Journal of Payavard Salamat
Vol. 19, No. 6; Feb. 2026: 552-564

Assessment of Hospital Information System's Compliance with Physical and Technical Safeguards for Health Data: A Study at Birjand University of Medical Sciences in 2024

Ahmad Negahban[1] (Ph.D.), Azam Salehzadeh[2] (M.S.), Razieh Farrahi[1] (Ph.D.), Alireza Nourozi[3] (B.S.), Sina Tavakoli[3] (B.S.)

1 Assistant Professor, Department of Health Information Technology, Ferdows Faculty of Medical Sciences, Birjand University of Medical Sciences, Birjand, Iran
2 Ph.D. Candidate in Health Information Management, School of Health Management and Information Sciences, Iran University of Medical Sciences, Tehran, Iran
3 Bachelor of Sciences Student in Health Information Technology, Student Research Committee, Birjand University of Medical Sciences, Birjand, Iran

Abstract

Received: 25 May. 2025

Accepted: 28 Dec. 2025

Background and Aim: With the digitalization of healthcare, hospital information systems handle vast amounts of sensitive data, making their protection crucial. This study aimed to assess the compliance of these systems in hospitals affiliated with Birjand University of Medical Sciences with the physical and technical safeguard standards of Health Insurance Portability and Accountability Act (HIPAA) in 2024.

Materials and Methods: This cross-sectional descriptive study was conducted in 15 hospitals affiliated with Birjand University of Medical Sciences. The study population consisted of Information Technology (IT) unit managers, who were selected using a census method (15 individuals). The research instrument was a researcher-developed checklist consisting of 56 items based on the physical and technical standards of HIPAA. The face validity of the checklist was confirmed by five experts in Health Information Management, Medical Informatics, and Health Policy, and its reliability was verified with a Cronbach's alpha coefficient of 0.84. Data were analyzed using SPSS software and descriptive statistics, including frequency, percentage, mean, and standard deviation.

Results: A total of 15 information technology managers (14 men and 1 woman) from 15 hospitals, including 8 teaching and 7 non-teaching hospitals, participated in the study. The findings showed that the hospital information systems of Birjand University of Medical Sciences complied with the HIPAA physical and technical safeguard standards at rates of 81.7% and 86.7%, respectively. In the domain of physical safeguards, the workstation security standard demonstrated the highest level of compliance, with a mean score of 89.3%. Full compliance (100%) was observed for certain indicators, including emergency access procedures for facilities and physical access control procedures. In contrast, the lowest compliance in this domain was related to the device and media controls standard, with a mean score of 74.9%, particularly in the identification and tracking of hardware and electronic media. In the domain of technical safeguards, the overall mean compliance rate was 86.7%. Among these standards, person or entity authentication achieved the highest level of compliance, with all hospitals demonstrating full compliance (100%). In addition, access control (93.3%), audit controls (86.7%), and transmission security (85.3%) were all at desirable levels. However, the lowest compliance was observed for the integrity standard (50%), highlighting the need to strengthen technical infrastructure and implement more advanced electronic mechanisms to ensure data accuracy and integrity.

Conclusion: Although the overall level of compliance in the hospitals under study is satisfactory, significant gaps remain, particularly in device and media control and data integrity. These deficiencies may lead to breaches of patient privacy and undermine public trust in the healthcare system. It is recommended that senior hospital managers and health policymakers address these deficiencies by developing and implementing clear internal guidelines, investing in appropriate supportive technologies, and conducting continuous, targeted training programs for all personnel. In addition, periodic compliance monitoring is essential to ensure continuous improvement.

Keywords: Hospital Information System, Data Security, Compliance, HIPAA, Privacy, Health Information Technology

*** Corresponding Author:**
Farrahi R
Email:
Farrahi1@bums.ac.ir

مجله پیاورد سلامت
دوره ۱۹، شماره ۶؛ بهمن ۱۴۰۴؛ ۵۶۴-۵۵۲
مقاله پژوهشی

ارزیابی انطباق سیستم اطلاعات بیمارستان‌های دانشگاه علوم پزشکی بیرجند با استانداردهای حفاظت فیزیکی و فنی داده‌های سلامت در سال ۱۴۰۳

احمد نگهبان[۱]، اعظم صالح‌زاده[۲]، راضیه فرهی[۱*]، علیرضا نوروزی[۳]، سینا توکلی[۳]

چکیده

زمینه و هدف: با دیجیتالی شدن خدمات سلامت، سیستم‌های اطلاعات بیمارستانی حجم زیادی از داده‌های حساس را پردازش و مدیریت می‌کنند؛ بنابراین حفاظت از این اطلاعات امری بسیار حیاتی است. این مطالعه با هدف ارزیابی میزان انطباق سیستم اطلاعات بیمارستانی در بیمارستان‌های دانشگاه علوم پزشکی بیرجند با استانداردهای حفاظت فیزیکی و فنی قانون قابلیت انتقال و پاسخ‌گویی بیمه‌های سلامت (HIPAA) در سال ۱۴۰۳ انجام شد.

روش بررسی: این، مطالعه‌ای توصیفی- مقطعی بود که در ۱۵ بیمارستان آموزشی و غیرآموزشی تابعه دانشگاه علوم پزشکی بیرجند انجام گرفت. جامعه پژوهش، مدیران واحد فناوری اطلاعات بیمارستان بودند که به‌روش تمام‌شماری(۱۵ نفر) انتخاب شدند. ابزار پژوهش، چک‌لیستی محقق‌ساخته شامل ۵۶ گویه بر اساس استاندارد فیزیکی و فنی HIPAA بود که روایی صوری چک‌لیست با بررسی ۵ نفر متخصص مدیریت اطلاعات سلامت، انفورماتیک پزشکی و سیاست‌گذاری سلامت تأیید و پایایی آن با آلفای کرونباخ ۰/۸۴ تأیید گردید. داده‌ها با نرم‌افزار SPSS و با استفاده از آمار توصیفی(فراوانی، درصد، میانگین و انحراف‌معیار) تحلیل شدند.

