیر؛ و پیش‌نماز، سید امین (۱۴۰۳). مطالعه تطبیقی مالیت و مالکیت پرونده‌های الکترونیک سلامت. تحقیق و توسعه در حقوق خصوصی، ۱(۲)، ۲۶۳-۲۹۸. DOI: 10.22034/jpl.2025.720740
۸. نوری یوشانلوئی، جعفر، و آزادبخت، شبیر (۱۴۰۱). تحولات تقنینی مربوط به اصل محرمانگی اطلاعات پزشکی در حقوق ایران و فرانسه. اخلاق و تاریخ پزشکی، ۱۵(۱)، ۲۲۴-۲۳۸.

گزارش‌ها

۱. بختیاری علی آباد، محمد (۱۴۰۱/۰۲/۰۶). بررسی پرونده الکترونیک سلامت در ایران: الزامات قانونی و چالش‌های اجرا. تهران: مرکز پژوهش‌های مجلس شورای اسلامی. ۱۸۱۸۱.
۲. قوانین و مقررات
۳. آیین‌نامه اجرایی قانون انتشار و دسترسی آزاد به اطلاعات (۱۳۹۴). هیئت وزیران. ایران.
۴. آیین‌نامه برنامه اجرایی توسعه و استقرار نظام جامع سلامت الکترونیک (۱۴۰۱). وزارت بهداشت، درمان، و آموزش پزشکی. ایران.

۵. شیوه‌نامه تشخیص و تفکیک اطلاعات مربوط به حریم خصوصی و اطلاعات شخصی از اطلاعات عمومی (۱۳۹۷). کمیسیون انتشار و دسترسی آزاد به اطلاعات. ایران.
۶. قانون انتشار و دسترسی آزاد به اطلاعات (۱۳۸۷). مجلس شورای اسلامی. ایران.
۷. قانون برنامه پنجم توسعه اقتصادی، اجتماعی، و فرهنگی (۱۳۸۹). مجلس شورای اسلامی. ایران.
۸. قانون برنامه چهارم توسعه اقتصادی، اجتماعی، و فرهنگی جمهوری اسلامی ایران (۱۳۸۳). مجلس شورای اسلامی. ایران.
۹. قانون بودجه ۱۴۰۲ کل کشور (۱۴۰۲). مجلس شورای اسلامی. ایران.
۱۰. قانون تجارت الکترونیکی (۱۳۸۲). مجلس شورای اسلامی. ایران.
۱۱. قانون جرایم رایانه‌ای (۱۳۸۸). مجلس شورای اسلامی. ایران.
۱۲. قانون مجازات اسلامی (تعزیرات و مجازات‌های بازدارنده) (۱۳۷۵). مجلس شورای اسلامی. ایران.
۱۳. قانون مدیریت داده‌ها و اطلاعات ملی (۱۴۰۱). مجلس شورای اسلامی. ایران.

اسناد

۱. سند تحول دولت مردمی (۱۴۰۰). مصوب دولت سیزدهم. ایران.
۲. نقشه راه سلامت الکترونیک (۱۳۹۸-۱۴۰۰). وزارت بهداشت، درمان، و آموزش پزشکی ایران. ایران.

ب) انگلیسی

کتاب‌ها

1. Cooke, P. (2007). *Law of Tort*. (8th ed.). Longman.
2. Sperling, D. (2008). *Posthumous Interests; Legal and Ethical Perspective*. Cambridge University Press.

مقالات

1. Alpert, J. S. (2016). The electronic medical record in 2016: Advantages and disadvantages. *Digital Medicine*, 2(2), 48-51.
2. Barrows Jr, R. C., & Clayton P. D. (1996). Privacy, confidentiality, and electronic medical records. *Journal of the American medical informatics association*, 3(2), 139-148.
3. Bauer, K. A. (2009). Privacy and Confidentiality in the Age of E-Medicine. *J. Health Care L. & Pol'y* 12, 47-62.
4. Bayer, R; Santelli J. & Klitzman, R. (2015). New challenges for electronic health records: confidentiality and access to sensitive health information about parents and adolescents. *Jama*, 313(1), 29-30.
5. Bomash, K. (2008). Privacy and public health in the information age: electronic health records and the Minnesota health records act. *Minn. JL Sci. & Tech.* 10, 117-143.
6. Carter, P. I. (1999). Health information privacy: can Congress protect confidential medical information in the information age. *Wm. Mitchell L. Rev.* 25, 223-286.



