eduhealthsci: 10.22034/edus.2025.546218.1016

New Approaches in
Educational Management and Health Sciences

Journal Homepage: https://www.eduhealthsci.ir/

Cybercrimes in the Healthcare Sector: An Analysis of Unauthorized Access to Patients' Sensitive Data

Maryam Tahriyan [1], Fatemeh Fathi Ziny [2], Seyyed Amirhossein Nurbakhsh [3]✉

1. Department of Private Law, Behshahr Branch, Islamic Azad University, Behshahr, Iran.
E-mail: tahriyanmarryam@gmail.com
2. Department of Private Law, Behshahr Branch, Islamic Azad University, Behshahr, Iran.
E-mail: fatemeh.fathii89@gmail.com
***3. Corresponding Author**, Department of Private Law, Behshahr Branch, Islamic Azad University, Behshahr, Iran.*
E-mail: www.amir.hosein.2073@gmail.com

Article Info

Article type:
Research

Article history:
Received:
24 Sep 2024
Received in revised form:
11 Nov 2024
Accepted:
07 Dec 2024
Published online:
31 Jan 2024

Keywords:
Cybercrime,
Healthcare,
Crime.

ABSTRACT

Introduction: The digitization of medical records has increased the risk of unauthorized access to patients' sensitive data, posing a significant challenge in the field of healthcare cybercrime. Therefore, this study aimed to investigate cybercrimes in healthcare, focusing on the analysis of unauthorized access to patients' sensitive information.

Methods: This study employed a qualitative–analytical approach to examine the types of unauthorized access, intrusion methods, and their legal and security implications. Data were collected from scientific articles, reports from healthcare organizations, and real case files, and were analyzed using content analysis.

Results: The findings indicate that security vulnerabilities in health information systems and legal shortcomings are the main factors contributing to such crimes. The results can inform the development of policies and strategies to prevent unauthorized access.

Conclusion: Protecting patients' privacy and data in the digital era requires the establishment of a resilient security ecosystem. This ecosystem should be built on three pillars: smart and dynamic laws and regulations that keep pace with technological advancements; robust technical and managerial infrastructures that safeguard data against attacks; and, most importantly, a knowledgeable, responsible, and committed workforce that bridges the first two pillars and serves as the primary line of defense.

Cite this article: Tahriyan M, Fathi Ziny F, Nurbakhsh SA. Cybercrimes in the Healthcare Sector: An Analysis of Unauthorized Access to Patients' Sensitive Data. Journal of Modern Approaches in Education Management and Health Sciences. 2024; 01 (04): 15-25. Doi: 10.22034/edus.2025.546218.1016

eduhealthsci: 10.22034/edus.2025.546218.1016

New Approaches in
Educational Management and Health Sciences

Journal Homepage: https://www.eduhealthsci.ir/

Extended Abstract

Introduction

The ongoing digital transformation of healthcare systems has fundamentally altered the way patient data is collected, stored, and managed. Electronic health records (EHRs) and other digital health information systems have brought numerous benefits, including enhanced accessibility, improved patient care coordination, and streamlined clinical workflows. However, this digitization has also created new vulnerabilities, exposing sensitive patient data to unauthorized access and misuse. Cybercrimes targeting healthcare data have become a critical issue worldwide, as unauthorized access to personal health information can result in severe consequences, including identity theft, financial fraud, reputational damage, and even endangerment of patient safety. Healthcare data is inherently valuable because it contains detailed information about an individual's medical history, treatments, genetic information, and insurance details. Unlike financial data, which can often be reversed or compensated in case of theft, breaches of healthcare data have long-lasting implications, as medical information is permanent and irreplaceable. The prevalence of cyberattacks in healthcare highlights the urgent need to understand the mechanisms through which unauthorized access occurs, identify the vulnerabilities in existing health information systems, and examine the legal and regulatory gaps that exacerbate these risks. Recent studies indicate that healthcare institutions are increasingly targeted due to the combination of high-value data, often outdated IT infrastructures, and insufficient cybersecurity awareness among staff. Intrusion methods vary widely, ranging from phishing and malware attacks to insider threats and exploitation of system misconfigurations. Furthermore, inconsistencies in national and international legislation, as well as fragmented regulatory enforcement, often leave healthcare organizations inadequately protected against cyber threats. Understanding these dynamics is crucial for designing preventive strategies, strengthening security protocols, and safeguarding patient privacy. The primary objective of this study is to analyze cybercrimes in the healthcare sector, focusing specifically on unauthorized access to sensitive patient data. By examining documented cases, relevant literature, and reports from healthcare organizations, this study aims to provide a comprehensive understanding of the factors contributing to such crimes and their broader implications. The insights gained are intended to inform policymakers, IT professionals, and healthcare managers about effective approaches to enhance cybersecurity measures, align organizational practices with legal frameworks, and ultimately protect patient data in an increasingly digitalized healthcare environment.

Methods

This study employed a qualitative–analytical approach to examine the types of unauthorized access, intrusion methods, and their legal and security implications. Data were collected from scientific articles, reports from healthcare organizations, and real case files, and were analyzed using content analysis.

Results

The findings indicate that security vulnerabilities in health information systems and legal shortcomings are the main factors contributing to such crimes. The results can inform the development of policies and strategies to prevent unauthorized access.