یافته‌ها: در مجموع ۱۵ نفر از مدیران واحد فناوری اطلاعات(۱۴ مرد و ۱ زن) از ۸ بیمارستان آموزشی و ۷ بیمارستان غیرآموزشی در مطالعه شرکت نمودند. یافته‌ها نشان داد که میزان انطباق سیستم اطلاعات بیمارستان‌های دانشگاه علوم پزشکی بیرجند با استانداردهای حفاظت فیزیکی و فنی HIPAA به‌ترتیب ۸۱/۷ و ۸۶/۷ درصد بود. در حوزه حفاظت فیزیکی، استاندارد امنیت ایستگاه کاری با میانگین ۸۹/۳ درصد بالاترین میزان انطباق را داشت و در برخی شاخص‌ها، از جمله وجود رویه‌های دسترسی اضطراری به تأسیسات و روش‌های کنترل دسترسی فیزیکی، انطباق کامل(۱۰۰ درصد) مشاهده شد. در مقابل، کمترین میزان انطباق در این حوزه مربوط به استاندارد کنترل‌های دستگاه و رسانه با میانگین ۷۴/۹ درصد بود، به‌ویژه در زمینه شناسایی و ردیابی سخت‌افزارها و رسانه‌های الکترونیکی. در حوزه حفاظت فنی، میانگین انطباق کلی ۸۶/۷ درصد به‌دست آمد؛ به‌گونه‌ای که استاندارد احراز هویت با انطباق کامل(۱۰۰ درصد) بالاترین وضعیت را داشت. همچنین، استانداردهای کنترل دسترسی(۹۳/۳ درصد)، کنترل‌های حسابرسی(۸۶/۷ درصد) و امنیت انتقال اطلاعات(۸۵/۳ درصد) در سطح مطلوبی قرار داشتند. با این‌حال، کمترین میزان انطباق مربوط به استاندارد یکپارچگی با ۵۰ درصد بود که بیانگر ضرورت تقویت زیرساخت‌های فنی و به‌کارگیری سازوکارهای الکترونیکی پیشرفته‌تر برای تضمین صحت و یکپارچگی داده‌ها است.

نتیجه‌گیری: اگرچه سطح کلی انطباق در بیمارستان‌های مورد مطالعه در حد مطلوبی قرار دارد، اما شکاف‌های قابل‌توجهی به‌ویژه در حوزه‌های کنترل دستگاه‌ها و رسانه‌ها و همچنین یکپارچگی داده‌ها مشاهده می‌شود. این کاستی‌ها می‌تواند به نقض حریم خصوصی بیماران و خدشه‌دار شدن اعتماد عمومی به نظام سلامت بینجامد. توصیه می‌شود مدیران ارشد بیمارستان‌ها و سیاست‌گذاران حوزه سلامت با تدوین و اجرای دستورالعمل‌های دقیق داخلی، سرمایه‌گذاری در فناوری‌های پشتیبان و برگزاری دوره‌های آموزشی مستمر و هدفمند برای کلیه پرسنل، نسبت به رفع این نواقص اقدام کنند. همچنین پایش دوره‌ای انطباق برای تضمین بهبود مستمر ضروری است.

واژه‌های کلیدی: سیستم اطلاعات بیمارستانی، امنیت داده، انطباق، قانون قابلیت انتقال و پاسخ‌گویی بیمه‌های سلامت، حریم خصوصی، فناوری اطلاعات سلامت

دریافت مقاله: ۱۴۰۴/۳/۴
پذیرش مقاله: ۱۴۰۴/۱۰/۷

* نویسنده مسئول:
راضیه فرهی؛
دانشکده علوم پزشکی فردوس دانشگاه علوم پزشکی بیرجند

Email:
Farrahi1@bums.ac.ir

۱ استادیار گروه فناوری اطلاعات سلامت، دانشکده علوم پزشکی فردوس، دانشگاه علوم پزشکی بیرجند، بیرجند، ایران

۲ دانشجوی دکتری مدیریت اطلاعات سلامت، دانشکده مدیریت و اطلاع‌رسانی پزشکی، دانشگاه علوم پزشکی ایران، تهران، ایران

۳ دانشجوی کارشناسی فناوری اطلاعات سلامت، کمیته تحقیقات دانشجویی، دانشگاه علوم پزشکی بیرجند، بیرجند، ایران

مقدمه

در عصر دیجیتال، اطلاعات سلامت به دارایی‌هایی حیاتی و فوق‌حساس تبدیل شده‌اند که مدیریت مؤثر آن‌ها نقش تعیین‌کننده‌ای در کیفیت مراقبت‌های بهداشتی دارد. سیستم‌های اطلاعات بیمارستانی به‌عنوان زیرساخت اصلی فناوری اطلاعات در مراکز درمانی، امکان مدیریت یکپارچه، ذخیره‌سازی الکترونیکی و تبادل امن سوابق سلامت بیماران را فراهم می‌کنند(۱). این سیستم‌ها فراتر از ثبت ساده‌ی اطلاعات، با خودکارسازی فرآیندهای بالینی، اداری و مالی، به بهبود تصمیم‌گیری، بهینه‌سازی منابع و ارتقای کیفیت مراقبت، کمک شایانی می‌کنند(۳و۲). با این‌حال، دیجیتالی‌سازی هرچند مزایای بسیاری دارد، همان‌طور که مطالعات نشان می‌دهند، حجم عظیم داده‌های حساس سلامت را در معرض تهدیداتی مانند نقض امنیت، دسترسی غیرمجاز و سوءاستفاده قرار داده است(۵و٤). بنابراین، تأمین امنیت این داده‌ها نه تنها یک ضرورت فنی، بلکه تعهدی اخلاقی در قبال حفظ حریم خصوصی بیماران و صیانت از اعتماد عمومی به نظام سلامت است.

برای مقابله با تهدیدات فزاینده، چارچوب‌های قانونی و فنی مانند«قانون قابلیت انتقال و پاسخ‌گویی بیمه‌های سلامت (HIPAA: Health Insurance Portability and Accountability Act) در آمریکا تدوین شده‌اند که حفاظت از اطلاعات سلامت را به یک الزام قانونی تبدیل می‌کنند(۷و٦). در چارچوب امنیتی این قانون، مفاهیم کلیدی زیر تعریف می‌شوند:

«امحای امن» (Secure Disposal) به فرآیند حذف یا نابودسازی ایمن و غیرقابل‌بازگشت داده‌ها از سخت‌افزارها و رسانه‌های ذخیره‌سازی(مانند هارد دیسک، نوار مغناطیسی یا فلش‌مموری) پیش از خروج آن‌ها از چرخه‌ی استفاده، اسقاط، بازیافت یا استفاده‌ی مجدد گفته می‌شود(۸). «برنامه عملیات اضطراری» (Emergency Mode Operation) این برنامه مجموعه‌ای از رویه‌های مدون و از پیش تعیین‌شده است که با هدف حفاظت از سیستم‌های اطلاعاتی و تضمین تداوم ارایه خدمات حیاتی سازمان، هنگام وقوع شرایط بحرانی(نظیر قطعی طولانی‌مدت برق، خرابی‌های عمده یا بلایای طبیعی)، تدوین می‌شود(۹). «نگهداری سوابق» (Maintenance Records) الزام مستندسازی و حفظ مدارک مربوط به خط‌مشی‌ها، رویه‌ها، فعالیت‌ها و ارزیابی‌های امنیتی اشاره دارد(٦).

این الزامات عموماً در دو حوزه کلیدی«حفاظت فیزیکی» شامل کنترل دسترسی به محیط‌های فیزیکی و تجهیزات و «حفاظت فنی» شامل مکانیزم‌هایی مانند رمزنگاری و کنترل دسترسی منطقی دسته‌بندی می‌شوند و اساس تحقق اصول سه‌گانه‌ی امنیت اطلاعات را تشکیل می‌دهند(٦). در سطح ملی ایران، باوجود برخی اقدامات مانند بررسی مکانیسم‌های امنیت و حریم خصوصی اینترنت اشیا در صنعت مراقبت سلامت و غیر سلامت(۱۰)، خلأ یک چارچوب استاندارد جامع و الزام‌آور احساس می‌شود که لزوم توجه به چارچوب‌های بین‌المللی را پررنگ‌تر می‌سازد(۱۱).