7. Francis, L. P. (2011). When patients interact with EHRs: problems of privacy and confidentiality. *Hous. J. Health L. & Pol'y*, 12, 171-199.
8. Glenn, C. L. (2000). Protecting health information privacy: the case for self-regulation of electronically held medical records. *Vand. L. Rev.*, 53, 1605-1635.
9. Gostin, L. (1997). Health care information and the protection of personal privacy: ethical and legal considerations. *Annals of Internal Medicine*, 127(8), 683-690.
10. Griener, G. (2005). Electronic health records as a threat to privacy. *Health L. Rev.*, 14, 14-17.
11. Hall, M. A. (2009). Property, privacy, and the pursuit of interconnected electronic medical records. *Iowa L. Rev.*, 95, 631-663.
12. Hiller, J.; McMullen, M. S.; Chumney, W. M. & Baumer D. L. (2011). Privacy and security in the implementation of health information technology (electronic health records): US and EU compared. *BUJ Sci. & Tech. L.*, 17, 1-39.
13. Keshta, I. & Ammar O. (2021). Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal*, 22(2), 177-183.
14. Kruse, C. S.; Smith, B.; Vanderlinden, H. & Nealand, A. (2017). Security techniques for the electronic health records. *Journal of medical systems*, 41, 1-9.
15. Kruser, K. (2007). The adoption of electronic health records: benefits and challenges. *Annals Health L.*, 16, 317-322.
16. Lachmann, P. J. (2003). Consent and confidentiality—where are the limits? An introduction. *Journal of medical ethics*, 29(1), 2-3.
17. Menachemi, N. & Collum, T. H. (2011). Benefits and drawbacks of electronic health record systems. *Risk management and healthcare policy*, 4, 47-55.
18. Mikhail, Z. & Olga, B. (2020). Telemedicine: current state and COVID-19 lessons. *Legal Issues in the digital Age*, 2, 92-143.
19. Miller, S. J. (2008). Electronic Medical Records: How the Potential for Misuse Outweighs the Benefits of Transferability. *J. Health & Biomedical L.*, 4, 353-373.
20. Murdoch, T. B. & Detsky, A. S. (2013). The inevitable application of big data to health care. *Jama*, 309(13), 1351-1352.
21. Oh, S.; Seo, Y.; Lee, E. & Kim, Y. (2021). A comprehensive survey on security and privacy for electronic health data. *International Journal of Environmental Research and Public Health*, 18(18), 1-47.
22. Pasquale, F. & Ragone, T. A. (2013). "Protecting health privacy in an era of big data processing and cloud computing". *Stan. Tech. L. Rev.*, 17, 595-653.
23. Purvi Nema, N. U. S. R. L. & Riya Sinha, N. U. S. R. L. (2021). Privacy And Security Concerns In Electronic Health Records- A Comparative Study Between India And USA. *Journal of Law and Legal Studies*, 1(1), 1-27.
24. Riedl, B.; Neubauer, T.; Goluch, G.; Boehm, O.; Reinauer, G. & Krumboeck, A. (2007). A secure architecture for the pseudonymization of medical data. *In The Second International Conference on Availability, Reliability and Security (ARES'07)*, IEEE, 318-324.
25. Ries, N. M. (2005). Patient privacy in a wired (and wireless) world: Approaches to consent in the context of electronic health records. *Alta. L. Rev.*, 43, 681-712.
26. Ries, N. M., & Moysa, G. (2005). Legal protections of electronic health records: issues of consent and security. *Health L. Rev.*, 14, 18-25.