Conclusion

The findings of this study underscore that the protection of patient privacy and sensitive health information is a multidimensional challenge that requires a holistic, proactive, and resilient approach. Cybercrimes in healthcare are not merely technological issues but intersect with legal, organizational, and human factors. Security vulnerabilities in electronic health records, outdated software systems, and insufficient access controls are significant contributors to unauthorized data access. Simultaneously, gaps in legal frameworks, inconsistent regulatory enforcement, and limited awareness of cybersecurity best practices amplify the risk of data breaches. Addressing these challenges requires the development of a robust security ecosystem that integrates technological, legal, and human-centered solutions. On the technological front, healthcare institutions must adopt resilient IT infrastructures equipped with advanced threat detection, encryption protocols, multi-factor authentication, and regular vulnerability assessments. These measures are essential to protect data against evolving cyber threats and to ensure system integrity. From a legal and regulatory perspective, the creation of adaptive and dynamic policies is crucial. Laws and regulations must evolve in parallel with technological advancements, providing clear guidance on data protection, accountability, and enforcement mechanisms. Harmonization of international standards, cross-border cooperation, and stringent compliance requirements can help mitigate legal ambiguities that often leave healthcare organizations exposed to cyber threats. Equally important is the role of human capital. Healthcare professionals, administrators, and IT staff must be continuously trained to recognize cyber threats, understand best practices for data security, and adhere to institutional policies. Awareness and accountability are critical,

eduhealthsci: 10.22034/edus.2025.546361.1017

New Approaches in
Educational Management and Health Sciences

Journal Homepage: https://www.eduhealthsci.ir/

as human errors and insider threats remain leading causes of unauthorized access. Cultivating a culture of cybersecurity within healthcare organizations ensures that technology and policies are complemented by informed, responsible, and vigilant personnel. Ultimately, a resilient healthcare security ecosystem relies on the synergistic interaction of technology, law, and human expertise. By prioritizing these three pillars—robust technical infrastructures, adaptive regulatory frameworks, and knowledgeable personnel—healthcare organizations can significantly reduce the risk of unauthorized access, protect patient data, and maintain trust in digital health systems. The implications extend beyond compliance, highlighting the ethical responsibility of safeguarding patient privacy and the critical importance of cybersecurity in modern healthcare delivery.

Ethical Considerations

Funding
This research received no specific grant from any funding agency.

Authors' contribution
Conceptualization, Fatemeh Fathi Ziny; Methodology, Seyyed Amirhossein Nurbakhsh; Analysis, Seyyed Amirhossein Nurbakhsh; Investigation, Seyyed Amirhossein Nurbakhsh; Data Curation, Maryam Tahriyan; Writing - Original Draft Preparation, Fatemeh Fathi Ziny; Supervision, Maryam Tahriyan; Project Administration, Fatemeh Fathi Ziny.

Conflict of interest
The authors declare that there is no conflict of interest regarding this article.

Acknowledgments
The authors of the article express their gratitude to the officials of the Faculty of Private Law Department of Islamic Azad University, Behshahr Branch, for their support in the conduct of this research.

eduhealthsci: 10.22034/edus.2025.546218.1016

نشریه رویکردهای نوین در

مدیریت آموزش و علوم سلامت

لینک مجله :https://www.eduhealthsci.ir/

جرائم سایبری در حوزه سلامت: تحلیل جرم دسترسی غیرمجاز به داده‌های حساس بیماران

مریم طاهریان [۱] ، فاطمه فتحی زینی [۲] ، سید امیرحسین نوربخش [۳]✉

۱. گروه حقوق خصوصی، واحد بهشهر، دانشگاه آزاد اسلامی، بهشهر، ایران. رایانامه: tahriyanmarryam@gmail.com

۲. گروه حقوق خصوصی، واحد بهشهر ، دانشگاه آزاد اسلامی، بهشهر، ایران. رایانامه: fatemeh.fathii89@gmail.com

۳. ***نویسنده مسئول،*** گروه حقوق خصوصی، واحد بهشهر، دانشگاه آزاد اسلامی، بهشهر، ایران. رایانامه: www.amir.hosein.2073@gmail.com

اطلاعات مقاله

نوع مقاله: مقاله پژوهشی

تاریخ دریافت:
۱۴۰۳/ ۰۷/ ۰۳

تاریخ بازنگری:
۱۴۰۳/ ۰۸/ ۲۱

تاریخ پذیرش:
۱۴۰۳/ ۰۹/ ۱۷

تاریخ انتشار:
۱۴۰۳/ ۱۱/ ۱۲

کلیدواژه‌ها:
جرائم سایبری، سلامت، جرم.

چکیده

مقدمه: دیجیتالی شدن پرونده‌های پزشکی، خطر دسترسی غیرمجاز به داده‌های حساس بیماران را افزایش داده و این موضوع به چالشی مهم در حوزه جرائم سایبری سلامت تبدیل شده است؛ لذا هدف این مطالعه بررسی جرائم سایبری در حوزه سلامت: تحلیل جرم دسترسی غیرمجاز به داده‌های حساس بیماران بود.

روش پژوهش: این مطالعه با روش تحلیل کیفی–تحلیلی به بررسی انواع دسترسی غیرمجاز، روش‌های نفوذ و پیامدهای حقوقی و امنیتی آن می‌پردازد. داده‌ها از مقالات علمی، گزارش‌های سازمان‌های بهداشتی و پرونده‌های واقعی گردآوری و با تحلیل محتوا مورد بررسی قرار گرفتند.

یافته‌ها: نتایج نشان می‌دهد که ضعف‌های امنیتی در سامانه‌های اطلاعات سلامت و نقایص قانونی، مهم‌ترین عوامل بروز چنین جرائمی هستند. یافته‌ها می‌توانند به تدوین سیاست‌ها و راهکارهای پیشگیری از دسترسی غیرمجاز کمک کنند.