رعایت HIPAA یک تعهد اخلاقی و یک الزام قانونی برای محافظت از اطلاعات سلامت شخصی بیماران است(۱۲). در ایران باتوجه به تحقیقات انجام شده، اقداماتی مانند تدوین آیین‌نامه‌های داخلی در برخی دانشگاه‌های علوم پزشکی در راستای افزایش انطباق سیستم‌های اطلاعات سلامت با استانداردهای موجود صورت گرفته(۱۰) و لازم است ارزیابی‌های دوره‌ای و نظام‌مند در این زمینه انجام شود تا از بهبود مستمر و رعایت استانداردهای موجود اطمینان حاصل گردد. از سوی دیگر، از آخرین پژوهش‌های جامع صورت گرفته این حوزه در ایران، همچون مطالعه‌ی ارزیابی انطباق امنیتی در بیمارستان‌های دانشگاه علوم پزشکی شیراز سال‌ها می‌گذرد(۸). مطالعات انجام‌شده در ایران حاکی از آن است که رعایت اصول محرمانگی و امنیت اطلاعات سلامت در بسیاری از مراکز درمانی مطابق با استانداردهای مورد انتظار نیست(۱۳و۸). عواملی مانند نبود زیرساخت امنیتی یکپارچه، کمبود آگاهی و آموزش تخصصی پرسنل و عدم نظارت مستمر بر عملکرد سیستم‌ها از جمله دلایل اصلی این عدم انطباق گزارش شده‌اند(۱۱). یافته‌های مطالعات پیشین، ممکن است تصویر دقیقی از وضعیت کنونی سیستم‌های اطلاعات سلامت، به‌ویژه با توجه به شتاب دیجیتالی‌سازی خدمات سلامت پس از همه‌گیری کووید-۱۹، ارایه ندهند(١٤). به‌روزترین نسخه سیستم اطلاعات بیمارستانی تیراژه در

سال ۱۴۰۰ به‌طور یکپارچه در تمام بیمارستان‌های وابسته به دانشگاه علوم پزشکی بیرجند پیاده‌سازی شد و مطالعه‌ای که به بررسی میزان انطباق این سیستم با به‌روزترین استانداردهای حفاظت فیزیکی و فنی از داده‌های سلامت بیماران پرداخته باشد، انجام نشده است. ازاین‌رو این مطالعه به‌منظور فراهم‌سازی دیدی جامع و داده‌های ملموس برای برنامه‌ریزی عملیاتی در این حوزه به ارزیابی انطباق سیستم اطلاعات بیمارستان‌های دانشگاه علوم پزشکی بیرجند با استانداردهای حفاظت فیزیکی و فنی داده‌های سلامت در سال ۱۴۰۳ پرداخت.

نتایج این ارزیابی می‌تواند داده‌ای عینی و ملموس در اختیار مدیران فناوری اطلاعات و تصمیم‌گیران دانشگاه قرار دهد تا با شناسایی نقاط قوت و ضعف امنیتی، منابع را به‌طور هدفمند به سمت رفع آسیب‌پذیری‌ها و ارتقای سیاست‌های حفاظتی تخصیص دهند. افزایش سطح انطباق، منجر به کاهش ریسک نقض داده‌ها، پیشگیری از پیامدهای مخرب افشای اطلاعات بیماران(مانند آسیب مالی، روانی و اجتماعی)(۱۰و۳) و در نهایت، افزایش تاب‌آوری سیستم و اعتماد عمومی به خدمات سلامت دیجیتال خواهد شد. این مقاله پس از بیان روش تحقیق، یافته‌های حاصل از ارزیابی را در دو حوزه‌ی حفاظت فیزیکی و فنی ارایه و در نهایت، راهکارهای عملیاتی برای بهبود وضعیت موجود پیشنهاد خواهد کرد.

روش بررسی

این مطالعه‌ی کاربردی به روش توصیفی-مقطعی در سال ۱۴۰۳ در بیمارستان‌های تابعه دانشگاه علوم پزشکی بیرجند انجام شده است. جامعه پژوهش را مدیران واحد فناوری اطلاعات بیمارستان تشکیل می‌دادند که به‌دلیل کوچک بودن جامعه آماری همه مدیران به روش تمام‌شماری وارد مطالعه شدند. پس از گرفتن رضایت، از آن‌ها دعوت شد چک‌لیست طراحی شده را تکمیل نمایند.

چک‌لیست استفاده شده در این مطالعه براساس چک‌لیستی مطابق استانداردهای قانون HIPAA که توسط OCR (Office for Civil Rights) تنظیم شده بود تهیه گردید که شامل ۳ بخش اطلاعات دموگرافیگ(سن، جنس، سابقه‌کار، نوع بیمارستان و تعداد تخت فعال بیمارستان)، سوالات استاندارد حفاظت فیزیکی(در ٤ استاندارد، ۱۰ مؤلفه و شامل ۳۹ گویه) و سوالات استاندارد حفاظت فنی(در ۵ استاندارد، ۹ مؤلفه و شامل ۱۷ گویه) بود.

روایی صوری چک‌لیست با بررسی ۵ نفر متخصص مدیریت اطلاعات سلامت، انفورماتیک پزشکی و سیاست‌گذاری سلامت تأیید و پایایی چک‌لیست با آلفای کرونباخ ۰/۸٤ تایید گردید. شرکت‌کنندگان می‌بایست پاسخ‌های هر سوال مربوط به استانداردهای فیزیکی و فنی چک‌لیست را براساس سه گزینه‌ی(وجود دارد و اعمال می‌شود، وجود دارد ولی اعمال نمی‌شود و وجود ندارد) بیان می‌کردند.

پس از گردآوری چک‌لیست‌های تکمیل‌شده، داده‌ها در نرم‌افزار SPSS وارد شدند. برای توصیف داده‌ها و میزان اعمال استانداردها، از آمار توصیفی شامل جداول فراوانی، شاخص‌های مرکزی و پراکندگی استفاده گردید. میزان انطباق با استانداردهای تعیین‌شده، به‌صورت درصد محاسبه شد؛ بدین‌صورت که درصد مواردی که هر گویه خاص در چک‌لیست، در وضعیت«وجود دارد و اعمال می‌شود» قرار داشت، به‌عنوان میزان انطباق آن گویه در نظر گرفته شد. در نهایت، میانگین این درصدها برای گویه‌های هر حوزه، نشان‌دهنده‌ی انطباق کلی آن حوزه بود.