27. Rothstein, M. A. (2007). Health privacy in the electronic age. *The Journal of legal medicine*, 28(4), 487-501.
28. Shenoy, A. & Appel, J. M. (2017). Safeguarding confidentiality in electronic health records. *Cambridge Quarterly of Healthcare Ethics*, 26(2), 337-341.
29. Steward, M. (2005). Electronic medical records: privacy, confidentiality, liability. *The Journal of legal medicine*, 26(4), 491-506.
30. Terry, N. P. & Francis, L. P. (2017). Ensuring the privacy and confidentiality of electronic health records. *U. Ill. L. Rev.*, 183, 681-735.
31. Terry, N. P. (2014). Big data proxies and health privacy exceptionalism. *Health Matrix*, 24, 65-108.
32. Terry, N. P. (2012). Protecting patient privacy in the age of big data. *UMKC L. Rev.* 81, 385-416.
33. Terry, N. P. (2017). Regulatory disruption and arbitrage in health-care data protection. *Yale J. Health Pol'y L. & Ethics*, 17, 143-207.
34. Turk, M. (2015). Electronic health records: how to suture the gap between privacy and efficient delivery of healthcare. *Brook. L. Rev.*, 80, 565-597.
35. Winn, P. A. (2001). Confidentiality in cyberspace: the HIPAA privacy rules and the common law. *Rutgers LJ*, 33, 617-682.

سایت‌های اینترنتی

1. Centers for Medicare & Medicaid Services, Electronic Health Records, (2023), Availabale at: <https://www.cms.gov/medicare/e-health/ehealthrecords> (Accessed 27 May 2023).

قوانین و مقررات

1. General Data Protection Regulation (GDPR), Made by European Parliament and Council of the European Union, 14 April 2016.
2. The Health Information Technology for Economic and Clinical Health (HITECH), enacted under Title XIII of the American Recovery and Reinvestment Act of 2009, February 17, 2009.
3. The Health Insurance Portability and Accountability Act (HIPAA), Enacted by: the 104th United States Congress, August 21, 1996.
4. The Privacy Act, Enacted by: the 93rd United States Congress, December 31, 1974.



Extended Abstract

Statement of the Problem

Health law, as an interdisciplinary field, seeks to regulate the relationships among individuals, institutions, and the state in matters concerning the protection, provision, and promotion of health. The increasing complexity of healthcare services, the development of new medical technologies, the growth of medical malpractice claims, and the rising importance of patients' rights have made legal analysis in the field of health increasingly significant. This article focuses on one of the key issues in this field and attempts to identify and analyze existing legal and policy gaps.

Research Objective

The aim of this study is to answer the following questions:

First, what is an Electronic Health Record and what types does it include? Second, what are the advantages and benefits of using this record within the healthcare system? Third, what measures exist to safeguard Electronic Health Records? And fourth, what actions have the legal systems of the United States and Iran taken to protect patients' privacy and the confidentiality of Electronic Health Records? Is the existence of Electronic Health Records mandatory in the legal systems of the United States and Iran?

Research Method

This study adopts a descriptive-analytical method. The data and materials used in the article have been collected through library research and the examination of statutes, regulations, policy documents, scholarly articles, and reliable sources in the field of health law. Where necessary, a comparative approach has also been used to analyze the experiences of other legal systems.

Findings

The expansion and integration of modern technologies into the healthcare systems



of different countries appears inevitable, particularly given the significant benefits these technologies bring to improving the efficiency and quality of healthcare services. Nevertheless, the existence of advantages does not imply the absence of shortcomings. In other words, while the use of technology in healthcare can produce valuable outcomes, it is naturally accompanied by certain challenges and risks that should be addressed as far as possible. One of the most important of these challenges concerns the privacy and confidentiality of medical information contained in Electronic Health Records. Some advocates of privacy protection, with the aim of safeguarding these values, take a critical stance toward the use of Electronic Health Records and, in some cases, oppose their use altogether. However, considering the continuous advancement of modern technologies, protecting medical information does not appear to be an unattainable task. It should nonetheless be acknowledged that the adoption of security measures at different levels cannot guarantee absolute protection. In any event, although the Iranian healthcare system appears relatively well provided with legal provisions recognizing the principle of Electronic Health Records and even mandating their implementation, there are still no reliable legal provisions specifically addressing the security and protection of the information contained in such records.