نتیجه‌گیری: حفاظت از حریم خصوصی و داده‌های بیماران در عصر دیجیتال، نیازمند ایجاد یک اکوسیستم امنیتی تاب‌آور است. این اکوسیستم باید بر سه پایه استوار باشد: قوانین و مقررات هوشمند و پویا که همگام با تحولات فناوری حرکت می‌کنند؛ زیرساخت‌های فنی و مدیریتی مقاوم که از داده‌ها در برابر تهاجمات محافظت می‌نمایند؛ و مهم‌تر از همه، پرورش نیروی انسانی آگاه، مسئول و متعهد که حلقه اتصال این دو بوده و به عنوان اصلی‌ترین سد دفاعی عمل می‌کند.

استناد: طاهریان، مریم؛ فتحی زینی، فاطمه؛ نوربخش، سید امیرحسین. جرائم سایبری در حوزه سلامت: تحلیل جرم دسترسی غیرمجاز به داده‌های حساس بیماران. نشریه رویکردهای نوین در مدیریت آموزش و علوم سلامت. ۱۴۰۳؛ ۰۱ (۰۴): ۱۵–۲۵. Doi: 10.22034/edus.2025.546218.1016

| آدرس نشریه: https://www.eduhealthsci.ir | ایمیل: eduhealthsci@gmail.com

ناشر: جهاد دانشگاهی واحد استان مازندران.

مقدمه

در عصر حاضر، که داده به عنوان سرمایه ای حیاتی محسوب می‌شود، حوزه سلامت شاهد تحولی دیجیتالی بوده است. جایگزینی پرونده‌های کاغذی با سامانه‌های الکترونیک سلامت و پایگاه های داده عظیم، هرچند مدیریت اطلاعات و ارایه خدمات درمانی را تسهیل کرده، اما در مقابل، بستر جدیدی برای ارتکاب جرائم نوظهور فراهم آورده است. در این میان، داده‌های مرتبط با سلامت افراد، به دلیل ماهیت فوق العاده حساس و شخصی، به طعمه ای جذاب برای مجرمان سایبری تبدیل شده‌اند (۱). این داده‌ها که می‌توانند شامل سوابق بیماری، نتایج آزمایشات ژنتیکی، تصویربرداری‌های پزشکی و اطلاعات مالی باشند، نه تنها حریم خصوصی اشخاص را شکل می‌دهند، بلکه افشای غیرمجاز آنها می‌تواند تبعات اجتماعی، روانی و اقتصادی جبران ناپذیری برای اشخاص به دنبال داشته باشد. از این رو، امنیت این داده‌ها به چالشی پیچیده و در عین حال ضروری برای نهادهای درمانی و نظام‌های حقوقی بدل گشته است (۲).

جرم دسترسی غیرمجاز به این داده های حساس، به عنوان یکی از مصادیق بارز جرائم سایبری در حوزه سلامت، تنها یک نقض فنی نیست، بلکه تعرضی مستقیم به حق بنیادین حریم خصوصی و تمامیت روانی افراد محسوب می شود. اهمیت این موضوع زمانی مضاعف می گردد که درک کنیم چنین تهاجمی می تواند امنیت پزشکی بیماران را نیز به مخاطره اندازد؛ دستکاری در داده های پزشکی یا تاریخچه دارویی یک بیمار ممکن است به تجویزهای نادرست و در نهایت به خطر افتادن جان وی منجر شود (۳). از منظر کلان تر، شیوع چنین جرائمی می تواند اعتماد عمومی به سیستم سلامت دیجیتال را که شرط لازم برای توسعه و بهره مندی از مزایای آن است، به شدت تضعیف نماید. هنگامی که بیماران به امنیت اطلاعات خود در سامانه های درمانی اطمینان نداشته باشند، ممکن است از افشای کامل اطلاعات ضروری پزشکی خودداری کنند، که این امر دقت تشخیص و کیفیت درمان را به نحو چشمگیری کاهش خواهد داد (۴). ابعاد این تهدیدات تنها به نقض حریم خصوصی افراد محدود نمی‌شود، بلکه می‌تواند امنیت فیزیکی بیماران را نیز به طور مستقیم به خطر بیندازد. تصور کنید که یک مهاجم سایبری بتواند به سیستم یک بیمارستان دسترسی پیدا کند و نتایج آزمایش‌های پاتولوژی یا دوز داروهای تجویز شده را دستکاری کند. چنین عملی می‌تواند به تشخیص‌های نادرست، تجویزهای خطرناک و در نهایت به آسیب جانی غیرقابل جبران منجر شود. علاوه بر این، وقوع چنین حوادثی اعتماد عمومی به سیستم سلامت دیجیتال را که سنگ بنای توسعه خدمات پزشکی از راه دور و هوش مصنوعی در پزشکی است، به شدت خدشه‌دار می‌کند. هنگامی که بیماران به امنیت اطلاعات خود اطمینان نداشته باشند، ممکن است از افشای کامل اطلاعات ضروری برای درمان خودداری کنند که این امر به طور مستقیم بر کیفیت مراقبت‌های ارائه شده تأثیر منفی خواهد گذاشت.

ضرورت پرداختن آکادمیک به این موضوع از چند جنبه غیرقابل انکار است. سرعت فزاینده تحولات فناوری در حوزه سلامت، همواره بر پیچیدگی این جرائم می افزاید و قوانین موجود را با چالش روزافزونی برای همگامی مواجه می سازد (۵). دوم، فقدان آمار شفاف و مطالعات میدانی جامع در داخل کشور، تصویر واضحی از عمق و گستره این تهدیدات ارایه نمی دهد، که این خلأ، برنامه ریزی برای مقابله مؤثر را دشوار کرده است (۶). سوم، تحلیل کیفی این پدیده از منظر حقوق کیفری می‌تواند به شناسایی خلأهای تقنینی، نقاط ضعف در فرآیند رسیدگی قضایی و همچنین ارایه راهکارهایی برای پیشگیری و افزایش سطح حفاظت از داده های سلامت کمک شایانی نماید (۷). بنابراین، مقاله حاضر با تمرکز بر تحلیل جرم دسترسی غیرمجاز به داده های حساس بیماران، در پی آن است تا با واکاوی دقیق مؤلفه های قانونی، چالش های عملی و تبعات این پدیده مجرمانه، گامی در جهت تقنین هوشمندتر، افزایش امنیت سایبری در نهادهای درمانی و در نهایت، صیانت از حقوق و امنیت بیماران بردارد.