یافته‌ها

در این مطالعه در مجموع ۱۵ نفر مدیر واحد فناوری اطلاعات بیمارستان‌های دانشگاه علوم پزشکی بیرجند به نمایندگی از ۱۵ بیمارستان تابعه دانشگاه شرکت نمودند که ۱٤ نفر(۹۳/۳٪) مرد بودند. ۵۳/۳٪ بیمارستان‌های حاضر در مطالعه از نوع آموزشی بودند. میانگین تخت فعال بیمارستان‌های مورد بررسی(آموزشی و غیرآموزشی) ۱۰۰ تخت بود. میانگین سن شرکت‌کنندگان در مطالعه ۳٤±۵/۳۳ سال(٤۵-۲۷ سال) و میانگین سابقه کار آن‌ها ۸/۹۳±۳/۶۲ سال(۱۵-٤ سال) بود.

جدول ۱، میزان انطباق سیستم اطلاعات بیمارستان‌های دانشگاه علوم پزشکی بیرجند با استانداردهای حفاظت فیزیکی را نشان می‌دهد. به‌طورکلی در ۸۱/۷ درصد از بیمارستان‌های موردبررسی، استانداردهای حفاظت فیزیکی رعایت می‌شود.

جدول ۱: میزان انطباق سیستم اطلاعات بیمارستان‌های دانشگاه علوم پزشکی بیرجند با استانداردهای حفاظت فیزیکی HIPAA

استاندارد	مؤلفه‌های هر استاندارد	وجود دارد		وجود ندارد	میانگین درصد انطباق استاندارد
		اعمال می‌شود	اعمال نمی‌شود		
کنترل‌های دسترسی به تاسیسات	عملیات اضطراری				
	رویه‌هایی توسعه یافته‌اند که امکان دسترسی به تأسیسات را برای بازیابی داده‌های از دست‌رفته در مواقع اضطراری، مانند قطع برق فراهم کنند.	(۱۰۰)۱۵	۰	۰	
	می‌توان رویه‌ها و خط‌مشی‌ها را توسط آن دسته از کارکنان که مسئولیت فرآیند بازیابی داده‌ها را برعهده دارند، به‌درستی اجرا کرد.	(۷۳/۳)۱۱	(۲۶/۷)٤	۰	
	رویه و خط‌مشی مناسب برای شناسایی پرسنل مجاز برای ورود مجدد به مرکز برای انجام بازیابی اطلاعات وجود دارد.	(۷۳/۳)۱۱	(۱۳/۳)۲	(۱۳/۳)۲	
	برنامه امنیتی تأسیسات				
	خط‌مشی‌ها و رویه‌ها، روش‌های مورد استفاده برای کنترل دسترسی فیزیکی مانند قفل درب‌ها، سیستم‌های کنترل دسترسی الکترونیکی، افسران امنیتی یا نظارت تصویری وجود دارد.	(۱۰۰)۱۵	۰	۰	
	خط‌مشی‌ها و رویه‌هایی برای محافظت از تأسیسات و تجهیزات مرتبط در برابر دسترسی فیزیکی غیرمجاز، دستکاری و سرقت وجود دارد.	(۹۳/۳)۱٤	(٦/۷)۱	۰	
	خط‌مشی‌ها و رویه‌هایی که اجازه دسترسی فیزیکی غیرمجاز به سیستم‌های اطلاعات بیمارستان را محدود کند، تدوین شده است.	(۱۰۰)۱۵	۰	۰	
	در خط‌مشی‌ها و رویه‌ها، اقدامات کنترلی برای جلوگیری از دسترسی فیزیکی غیرمجاز، دستکاری و سرقت پیش‌بینی شده است.	(۱۰۰)۱۵	۰	۰	
	روش‌های کنترل دسترسی و اعتبارسنجی				
	خط‌مشی‌ها و رویه‌هایی که بر اساس آن افراد(کارکنان، شرکای تجاری، پیمانکاران و غیره) دارای صلاحیت را بر اساس عنوان و یا عملکرد شغلی شناسایی می‌کند.	(۸٦/۷)۱۳	(۱۳/۳)۲	۰	٪۸۱/۳
	رویه‌هایی برای کنترل و اعتبارسنجی دسترسی افراد به امکانات بر اساس نقش یا عملکرد آن‌ها، از جمله کنترل بازدیدکنندگان، و کنترل دسترسی به برنامه‌های نرم‌افزاری برای آزمایش و بازنگری وجود دارد.	(۷۳/۳)۱۱	(۱۳/۳)۲	(۱۳/۳)۲	
	در خط‌مشی‌ها، روش‌های کنترل و تأیید دسترسی کارمندان به امکانات، مانند استفاده از نگهبان، نشان‌های شناسایی، یا وسایل ورود مانند کارت‌های کلیدی مشخص شده است.	(٦٦/۷)۱۰	(۲٦/۷)٤	(٦/۷)۱	
	خط‌مشی‌ها، کنترل‌های مربوط به بازدیدکنندگان را مشخص می‌کنند، از جمله این‌که لازم است آن‌ها هنگام ورود ثبت‌نام کنند، کارت شناسایی بازدیدکننده بپوشند و توسط یک فرد مجاز همراهی شوند.	(٤٦/۷)۷	(٤٦/۷)۷	(٦/۷)۱	
	در رویه‌ها، افراد، نقش‌ها یا وظایف شغلیِ مجاز برای دسترسی به برنامه‌های نرم‌افزاری به‌منظور انجام آزمون و بازبینی با هدف کاهش خطا مشخص شده است.	(۸٦/۷)۱۳	(۱۳/۳)۲	۰	
	نگهداری سوابق				
	مدیریت به‌طور مرتب لیست افراد دارای دسترسی فیزیکی به امکانات حساس را بررسی می‌کند.	(۸۰)۱۲	(۱۳/۳)۲	(٦/۷)۱	
	خط‌مشی‌ها و رویه‌های برای نحوه مستندسازی تعمیرات و اصلاحات اجزای فیزیکی تأسیسات مرتبط با امنیت وجود دارد.	(۷۳/۳)۱۱	(۱۳/۳)۲	(۱۳/۳)۲	
	خط‌مشی‌ها و رویه‌ها همه مؤلفه‌های حفاظت فیزیکی را که به مستندات نیاز دارند، مشخص می‌کنند؟(به‌عنوان مثال اجزای سخت‌افزاری، دیوارها، درب‌ها و قفل‌ها یا حتی تغییر کلید قفل‌ها زمانی‌که فردی از کارکنان از کار خارج شده است).	(٦٦/۷)۱۰	(۳۳/۳)۵	۰	
استفاده از ایستگاه کاری	خط‌مشی‌ها و رویه‌هایی تدوین و اجرا می‌شوند که عملکردهای مناسبی را که باید انجام شوند، روشی که آن عملکردها باید انجام شوند و ویژگی‌های فیزیکی محیط اطراف یک ایستگاه کاری خاص که می‌تواند به اطلاعات سلامت حفاظت‌شده الکترونیکی (EPHI: Electronic Protected Health Information) دسترسی داشته باشد را مشخص کند.	(۷۳/۳)۱۱	(۲۰)۳	(٦/۷)۱	
	خط‌مشی‌ها و رویه‌ها مشخص می‌کنند کدام ایستگاه‌های کاری به EPHI دسترسی دارند و کدام ایستگاه‌ها فاقد دسترسی به EPHI هستند.	(٦٦/۷)۱۰	(۳۳/۳)۵	۰	
	خط‌مشی‌ها و رویه‌ها مشخص می‌کنند که ایستگاه‌های کاری در کجا قرار بگیرند تا فقط توسط افراد مجاز امکان مشاهده فراهم شود.	(۸٦/۷)۱۳	(۱۳/۳)۲	۰	٪۸۱/۳
	خط‌مشی‌ها و رویه‌ها استفاده از اقدامات امنیتی تکمیلی برای محافظت از ایستگاه‌های کاری دارای EPHI را مشخص می‌کنند؛ اقداماتی مانند به‌کارگیری صفحه‌های حریم خصوصی، فعال‌سازی محافظ صفحه‌نمایش دارای رمز عبور، یا خروج از سیستم هنگام ترک ایستگاه کاری.	(۸٦/۷)۱۳	(٦/۷)۱	(٦/۷)۱	
	خط‌مشی‌ها و رویه‌ها استفاده از ایستگاه کاری را برای کاربرانی که از مکان‌های راه‌دور (مانند دفاتر ماهواره‌ای یا راه‌دور) به EPHI دسترسی دارند نشان می‌دهد.	(۹۳/۳)۱٤	(٦/۷)۱	۰	