Conclusion

It is advisable that, within the Iranian legal system, legislation in this field should not be limited merely to recognizing the existence of Electronic Health Records. Rather, similar to the approach adopted in the United States, a clear framework should be established to define different levels of security as well as to determine the categories of individuals authorized to access such information. In addition, effective oversight mechanisms should be designed so that any modifications made to Electronic Health Records can be transparently tracked and recorded. Furthermore, the scope of authority of record holders regarding the modification or intervention in the data contained in these records should be clearly defined and regulated through explicit and systematic rules.



References

- Alpert, J. S. (2016). The electronic medical record in 2016: Advantages and disadvantages. *Digital Medicine*, 2(2), 48-51.
- Ansari, B. (2018). The Right of Access to Information: Freedom of Information. *Daftar-e Motale'at va BarnamehRizi-ye Resaneha*. (in Persian)
- Ansari, B. (2021). Privacy Rights. *SAMT*. (in Persian)
- Asemani O, Ebrahimi S. (2014). Medical confidentiality. *IJMEHM*, 6(6), 64-76. (in Persian)
- Bakhtiari Ali-Abad, Mohammad. A Review of Electronic Health Records in Iran: Legal Requirements and Implementation Challenges. Tehran: Islamic Consultative Assembly Research Center, 18181, 26 April 2022. (in Persian)
- Barrows Jr, R. C., & Clayton P. D. (1996). Privacy, confidentiality, and electronic medical records. *Journal of the American medical informatics association*, 3(2), 139-148.
- Bauer, K. A. (2009). Privacy and Confidentiality in the Age of E-Medicine. *J. Health Care L. & Pol'y* 12, 47-62.
- Bayer, R; Santelli J. & Klitzman, R. (2015). New challenges for electronic health records: confidentiality and access to sensitive health information about parents and adolescents. *Jama*, 313(1), 29-30.
- Bomash, K. (2008). Privacy and public health in the information age: electronic health records and the Minnesota health records act. *Minn. JL Sci. & Tech.* 10, 117-143.
- By-Law on the Executive Program for the Development and Implementation of the Comprehensive Electronic Health System (2022). Ministry of Health, Treatment and Medical Education, Iran. (in Persian)
- Carter, P. I. (1999). Health information privacy: can Congress protect confidential medical information in the information age. *Wm. Mitchell L. Rev.* 25, 223-286.
- Centers for Medicare & Medicaid Services, Electronic Health Records, (2023), Available at: <https://www.cms.gov/medicare/e-health/ehealthrecords> (Accessed 27 May 2023).
- Computer Crimes Law (2009). Islamic Consultative Assembly, Iran. (in Persian)
- Cooke, P. (2007). *Law of Tort*. (8th ed.). Longman.
- Directive on the Identification and Separation of Information Related to Privacy and Personal Information from Public Information (2018). Commission on Publication and Free Access to Information, Iran. (in Persian)
- Electronic Commerce Law (2003). Islamic Consultative Assembly, Iran. (in Persian)
- Electronic Health Roadmap (2019–2021). Ministry of Health, Treatment and Medical Education, Iran. (in Persian)
- Executive By-Law of the Law on Publication and Free Access to Information (2015). Council of Ministers, Iran. (in Persian)
- Fifth Economic, Social and Cultural Development Plan Act (2010). Islamic Consultative Assembly, Iran. (in Persian)
- Fourth Economic, Social and Cultural Development Plan of the Islamic Republic of Iran (2004). Islamic Consultative Assembly, Iran. (in Persian)
- Francis, L. P. (2011). When patients interact with EHRs: problems of privacy and confidentiality. *Hous. J. Health L. & Pol'y*, 12, 171-199.
- General Data Protection Regulation (GDPR), Made by European Parliament and Council of the European Union, 14 April 2016.