روش‌شناسی

این مطالعه با روش تحلیل کیفی - تحلیلی به بررسی انواع دسترسی غیرمجاز، روش‌های نفوذ و پیامدهای حقوقی و امنیتی آن می‌پردازد. داده‌ها از مقالات علمی، گزارش‌های سازمان‌های بهداشتی و پرونده‌های واقعی گردآوری و با تحلیل محتوا مورد بررسی قرار گرفتند.

یافته‌ها

مبانی مفهومی و ابعاد جرائم سایبری علیه داده‌های سلامت

در دنیای پیوسته دیجیتال امروز، حوزه سلامت به طور فزاینده‌ای به سیستم‌های اطلاعاتی وابسته شده است. این تحول دیجیتال اگرچه دستاوردهای چشمگیری در زمینه بهبود کیفیت مراقبت، تسهیل تحقیقات پزشکی و کاهش خطاهای انسانی به همراه آورده، اما در عین حال بستر جدیدی از آسیب‌پذیری را ایجاد کرده است. داده‌های سلامت به دلیل ماهیت فوق‌العاده حساسی که دارند، به یکی از اهداف جذاب برای مجرمان سایبری تبدیل شده‌اند. این داده‌ها که در قالب پرونده‌های الکترونیک سلامت، نتایج آزمایش‌های پاراکلینیکی، تصویربرداری‌های تشخیصی و اطلاعات ژنتیک ذخیره می‌شوند، تنها محدود به اطلاعات پزشکی نیستند، بلکه اغلب حاوی جزئیات هویتی، مالی و حتی اجتماعی افراد هستند. ارزش این اطلاعات در بازار سیاه بسیار بالا است، چرا که می‌تواند برای اهداف مختلفی از جمله کلاهبرداری مالی، اخاذی، جعل هویت و حتی جاسوسی صنعتی مورد سوء استفاده قرار گیرد.

ماهیت جرائم سایبری در این حوزه با چالش‌های مفهومی عمیقی همراه است. از یک سو، تعریف دقیق «داده حساس سلامت» نیازمند توجه به ابعاد اخلاقی، حقوقی و فنی است. آیا تمامی اطلاعات موجود در یک سامانه درمانی حساس محسوب می‌شوند؟ چگونه می‌توان بین داده‌های عادی و داده‌های با حساسیت فوق‌العاده تمایز قائل شد؟ از سوی دیگر، مفهوم «دسترسی غیرمجاز» خود دارای درجات و اشکال مختلفی است. این دسترسی می‌تواند از یک کنجکاوی ساده توسط یک کارمند تا یک حمله سازمان‌یافته توسط گروه‌های مجرمانه بین‌المللی را شامل شود. انگیزه‌های این جرائم نیز بسیار متنوع است و می‌تواند شامل انتقام‌جویی، سود مالی، جاسوسی رقابتی بین شرکت‌های دارویی یا حتی اهداف سیاسی باشد. این پیچیدگی در انگیزه و روش، مقابله با این پدیده را دشوار می‌سازد.

از دیدگاه کلان‌تر، جرائم سایبری علیه داده‌های سلامت را می‌توان یک تهدید علیه امنیت ملی تلقی کرد. یک حمله گسترده به زیرساخت‌های سلامت یک کشور می‌تواند منجر به اختلال در ارائه خدمات حیاتی، ایجاد هرج و مرج و بی‌اعتمادی عمومی شود. بنابراین، درک مبانی مفهومی این جرائم تنها به عنوان یک موضوع تخصصی در حقوق یا فناوری اطلاعات نیست، بلکه لازمه‌ای اساسی برای تدوین سیاست‌های امنیتی، قوانین بازدارنده و پروتکل‌های حفاظتی است که از منافع فردی بیماران تا ثبات نظام سلامت یک کشور را تحت پوشش قرار می‌دهد. این درک جامع اولین گام ضروری برای هرگونه اقدام موثر در جهت مقابله با این چالش رو به رشد است (۵).

تحلیل قانونی جرم دسترسی غیرمجاز در نظام حقوقی ایران

در نظام حقوقی ایران، تحلیل جرم دسترسی غیرمجاز به داده‌های سلامت مستلزم بررسی در چارچوب قوانین عام و خاص مرتبط با فضای سایبری و نیز مقررات ناظر بر اطلاعات پزشکی است. پایه اصلی قانونی این جرم، قانون جرائم رایانه‌ای مصوب ۱۳۸۸ است که به‌طور خاص به جرائم سایبری پرداخته است. ماده ۱ این قانون، دسترسی غیرمجاز را به‌عنوان اولین و اساسی‌ترین جرم سایبری معرفی می‌کند. بر این اساس، هرکس به طور غیرمجاز به داده‌ها یا سامانه‌های رایانه‌ای یا مخابراتی

که به وسیله تدابیر امنیتی حفاظت شده است، دسترسی یابد، مرتکب جرم شده است. داده‌های سلامت، به دلیل ماهیت حساس و ضرورت محرمانگی، قطعاً در زمره داده‌هایی قرار می‌گیرند که مشمول "تدابیر امنیتی" می‌شوند، حتی اگر این تدابیر در یک نهاد درمانی ضعیف یا ناقص پیاده‌سازی شده باشد. صرف وجود این داده‌ها در یک سامانه، ضرورت وجود حفاظت را ایجاب می‌کند و نقض این حریم، مصداق بارز دسترسی غیرمجاز است.