امنیت ایستگاه کاری	برای تمامی ایستگاه‌های کاری دارای دسترسی به EPHI، تدابیر حفاظتی فیزیکی به اجرا درآمده است تا دسترسی صرفاً برای کاربران مجاز محدود شود.	(۸۶/۷)۱۳	(۱۳/۳)۲	۰	٪۸۹/۳
	همه انواع ایستگاه‌های کاری که به EPHI دسترسی دارند، مانند لپ‌تاپ‌ها، رایانه‌های رومیزی، دستیارهای دیجیتال شخصی (PDA) شناسایی شده‌اند.	(۹۳/۳)۱۴	(۶/۷)۱	۰	
	حفاظت فیزیکی فعلی برای محافظت از ایستگاه‌های کاری با EPHI مؤثر است.	(۸۶/۷)۱۳	(۱۳/۳)۲	۰	
	حفاظت فیزیکی اضافی برای محافظت از ایستگاه‌های کاری با EPHI لازم است.	(۱۰۰)۱۵	۰	۰	
	حفاظت فیزیکی برای محافظت از ایستگاه‌های کاری که به EPHI دسترسی دارند در خط‌مشی‌ها و رویه‌های استفاده از ایستگاه کاری مستند شده است.	(۸۰)۱۲	(۲۰)۳	۰	
کنترل‌های دستگاه و رسانه	خط‌مشی‌ها و رویه‌هایی تدوین و اجرا می‌شوند که بر دریافت و حذف سخت‌افزار و رسانه‌های الکترونیکی حاوی EPHI، به داخل و خارج از یک مرکز، و جابجایی این اقلام در داخل مرکز نظارت کند.	(۵۳/۳)۸	(۴۶/۷)۷	۰	٪۷۴/۹
دور ریختن (امحا)	خط‌مشی‌ها و رویه‌هایی تدوین و اجرا می‌شوند که به امحای EPHI و یا سخت‌افزار یا رسانه الکترونیکی که روی آن ذخیره شده است می‌پردازد.	(۸۰)۱۲	(۲۰)۳	۰	
	خط‌مشی‌ها و رویه‌ها، فرآیند غیرقابل استفاده و غیرقابل دسترس کردن EPHI و یا سخت‌افزار یا رسانه الکترونیکی را مشخص می‌کنند.	(۸۰)۱۲	(۲۰)۳	۰	
	خط‌مشی‌ها و رویه‌ها استفاده از یک فناوری مانند نرم‌افزار یا یک قطعه سخت‌افزار تخصصی را برای غیرقابل استفاده کردن و غیرقابل دسترس کردن EPHI و یا سخت‌افزار یا رسانه الکترونیکی مشخص می‌کنند.	(۸۰)۱۲	(۱۳/۳)۲	(۶/۷)۱	
استفاده مجدد از رسانه	رویه‌هایی برای حذف EPHI از رسانه‌های الکترونیکی قبل از استفاده مجدد ایجاد و اجرا شده است.	(۸۶/۷)۱۳	(۱۳/۳)۲	۰	
	رویه‌ها، موقعیت‌هایی را مشخص می‌کنند که همه EPHI باید به‌طور دایم حذف شوند یا موقعیت‌هایی که رسانه‌های الکترونیکی فقط باید دوباره قالب‌بندی شوند تا هیچ فایلی در دسترس نباشد.	(۱۰۰)۱۵	۰	۰	
پاسخ‌گویی	فرآیندی برای نگهداری سوابق، فعالیت و اطلاعات افراد مسئول سخت‌افزار و رسانه‌های الکترونیکی حاوی EPHI وجود دارد.	(۹۳/۳)۱۴	(۶/۷)۱	۰	
	خط‌مشی‌ها و رویه‌ها، انواع سخت افزارها و رسانه‌های الکترونیکی را که باید ردیابی شوند مشخص می‌کند.	(۳۳/۳)۵	(۴۶/۷)۷	(۲۰)۳	
	انواع سخت افزارها و رسانه‌های الکترونیکی که باید ردیابی شوند، مانند هارددیسک، نوار یا دیسک مغناطیسی، دیسک نوری یا کارت حافظه دیجیتال شناسایی شده‌اند.	(۵۳/۳)۸	(۴۰)۶	(۶/۷)۱	
پشتیبان‌گیری و ذخیره‌سازی داده‌ها	هنگامی‌که چندین دستگاه از یک نوع وجود دارد، راهی برای شناسایی تک‌تک دستگاه‌ها و ثبت یا ضبط جداگانه آن‌ها، مانند شماره سریال یا مکانیسم‌های ردیابی دیگر وجود دارد.	(۵۳/۳)۸	(۳۳/۳)۵	(۱۳/۳)۲	
	فرآیندی برای ایجاد یک کپی قابل بازیابی و دقیق از EPHI، در صورت نیاز، قبل از جابجایی تجهیزات اجرا شده است.	(۹۳/۳)۱۴	(۶/۷)۱		
	این فرایند مواردی را که تهیه یک نسخه دقیق و قابل‌بازیابی از EPHI ضروری است، و همچنین موقعیت‌هایی را که پیش از جابه‌جایی تجهیزات نیازی به این کار نیست، شناسایی می‌کند.	(۸۰)۱۲	(۶/۷)۱	(۱۳/۳)۲	
	فرآیند شناسایی می‌کند که چه کسی مسئول ایجاد یک کپی قابل بازیابی و دقیق از EPHI قبل از جابجایی تجهیزات است.	(۸۶/۷)۱۳	(۶/۷)۱	(۶/۷)۱	
میانگین درصد انطباق کلی (حفاظت فیزیکی)					٪۸۱/۷

بیشترین میزان انطباق مربوط به استاندارد امنیت ایستگاه کاری با میانگین ۸۹/۳٪ بود که بیانگر توجه مناسب به اقدامات حفاظتی فیزیکی برای ایستگاه‌های کاری دارای EPHI است. همچنین در برخی شاخص‌ها مانند وجود رویه‌های دسترسی اضطراری به تأسیسات و وجود روش‌های کنترل دسترسی فیزیکی، انطباق کامل ۱۰۰ درصد گزارش شد. در مقابل، کمترین میزان انطباق مربوط به استاندارد کنترل‌های دستگاه و رسانه با میانگین ۷۴/۹٪ بود، به‌ویژه در شاخص‌هایی مانند شناسایی و ردیابی انواع سخت‌افزارها و رسانه‌های الکترونیکی.