- Glenn, C. L. (2000). Protecting health information privacy: the case for self-regulation of electronically held medical records. *Vand. L. Rev.*, 53, 1605-1635.
- Gostin, L. (1997). Health care information and the protection of personal privacy: ethical and legal considerations. *Annals of Internal Medicine*, 127(8), 683-690.
- Griener, G. (2005). Electronic health records as a threat to privacy. *Health L. Rev.*, 14, 14-17.
- Hall, M. A. (2009). Property, privacy, and the pursuit of interconnected electronic medical records. *Iowa L. Rev.*, 95, 631-663.
- Hiller, J.; McMullen, M. S.; Chumney, W. M. & Baumer D. L. (2011). Privacy and security in the implementation of health information technology (electronic health records): US and EU compared. *BUJ Sci. & Tech. L.*, 17, 1-39.
- Islamic Penal Code (Ta'zirat and Deterrent Punishments) (1996). Islamic Consultative Assembly, Iran. (in Persian)
- Karimi, A.; Rahimpour, I. & Hassani, M. (2010). Telemedicine Crimes Resulted from Electronic Health. *MLJ*, 4(14), 47-69. (in Persian)
- Katouzian, N. (2016). General Rules of Contracts: Effects of Contracts. Vol. 3. Sahamiye Entehshar. (in Persian)
- Keshta, I. & Ammar O. (2021). Security and privacy of electronic health records: Concerns and challenges. *Egyptian Informatics Journal*, 22(2), 177-183.
- Kruse, C. S.; Smith, B.; Vanderlinden, H. & Nealand, A. (2017). Security techniques for the electronic health records. *Journal of medical systems*, 41, 1-9.
- Kruser, K. (2007). The adoption of electronic health records: benefits and challenges. *Annals Health L.*, 16, 317-322.
- Lachmann, P. J. (2003). Consent and confidentiality—where are the limits? An introduction. *Journal of medical ethics*, 29(1), 2-3.
- Latifzadeh, M.; Qabuli Dorafshan, S. M. M.; Mohseni, S. & Abedi, M. (2023). Protection of Personal Data in EU Law and its Feasibility in the Iranian Legal System. *Public Law Studies Quarterly*, 53(2), 981-1005. DOI: 10.22059/jplsq.2021.324694.2786. (in Persian)
- Law on Publication and Free Access to Information (2008). Islamic Consultative Assembly, Iran. (in Persian)
- Mahdavinejad, G. (2008). Confidentiality in medical profession. *IJMEHM*, 1(4), 13-20. (in Persian)
- Menachemi, N. & Collum, T. H. (2011). Benefits and drawbacks of electronic health record systems. *Risk management and healthcare policy*, 4, 47-55.
- Mikhail, Z. & Olga, B. (2020). Telemedicine: current state and COVID-19 lessons. *Legal Issues in the digital Age*, 2, 92-143.
- Miller, S. J. (2008). Electronic Medical Records: How the Potential for Misuse Outweighs the Benefits of Tranferability. *J. Health & Biomedical L.*, 4, 353-373.
- Mirkamali, S. A. & Saleh Ahmadi, S. (2021). The Islamic Penal Code in the Current Legal Order. Vol. 2. Galus. (in Persian)
- Mirshekari, A. & Azadbakht, S. (2022). A Comparative Study of the Confidentiality of Deceased Persons' Medical Information. *Jurisprudence and Islamic Law*, 13(26), 269-300. DOI: 10.22034/law.2021.45522.2874. (in Persian)
- Mirshkari, A.; Azadbakht, S. & Pishnamaz, S. A. (2025). A Comparative Study of Financial Value and Ownership of Electronic Health Records: A Reflection on American and Iranian Law. *Research and development in private law*, 1(2), 263-298. DOI: 10.22034/