برای تحقق رکن مادی این جرم، صرف عمل دستیابی غیرقانونی کافی است و نیاز به وقوع نتیجه خاصی مانند افشا یا سرقت داده نیست. این امر، اهمیت قاعده مند کردن این جرم را نشان می‌دهد، چرا که همان لحظه نفوذ، ارزش کیفری پیدا می‌کند. در کنار این قانون عام، قوانین خاص دیگری نیز وجود دارند که بر حفاظت از داده‌های سلامت تأکید دارند. قانون نحوه انتشار و دسترسی به اطلاعات سلامت مصوب ۱۳۹۲، به‌طور مشخص بر لزوم محرمانگی اطلاعات بیماران و محدودیت دسترسی به آن تأکید کرده است. این قانون، دسترسی به این اطلاعات را منحصر به افرادی می‌داند که به‌طور مستقیم در فرآیند درمان بیمار نقش دارند یا به موجب قانون مجاز هستند. بنابراین، هرگونه دسترسی خارج از این چارچوب، مثلاً توسط یک کارمند اداری که نیازی به این داده‌ها ندارد یا یک فرد خارج از سازمان، مصداق بارز "دسترسی غیرمجاز" خواهد بود، حتی اگر این دسترسی از داخل خود سازمان و با استفاده از شناسه کاربری شخصی صورت گرفته باشد.

علاوه بر این، اگر جرم دسترسی غیرمجاز، مقدمه ای برای ارتکاب جرائم دیگری مانند اخاذی، افشای اطلاعات یا کلاهبرداری باشد، کیفیات مشدده دیگری نیز قابل اعمال خواهد بود. از منظر مسئولیت اشخاص حقوقی، ماده ۱۹ قانون جرائم رایانه‌ای، نهادهای درمانی را نیز می‌توان در قبال این جرم مسئول دانست. اگر ثابت شود که بیمارستان یا کلینیک به دلیل عدم اجرای تدابیر امنیتی لازم و استاندارد—مانند رمزنگاری داده‌ها، کنترل سطوح دسترسی یا آموزش پرسنل—زمینه ارتکاب جرم را فراهم کرده است، این شخص حقوقی به مجازات هایی از قبیل پرداخت جریمه نقدی، تعلیق پروانه یا مصادره اموال محکوم خواهد شد. این امر اهمیت مدیریت ریسک و سرمایه‌گذاری در امنیت سایبری را برای ارائه‌دهندگان خدمات سلامت دوچندان می‌کند. در نهایت، رویه قضایی ایران در برخورد با این جرم در حال تکوین است و پرونده‌های معدودی به طور خاص در حوزه سلامت به نتیجه رسیده‌اند. با این حال، با افزایش حساسیت‌ها و وقوع حوادث عینی، انتظار می‌رود دادگاه‌ها با تفسیری منطبق با ضرورت‌های روز و حفاظت از حقوق بیماران، به سمت تشدید برخورد با مرتکبان این جرائم حرکت کنند (۹).

در تحلیل رکن معنوی این جرم، باید به سوءنیت عام مرتکب توجه داشت. یعنی فرد با علم و آگاهی نسبت به غیرمجاز بودن دسترسی خود، اقدام به این عمل کند. این آگاهی می‌تواند از قوانین داخلی بیمارستان، موافقت‌نامه‌های امضا شده توسط کارکنان یا حتی ذات آشکارا خصوصی داده‌ها ناشی شود. در خصوص مجازات، ماده ۱ قانون جرائم رایانه‌ای، حبس از نود و یک روز تا شش ماه یا جزای نقدی از پنج تا ده میلیون ریال یا هر دو مجازات را پیش‌بینی کرده است. اما نکته حائز اهمیت، شدت عمل قانون در مواردی است که این دسترسی غیرمجاز به منظور تحصیل داده‌های سری یا حساس صورت گیرد. با استناد به ماده ۳ همین قانون، اگر داده‌های بهدست‌آمده، جزو داده‌های سری مطابق قانون باشد، مجازات مشدد خواهد بود. داده‌های سلامت، به ویژه موارد مرتبط با بیماری‌های خاص، ژنتیک یا موضوعات با حساسیت اجتماعی بالا، می‌توانند با تفسیر قضایی گسترده، تحت عنوان "داده‌های سری" قرار گیرند که مجازات مرتکب را به حبس از شش ماه تا دو سال افزایش می‌دهد (۴).

راهکارهای فنی و مدیریتی برای پیشگیری و حفاظت از داده‌ها

حفاظت از داده‌های حساس سلامت در برابر تهدیدات سایبری نیازمند به کارگیری راهبردی چندسطحی و همه‌جانبه است که همزمان به ابعاد فنی، مدیریتی و انسانی توجه کند. در بعد فنی، اجرای تمهیدات امنیتی نیرومند نخستین خط دفاع به شمار می‌رود. به کارگیری رمزنگاری کامل برای داده‌ها چه در حالت ذخیره و چه در حال انتقال، اقدامی اجتناب‌ناپذیر است. این کار