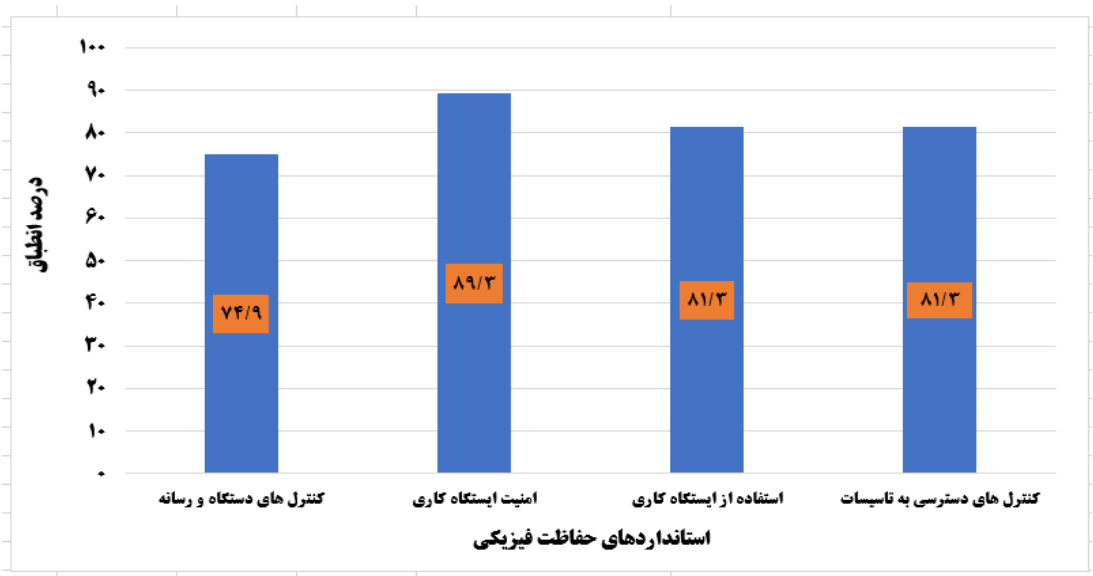
مطابق جدول ۲، که میزان تطابق سیستم اطلاعات بیمارستان‌های دانشگاه علوم پزشکی بیرجند با استانداردهای حفاظت فنی را نشان می‌دهد، به‌طوری‌که در ۸۶/۷ درصد از بیمارستان‌های مورد بررسی استانداردهای حفاظت فنی رعایت می‌شود.

جدول ۲: میزان انطباق سیستم اطلاعات بیمارستان‌های دانشگاه علوم پزشکی بیرجند با استانداردهای حفاظت فنی HIPAA

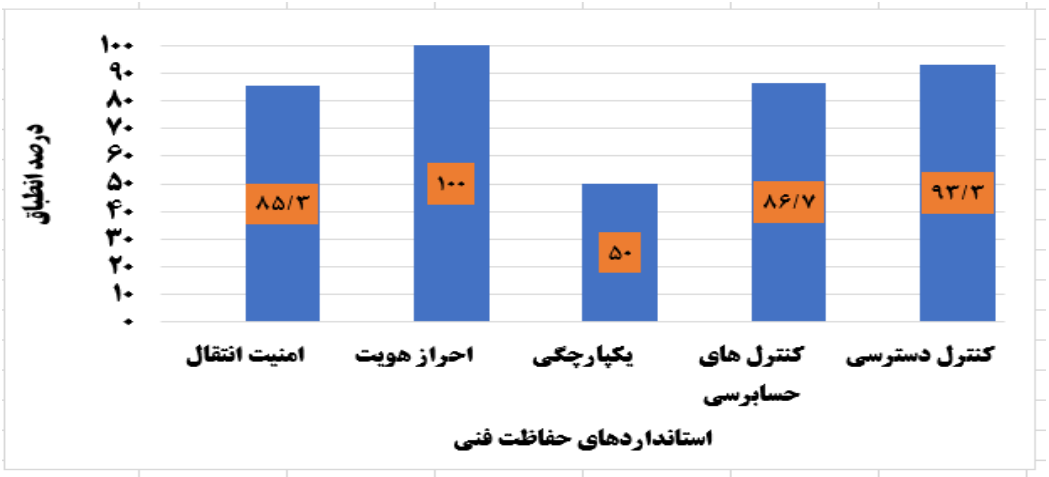
استاندارد	مؤلفه‌های هر استاندارد		وجود دارد		وجود ندارد	میانگین درصد انطباق استاندارد
			اعمال می‌شود	اعمال نمی‌شود		
کنترل دسترسی	شناسایی منحصر به فرد کاربر	هریک از کارمندان شناسه کاربری منحصر به فرد دارند.	۱۵(۱۰۰)	۰	۰	٪۹۳/۳
		از فرمت مشخصی برای شناسایی منحصر به فرد کاربر استفاده می‌شود.	۱۵(۱۰۰)	۰	۰	
		می‌توان از شناسه کاربری منحصر به فرد برای ردیابی فعالیت کاربر در داخل سیستم‌های اطلاعاتی حاوی اطلاعات سلامت الکترونیک حفاظت شده استفاده کرد.	۱۵(۱۰۰)	۰	۰	
	روش دسترسی اضطراری	در مواقع اضطراری لیست افراد واجد شرایط برای دسترسی به اطلاعات EPHI وجود دارد.	۱۳(۸۶/۷)	۱(۶/۷)	۱(۶/۷)	
		خط‌مشی‌ها و رویه‌هایی برای دسترسی مناسب به EPHI در شرایط اضطراری وجود دارد.	۱٤(۹۳/۳)	۱(۶/۷)	۰	
	خروج خودکار از سیستم	سیستم‌های اطلاعاتی فعلی دارای قابلیت خروج خودکار هستند.	۱۳(۸۶/۷)	۱(۶/۷)	۱(۶/۷)	
		ویژگی خروج خودکار در تمام ایستگاه‌های کاری با دسترسی به EPHI فعال است.	۱۳(۸۶/۷)	۱(۶/۷)	۱(۶/۷)	
	رمزگذاری و رمزگشایی	مکانیزم‌هایی برای جلوگیری از دسترسی افراد فاقدصلاحیت به EPHI رمزگذاری شده وجود دارد.	۱٤(۹۳/۳)	۱(۶/۷)	۰	
کنترل‌های حسابرسی		مکانیزم‌های کنترل حسابرسی(ممیزی) مناسب برای ثبت و بررسی فعالیت در سیستم‌های اطلاعات بیمارستان دارای EPHI وجود دارد.	۱۳(۸۶/۷)	۲(۱۳/۳)	۰	٪۸۶/۷
یکپارچگی		سیستم اطلاعات بیمارستان، عملکرد یا فرآیندی که به‌طور خودکار یکپارچگی داده‌هایی مانند تأیید اطلاعات شناسایی کننده یا امضای دیجیتال را بسنجد، دارد.	۲(۱۳/۳)	۷(٤٦/۷)	٦(٤۰)	٪۵۰
		مکانیسم‌های الکترونیکی برای محافظت از یکپارچگی EPHI در حال حاضر استفاده می‌شود.	۱۳(۸۶/۷)	۲(۱۳/۳)	۰	
احراز هویت		در سیستم مکانیزم‌های احراز هویت مناسب وجود دارد.	۱۵(۱۰۰)	۰	۰	۱۰۰
امنیت انتقال	کنترل‌های یکپارچگی	اقدامات امنیتی برای محافظت از EPHI در طول انتقال اطلاعات به‌کارگرفته می‌شود	۱۵(۱۰۰)	۰	۰	٪۸۵/۳
		تحلیل ریسک، سناریوهایی را که ممکن است منجر به اصلاح EPHI توسط منابع غیرمجاز در حین انتقال شود، شناسایی کرده است.	۱۲(۸۰)	۱(۶/۷)	۲(۱۳/۳)	
	رمزگذاری	بیمارستان خط‌مشی مناسب و مشخص برای انتقال EPHI دارند.	۱۳(۸۶/۷)	۲(۱۳/۳)	۰	
		بیمارستان بازه زمانی برای انتقال EPHI مشخص کرده است.	۱۳(۸۶/۷)	۲(۱۳/۳)	۰	
		روش‌های رمزگذاری مناسب برای محافظت از اطلاعات در حین انتقال EPHI وجود دارد.	۱۱(۷۳/۳)	۲(۱۳/۳)	۲(۱۳/۳)	
میانگین درصد انطباق کلی (حفاظت فنی)						٪۸۶/۷