- jpl.2025.720740. (in Persian)
- Mohseni, F. (2015). Information Privacy: A Criminal Law Study in the Legal Systems of Iran, the United States of America, and Imami Jurisprudence. Imam Sadiq University. (in Persian)
- Murdoch, T. B. & Detsky, A. S. (2013). The inevitable application of big data to health care. *Jama*, 309(13), 1351-1352.
- National Budget Law of 1402 (2023). Islamic Consultative Assembly, Iran. (in Persian)
- National Data and Information Management Law (2022). Islamic Consultative Assembly, Iran. (in Persian)
- Nory Yoshanloey, J. & Azadbakht, S. (2022). Legislative Developments of the Confidentiality Principle of Medical Information in Iranian and French Law. *IJMEHM*, 15 (1), 224-238. (in Persian)
- Oh, S.; Seo, Y.; Lee, E. & Kim, Y. (2021). A comprehensive survey on security and privacy for electronic health data. *International Journal of Environmental Research and Public Health*, 18(18), 1-47.
- Parvizi M, & Ehtesham F. (2018). Patient Confidentiality: Is it Trending from Absolute to Partial?. *Iran J Cult Health Promot*, 2 (2), 248-257. (in Persian)
- Pasquale, F. & Ragone, T. A. (2013). "Protecting health privacy in an era of big data processing and cloud computing". *Stan. Tech. L. Rev.*, 17, 595-653.
- Purvi Nema, N. U. S. R. L. & Riya Sinha, N. U. S. R. L. (2021). Privacy And Security Concerns In Electronic Health Records- A Comparative Study Between India And USA. *Journal of Law and Legal Studies*, 1(1), 1-27.
- Riedl, B.; Neubauer, T.; Goluch, G.; Boehm, O.; Reinauer, G. & Krumboeck, A. (2007). A secure architecture for the pseudonymization of medical data. *In The Second International Conference on Availability, Reliability and Security (ARES'07)*, IEEE, 318-324.
- Ries, N. M. (2005). Patient privacy in a wired (and wireless) world: Approaches to consent in the context of electronic health records. *Alta. L. Rev.*, 43, 681-712.
- Ries, N. M., & Moysa, G. (2005). Legal protections of electronic health records: issues of consent and security. *Health L. Rev.*, 14, 18-25.
- Rothstein, M. A. (2007). Health privacy in the electronic age. *The Journal of legal medicine*, 28(4), 487-501.
- Salmanlou, M. (2019). Privacy Rights. Ganje Danesh. (in Persian)
- Sanad-e Tahavvol-e Dowlat-e Mardomi (2021). Approved by the Thirteenth Government, Iran. (in Persian)
- Shenoy, A. & Appel, J. M. (2017). Safeguarding confidentiality in electronic health records. *Cambridge Quarterly of Healthcare Ethics*, 26(2), 337-341.
- Sperling, D. (2008). *Posthumous Interests; Legal and Ethical Perspective*. Cambridge University Press.
- Steward, M. (2005). Electronic medical records: privacy, confidentiality, liability. *The Journal of legal medicine*, 26(4), 491-506.
- Terry, N. P. & Francis, L. P. (2017). Ensuring the privacy and confidentiality of electronic health records. *U. Ill. L. Rev.*, 183, 681-735.
- Terry, N. P. (2012). Protecting patient privacy in the age of big data. *UMKC L. Rev.* 81, 385-416.
- Terry, N. P. (2014). Big data proxies and health privacy exceptionalism. *Health Matrix*, 24, 65-108.



- Terry, N. P. (2017). Regulatory disruption and arbitrage in health-care data protection. *Yale J. Health Pol'y L. & Ethics*, 17, 143-207.
- The Health Information Technology for Economic and Clinical Health (HITECH), enacted under Title XIII of the American Recovery and Reinvestment Act of 2009, February 17, 2009.
- The Health Insurance Portability and Accountability Act (HIPAA), Enacted by: the 104th United States Congress, August 21, 1996.
- The Privacy Act, Enacted by: the 93rd United States Congress, December 31, 1974.
- Turk, M. (2015). Electronic health records: how to suture the gap between privacy and efficient delivery of healthcare. *Brook. L. Rev.*, 80, 565-597.
- Winn, P. A. (2001). Confidentiality in cyberspace: the HIPAA privacy rules and the common law. *Rutgers LJ*, 33, 617-682.