تضمین می‌کند که حتی در صورت رخنه به سامانه، داده‌های ربوده شده برای مهاجم بی‌فایده باشند. استقرار سامانه‌های کنترل دسترسی بر پایه اصل کمترین دسترسی نیز بسیار حیاتی است؛ بدین معنا که هر کاربر تنها به حداقل داده‌ها و امکاناتی دسترسی دارد که برای انجام وظایفش کاملاً ضروری است. این رویکرد، سطح آسیب‌پذیری را به شکل چشمگیری کاهش می‌دهد. افزون بر این، استفاده از روش‌های پیشرفته تأیید هویت چندعاملی برای ورود به سامانه‌های دارای اطلاعات حساس، به ویژه برای کارکنان دارای دسترسی سطوح بالا، یک ضرورت انکارناپذیر است. پایش بی‌وقفه ترافیک شبکه و ثبت و تحلیل گزارش‌های دسترسی برای شناسایی رفتارهای غیرمعمول و مشکوک نیز امکان کشف به موقع رخنه‌ها را فراهم می‌آورد (۱). از نگاه مدیریتی، تنظیم و اجرای سیاست‌های روشن امنیت اطلاعات، چارچوبی برای همه اقدامات حفاظتی پدید می‌آورد. این سیاست‌ها باید به روشنی نقش‌ها و مسئولیت‌ها، پروتکل‌های واکنش به رویدادهای امنیتی و ضوابط برخورد با نقض داده‌ها را تعریف کنند. انجام منظم ارزیابی خطر و آزمون نفوذپذیری به شناسایی نقاط ضعف پیش از بهره‌برداری مجرمانه کمک بزرگی می‌کند. انعقاد پیمان‌های محرمانگی الزام‌آور با همه کارکنان، پیمانکاران و شرکای خارجی که به گونه‌ای به داده‌ها دسترسی دارند، یک نیاز مدیریتی کلیدی است. همچنین، داشتن یک برنامه بازیابی پس از رویدادهای اضطراری و پشتیبان‌گیری منظم و امن از داده‌ها، اطمینان می‌دهد که در صورت رخداد یک حمله سایبری جدی مانند باج‌افزار، تداوم ارائه خدمات امکان‌پذیر باشد (۳).

اما هیچ راهکار فنی و مدیریتی بدون توجه به عامل انسانی به نتیجه مطلوب نمی‌رسد. از این رو، سرمایه‌گذاری پیوسته بر آموزش و افزایش آگاهی کارکنان، مهم‌ترین بخش این راهبرد است. آموزش‌ها نباید به صورت موردی و ظاهری باشند، بلکه باید مستمر، کاربرمحور و دربرگیرنده شبیه‌سازی حملات فیشینگ و آزمون‌های سنجش آگاهی باشند. کارکنان باید به طور مکرر درباره انواع تهدیدات، روش‌های شناسایی رایانامه‌ها و پیام‌های مشکوک، اهمیت استفاده از گذرواژه‌های نیرومند و پروتکل‌های گزارش‌دهی رویدادهای امنیتی آموزش ببینند. ایجاد یک فرهنگ امنیتی در درون سازمان که در آن هر کارمند خود را مسئول حفاظت از داده‌ها بداند و بدون ترس از بازخواست، خطاها و رویدادهای احتمالی را گزارش کند، به همان اندازه اجرای دیواره‌های آتش پیشرفته اهمیت دارد. در پایان، این پیوند هماهنگ فناوری، فرآیند و افراد است که می‌تواند یک محیط امن و تاب‌آور را در برابر تهدیدات پیچیده سایبری پدید آورد.

چالش‌های فرآیند اثبات و پیگرد قضایی جرم

پیگرد قضایی و اثبات جرم دسترسی غیرمجاز به داده‌های حساس سلامت در محاکم قضایی با چالش‌های متعددی روبرو است که این چالش‌ها ناشی از ماهیت خاص این جرائم و ساختارهای حاکم بر فضای سایبری است. یکی از عمده‌ترین مشکلات، استنادپذیری ادله دیجیتال و حفظ تمامیت آن در طول فرآیند دادرسی است. برخلاف ادله ملموس در جرائم سنتی، داده‌های دیجیتال به سادگی قابل تغییر، حذف یا جعل هستند و کوچک‌ترین خطا در جمع‌آوری یا نگهداری آنها می‌تواند به بی‌اعتباری کامل ادله بینجامد. فقدان زیرساخت‌های مناسب برای کشف و جمع‌آوری علمی ادله دیجیتال در مراجع قضایی و انتظامی، این چالش را تشدید می‌کند.

از سوی دیگر، شناسایی مرتکبان واقعی این جرائم به دلیل استفاده از روش‌های پنهان‌سازی هویت مانند فناوری‌های ناشناس‌ساز یا آی‌پی‌های جعلی، با دشواری‌های فنی بسیاری همراه است. مجرمان سایبری اغلب از قلمروهای قضایی مختلف عمل می‌کنند که همکاری بین‌المللی برای ردیابی و دستگیری آنها را پیچیده می‌سازد. حتی در مواردی که هویت مرتکب مشخص شود، اثبات قصد مجرمانه و سوءنیت وی در دادگاه می‌تواند چاره‌ساز باشد، چرا که در بسیاری از موارد، دسترسی غیرمجاز ممکن است به اشتباه یا از روی غفلت رخ داده باشد.