در میان استانداردهای فنی، احراز هویت با میزان انطباق ۱۰۰ درصد بالاترین وضعیت را داشته و تمامی بیمارستان‌ها از مکانیزم‌های مناسب احراز هویت استفاده می‌کردند. همچنین استانداردهای کنترل دسترسی با ۹۳/۳ درصد و کنترل‌های حسابرسی ۸۶/۷ درصد در سطح مطلوبی قرار داشت. در بخش امنیت انتقال اطلاعات نیز میانگین انطباق ۸۵/۳ درصد به‌دست آمد که نشان‌دهنده اجرای قابل قبول اقدامات حفاظتی در زمان انتقال EPHI است، هرچند در برخی مؤلفه‌ها مانند تعیین بازه زمانی انتقال و استفاده از روش‌های رمزگذاری مناسب، هنوز نواقصی مشاهده می‌شود. کمترین میزان انطباق مربوط به استاندارد یکپارچگی ۵۰ درصد بود، به‌ویژه در زمینه استفاده از سازوکارهای خودکار برای سنجش و تضمین یکپارچگی داده‌ها؛ که نشان‌دهنده نیاز به تقویت زیرساخت‌های فنی و به‌کارگیری مکانیزم‌های الکترونیکی پیشرفته‌تر در این حوزه است.

در نمودار یک و دو میزان انطباق سیستم اطلاعات بیمارستان‌های تابعه دانشگاه علوم پزشکی بیرجند با استانداردهای فیزیکی و فنی HIPAA نشان داده شد.



نمودار ۱: میانگین درصد انطباق در حوزه‌های حفاظت فیزیکی HIPAA



نمودار ۲: میانگین درصد انطباق در حوزه‌های حفاظت فنی HIPAA

همان‌طور که در نمودارهای ۱ و ۲ مشاهده می‌شود، میزان انطباق در استانداردهای فنی در مقایسه با استانداردهای فیزیکی HIPAA ناهمگون است. در حوزه فیزیکی«استاندارد امنیت ایستگاه کاری» با ۸۹/۳ درصد بیشترین میزان انطباق را نشان می‌دهد. در حوزه فنی نیز شکاف قابل توجهی میان عملکرد بسیار مطلوب در«احراز هویت»(۱۰۰٪) و عملکرد ضعیف در«یکپارچگی داده‌ها» (۵۰٪) مشاهده می‌شود.

بحث

هدف از این مطالعه، بررسی میزان تطابق سیستم اطلاعات بیمارستان‌های دانشگاه علوم پزشکی بیرجند با استانداردهای حفاظت فیزیکی و فنی استاندارد HIPAA بود. نتایج نشان داد که به‌طور کلی ۸۱/۷ درصد از بیمارستان‌های مورد بررسی، استانداردهای حفاظت فیزیکی را رعایت می‌کنند. در این بخش، بیشترین میزان انطباق مربوط به حیطه‌ی امنیت ایستگاه کاری(۸۹/۳٪) و کمترین میزان انطباق مربوط به حیطه‌ی کنترل دستگاه و رسانه(۷٤/۹٪) بود. در بخش حفاظت فنی نیز ۸٦/۷ درصد از بیمارستان‌ها استانداردهای مربوط را رعایت کرده بودند. بالاترین میزان تطابق در این بخش به احراز هویت فرد یا نهاد(۱۰۰٪) اختصاص داشت؛ درحالی‌که کمترین میزان انطباق در حیطه‌ی یکپارچگی(۵۰٪) مشاهده شد. این یافته‌ها نشان می‌دهد که علی‌رغم رعایت نسبی استانداردهای حفاظت اطلاعات، همچنان در برخی حوزه‌های حساس مانند کنترل صحت داده‌ها و ردیابی سخت‌افزارها، کاستی‌هایی وجود دارد که نیازمند توجه و بهبود بیشتر است.