چالش دیگر، عدم تخصص کافی در میان ضابطان قضایی، بازپرسان و حتی قضات در برخورد با پرونده‌های پیچیده سایبری است. درک فنی دقیق از نحوه عملکرد سامانه‌های اطلاعاتی، روش‌های نفوذ و شیوه‌های ردیابی، برای رسیدگی عادلانه به این پرونده‌ها ضروری است که متأسفانه در بسیاری از موارد این تخصص وجود ندارد. این امر منجر به طولانی شدن فرآیند رسیدگی، اتکای بیش از حد به نظر کارشناسان خارجی و در نهایت ممکن است به صدور آرای غیرمنطبق با واقعیت‌های فنی بینجامد. همچنین، عدم وجود سازوکارهای گزارش‌دهی شفاف و یکپارچه از سوی نهادهای درمانی، کشف این جرائم را با مشکل مواجه ساخته است. بسیاری از نقض‌های امنیتی به دلیل ترس از آسیب به اعتبار مؤسسه یا پیچیدگی‌های قانونی، گزارش نمی‌شوند که این امر امکان جمع‌آوری آمار واقعی و اتخاذ اقدامات پیشگیرانه را کاهش می‌دهد. در نهایت، ناکافی بودن مجازات‌های پیش‌بینیشده در قوانین فعلی برای جرائم سایبری سلامت، به ویژه در مقایسه با خسارات گسترده‌ای که این جرائم می‌توانند وارد آورند، انگیزه بازدارندگی لازم را برای مجرمان ایجاد نمی‌کند. این چالش‌ها در کنار یکدیگر، فرآیند اثبات و پیگرد قضایی این جرائم را به مسیری دشوار و پرمانع تبدیل کرده است (۴).

نقش آموزش و فرهنگ‌سازی در کاهش تهدیدات سایبری

نقش آموزش و فرهنگ‌سازی در کاهش تهدیدات سایبری در حوزه سلامت، به ویژه در حفاظت از اطلاعات بیماران، از جایگاه بی‌بدیلی برخوردار است. اگرچه راهکارهای فنی و سخت‌افزاری لازمه اولیه تأمین امنیت هستند، اما این اقدامات به تنهایی کافی نیستند. تجربه نشان داده است که انسان به عنوان ضعیف‌ترین حلقه در زنجیره امنیتی، اغلب نقطه شکست محسوب می‌شود. یک خطای ساده انسانی، مانند باز کردن یک پیوست آلوده یا افشای غیرعمدی گذرواژه، می‌تواند تمامی تدابیر پیچیده امنیتی را بی‌اثر کند و حریم خصوصی هزاران بیمار را به مخاطره بیندازد. اینجاست که آموزش مستمر و هدفمند پرسنل به عاملی تعیین‌کننده تبدیل می‌شود.

آموزش در این حوزه نباید صرفاً به ارائه یک سری دستورالعمل خشک و اداری محدود شود. بلکه باید به گونه‌ای طراحی گردد که برای پرسنل حوزه سلامت (از پزشک و پرستار تا نیروهای اداری) ملموس و کاربردی باشد. کارکنان باید به طور شفاف درک کنند که چگونه یک نقض امنیتی، نه تنها یک مشکل فنی برای بخش فناوری اطلاعات، بلکه یک تهدید جدی برای ایمنی و سلامت بیماران محسوب می‌شود. برای مثال، دستکاری غیرمجاز در داده‌های پزشکی یک بیمار می‌تواند به تجویز نادرست دارو، تشخیص اشتباه یا به تأخیر افتادن درمان منجر شود و مستقیماً جان فرد را به خطر بیندازد. یا افشای اطلاعات مربوط به یک بیماری خاص می‌تواند موجب بروز تبعات اجتماعی شدید و آسیب‌های روانی جبران‌ناپذیر برای بیمار گردد (۶).

فرهنگ‌سازی نیز گام مکمل و ضروری پس از آموزش است. هدف نهایی باید ایجاد یک "فرهنگ امنیتی" در سراسر سازمان باشد؛ فرهنگی که در آن هر فرد، خود را مسئول و نگهبان اطلاعات بیماران بداند و امنیت سایبری به یک ارزش نهادینه شده و بخشی از استانداردهای روزمره ارائه خدمات درمانی تبدیل شود. این امر مستلزم تعهد و حمایت بی‌قید و شرط مدیریت ارشد سازمان است. رهبران مؤسسات درمانی باید با اختصاص منابع کافی، تقدیر از رفتارهای مسئولانه و ایجاد فضای اعتماد—به طوری که کارکنان بدون ترس از عواقب، خطاها و حوادث امنیتی را گزارش کنند—زمینه این تحول فرهنگی را فراهم آورند.

برنامه‌های آموزشی مؤثر شامل دوره‌های منظم به‌روزرسانی شده، شبیه‌سازی حملات فیشینگ، و کارگاه‌های عملی برای پاسخ به حوادث امنیتی است. این برنامه‌ها باید به زبانی ساده و بدون اصطلاحات پیچیده فنی ارائه شوند و بر مسئولیت اخلاقی و قانونی هر فرد در قبال حفظ اسرار بیماران تأکید کنند. وقتی که پرسنل به طور کامل درک کنند که حفاظت از داده‌ها، در واقع حفاظت از خود بیماران است، انگیزه درونی بسیار قوی‌تری برای رعایت پروتکل‌های امنیتی پیدا خواهند کرد. در نهایت، سرمایه‌گذاری بر آموزش و فرهنگ‌سازی، نه یک هزینه، بلکه یک سرمایه‌گذاری اساسی برای ایجاد اعتماد، حفظ اعتبار مؤسسه و مهم‌تر از همه، تضمین ایمنی و حقوق بیماران است.

نتیجه‌گیری

با توجه به مباحث مطروحه، می‌توان دریافت که مقابله با جرم دسترسی غیرمجاز به داده‌های حساس سلامت، تنها از طریق یک رویکرد یک‌بعدی و متمرکز بر فناوری میسر نیست. این چالش چندوجهی، نیازمند پاسخی جامع و هماهنگ است که در آن حقوق بیماران در کانون توجه قرار گیرد. یافته‌های این تحقیق نشان می‌دهد که اگرچه وجود چارچوب‌های قانونی شفاف و بازدارنده، همچون قانون جرائم رایانه‌ای، شرط لازم برای پیگرد قضایی است، اما این امر به تنهایی کافی نیست. چالش‌های عملی در فرآیند اثبات، از جمله دشواری در حفظ تمامیت ادله دیجیتال و ناکافی بودن تخصص‌های فنی در دستگاه قضایی، گواه این مدعاست (۲). یافته‌های این تحقیق نشان می‌دهد که راهکارهای فنی و مدیریتی، هرچند ضروری، در صورت عدم همراهی با سرمایه‌گذاری بر عنصر انسانی، ناقص خواهند بود. آموزش مستمر و فرهنگ‌سازی هدفمند میان تمامی دست‌اندرکاران حوزه سلامت، از پزشک تا نیروی اداری، به عنوان مؤثرترین ابزار پیشگیرانه شناسایی شده است. هنگامی که پرسنل به درکی عمیق از پیوند ناگسستنی بین امنیت داده‌ها و ایمنی فیزیکی و روانی بیماران نائل آیند، نه به عنوان یک الزام اداری، بلکه به عنوان یک مسئولیت اخلاقی، پروتکل‌های امنیتی را رعایت خواهند کردکه با نتایج تحقیقات فرورلی (Ferorelli) و همکاران (۲۰۱۹) (۳) همسو و همراستاست. در نتیجه، می‌توان ادعا کرد که حفاظت از حریم خصوصی و داده‌های بیماران در عصر دیجیتال، نیازمند ایجاد یک اکوسیستم امنیتی تاب‌آور است. این اکوسیستم باید بر سه پایه استوار باشد: قوانین و مقررات هوشمند و پویا که همگام با تحولات فناوری حرکت می‌کنند؛ زیرساخت‌های فنی و مدیریتی مقاوم که از داده‌ها در برابر تهاجمات محافظت می‌نمایند؛ و مهم‌تر از همه، پرورش نیروی انسانی آگاه، مسئول و متعهد که حلقه اتصال این دو بوده و به عنوان اصلی‌ترین سد دفاعی عمل می‌کند. تنها در سایه چنین نگرش جامعی می‌توان اعتماد عمومی را به سیستم سلامت دیجیتال تقویت کرد و از حقوق و سلامتی بیماران به عنوان عالی‌ترین ارزش، صیانت نمود.

ملاحظات اخلاقی

حامی مالی

این تحقیق هیچ بودجه‌ای دریافت نکرده است.

مشارکت نویسندگان

مفهوم سازی، فاطمه فتحی زینی؛ روش شناسی، سید امیرحسین نوربخش؛ تحلیل، سید امیرحسین نوربخش؛ تحقیق، سید امیرحسین نوربخش؛ مدیریت داده، مریم طاهریان؛ نگارش - تهیه پیش نویس اصلی، فاطمه فتحی زینی؛ سرپرستی، مریم طاهریان؛ مدیریت پروژه، فاطمه فتحی زینی.

تعارض منافع

بنابر اظهار نویسنده، این مقاله تعارض منافع ندارد.

تشکر و قدردانی

نویسندگان مقاله مراتب قدردانی خود را از مسئولین دانشکده حقوق دانشگاه آزاد اسلامی واحد بهشهر در اجرای این پژوهش ابراز می‌دارند.

References

1. Skinner GCM, Farrington DP. The healthcare plight of offenders in the community. Crim Behav Ment Health. 2022;32(4):249-254. doi: 10.1002/cbm.2258

2. Raj A. Streamlining healthcare delivery for sex-trafficked adolescents. Curr Probl Pediatr Adolesc Health Care. 2024;54(2):101553. doi: 10.1016/j.cppeds.2023.101553
3. Ferorelli D, Celentano FE, Benevento M, Dell'Erba A, Solarino B. Destruction of telecommunications hinders access to healthcare: A crime against humanity? J Telemed Telecare. 2023;29(1):72. doi: 10.1177/1357633X221103829
4. Pratt C, Taylor R, Smith SD. Health Equity and Access to Health Care as a Social Determinant of Health: The Role of the Primary Care Provider. Prim Care. 2023;50(4):549-559. doi: 10.1016/j.pop.2023.04.006
5. Neprash HT, McGlave CC, Cross DA, Virnig BA, Puskarich MA, Huling JD, Rozenshtein AZ, Nikpay SS. Trends in Ransomware Attacks on US Hospitals, Clinics, and Other Health Care Delivery Organizations, 2016-2021. JAMA Health Forum. 2022;3(12):e224873. doi: 10.1001/jamahealthforum.2022.4873
6. Ullah F, Srivastava G, Xiao H, Ullah S, Lin JC, Zhao Y. A Scalable Federated Learning Approach for Collaborative Smart Healthcare Systems With Intermittent Clients Using Medical Imaging. IEEE J Biomed Health Inform. 2024;28(6):3293-3304. doi: 10.1109/JBHI.2023.3282955
7. Ewoh P, Vartiainen T. Vulnerability to Cyberattacks and Sociotechnical Solutions for Health Care Systems: Systematic Review. J Med Internet Res. 2021;26:e46904. doi: 10.2196/46904
8. Kim L. Cybercrime, ransomware, and the role of the informatics nurse. Nursing. 2020;50(3):63-65. doi: 10.1097/01.NURSE.0000654064.67531.c5
9. Aljuraid R, Justinia T. Classification of Challenges and Threats in Healthcare Cybersecurity: A Systematic Review. Stud Health Technol Inform. 2022 ;295:362-365. doi: 10.3233/SHTI220739