این نتایج با مطالعه‌ی Kruse و همکاران(۱۵) همخوانی دارد که نشان داد ۷۹ درصد از سازمان‌های مراقبت بهداشتی استانداردهای حفاظت فیزیکی HIPAA را رعایت می‌کنند. مطالعه‌ی Davis و Having (۱٦) نیز نشان داد که اگرچه بیمارستان‌های ایالات متحد آمریکا انطباق بالایی با استانداردهای حفاظت فیزیکی HIPAA داشتند؛ اما میزان انطباق در بخش ارزیابی‌های دوره‌ای کمتر بود. مطالعه‌ی Anthony و همکاران(۱۷) که ۳۲۲۱ بیمارستان متوسط و بزرگ را تحلیل کردند، نشان داد که استراتژی‌های سازمانی تأثیر قابل‌توجهی بر نرخ‌های انطباق دارند؛ و بیانگر این است که بیمارستان‌های بزرگ‌تر به‌دلیل داشتن منابع بیشتر معمولاً انطباق بهتری دارند؛ درحالی‌که مطالعه‌ی Chen و Benusa (۱۸) تأکید می‌کند که ارایه‌دهندگان کوچک خدمات بهداشتی اغلب به‌دلیل محدودیت‌های کارکنان و منابع مالی با چالش‌هایی در زمینه‌ی انطباق حفاظت داده مواجه هستند. همچنین در مطالعه‌ای دیگر گزارش شد که تنها ٦۵ درصد از بیمارستان‌ها به‌طور کامل از این استانداردها پیروی می‌کنند؛ که نشان‌دهنده‌ی تفاوت‌های احتمالی در روش‌های ارزیابی یا تفاوت‌های منطقه‌ای است(۱۹). با توجه به پایین بودن میزان انطباق در حیطه‌ی کنترل دستگاه و رسانه(۷٤/۹ درصد)، پیشنهاد می‌شود که بیمارستان‌ها برنامه‌های آموزشی ویژه‌ای برای کارکنان در زمینه‌ی مدیریت صحیح دستگاه‌ها و رسانه‌های حاوی اطلاعات حساس بیماران ارایه دهند و سیاست‌های سختگیرانه‌تری برای کنترل و نظارت بر این موارد اعمال کنند تا اطمینان حاصل شود که تمام کارکنان از پروتکل‌های ضروری آگاه بوده و به آن‌ها پایبند هستند؛ که در نهایت فرهنگ امنیت را در محیط بیمارستان ترویج می‌دهد. یافته‌های این مطالعه نشان می‌دهد که سطح انطباق در حوزه‌های مختلف استاندارد HIPAA به‌طور محسوسی متفاوت است. برای نمونه، درحالی‌که انطباق در حوزه‌هایی مانند«امنیت ایستگاه کاری»(۱۰۰٪) و «احراز هویت فرد یا نهاد» بسیار بالا بود، حوزه‌های«کنترل دستگاه و رسانه»(۷٤/۹٪) و «یکپارچگی»(۵۰٪) نقاط ضعف جدی را نشان دادند. مرور ادبیات نشان می‌دهد که چنین شکاف‌هایی ممکن است متأثر از عواملی فراتر از فناوری، مانند فرهنگ سازمانی، منابع مالی و آگاهی در خصوص امنیت باشد. نتایج مطالعاتی مانند پژوهش Warkentin و همکاران(۲۰) و Sari و همکاران(۲۱) نشان داده‌اند که ویژگی‌هایی چون فرهنگ سازمانی، حمایت مدیریتی و دسترسی به منابع می‌توانند نقش تعیین‌کننده‌ای در سطح پایبندی به استانداردها ایفا کنند. این عوامل ممکن است تا حدی توضیح‌دهنده‌ی عملکرد ضعیف‌تر در حوزه‌های حساسی مانند کنترل دستگاه‌ها و یکپارچگی داده‌ها در مطالعه حاضر باشند. از این رو، بهبود انطباق، نیازمند راهبردهای سفارشی است که علاوه بر ارتقای فناوری و آموزش، بستر سازمانی و نهادی حاکم بر بیمارستان را نیز مورد توجه قرار دهد. برخی مطالعات نیز نشان داده‌اند که چالش‌هایی مانند ادغام ناکامل پروتکل‌های امنیتی یا کمبود ارزیابی‌های دوره‌ای می‌تواند منجر به ایجاد سیلوهای داده و ناهماهنگی در انطباق شود(۲۲و۱۷). این عوامل ممکن است تا حدی توضیح‌دهنده‌ی نرخ پایین انطباق در اقدامات یکپارچگی داده‌ها در مطالعه حاضر باشند. همچنین، حمایت‌های مدیریتی به‌عنوان پیش‌بینی‌کننده‌های کلیدی اثربخشی اقدامات امنیتی شناسایی شده‌اند(۲۳). بنابراین، برای بهبود انطباق در حوزه‌های ضعیف‌تر، تمرکز بر عوامل سازمانی و انسانی، در کنار راهکارهای فنی، ضروری به‌نظر می‌رسد.

یافته‌های این مطالعه نشان می‌دهد که اکثر بیمارستان‌های مورد بررسی(۸۱/۷٪) استانداردهای حفاظت فیزیکی HIPAA را رعایت می‌کنند؛ اما همچنان شکاف‌هایی در برخی حوزه‌ها وجود دارد. این نتایج با برخی مطالعات دیگر همخوانی دارد؛ یک مطالعه پیمایشی در بیمارستان‌های ایالات متحد آمریکا در سال‌های ۲۰۰٤ و ۲۰۰۵ نشان داد که حفاظت‌های فیزیکی برای محدود کردن دسترسی به سیستم‌های اطلاعات الکترونیکی از جمله استانداردهایی بوده‌اند که

بالاترین میزان انطباق را داشته‌اند(۱۶). همچنین، یک مطالعه مقطعی در یکی از بیمارستان‌های مصر، میانگین کلی انطباق با HIPAA را ۸۵ درصد گزارش کرد و سطح بالایی از انطباق را به‌ویژه در حوزه حفاظت‌های مدیریتی نشان داد(۲۴).

با این‌حال، برخی مطالعات دیگر سطوح پایین‌تر یا متغیرتری از انطباق را گزارش کرده‌اند، به‌ویژه زمانی که دامنه ارزیابی شامل اقدامات امنیتی گسترده‌تر یا انواع خاصی از ارایه‌دهندگان خدمات سلامت بوده است. برای نمونه، پژوهشی در مراکز پزشکی دانشگاهی به«انطباق محدود با الزامات امنیتی HIPAA» اشاره کرده است(۲۵). همچنین، مطالعه‌ای درباره ارایه‌دهندگان خدمات سلامت روان طرف قرارداد با ایالت نیوجرسی نشان داد که بیشتر سازمان‌های مورد بررسی برای انطباق با الزامات امنیتی HIPAA آمادگی کافی نداشته‌اند(۲۶). به‌طور کلی، برخی بررسی‌ها نشان می‌دهند که بسیاری از ارایه‌دهندگان خدمات سلامت در دستیابی و حفظ انطباق با HIPAA با چالش‌هایی مانند محدودیت منابع، فناوری‌های قدیمی و ماهیت پویای تهدیدات سایبری مواجه هستند(۲۷). در مطالعه‌ی Kwon و Johnson (۲۸)، میزان انطباق بیمارستان‌ها با استانداردهای حفاظت فیزیکی HIPAA در حدود ۸۰٪ گزارش شد. این تفاوت‌ها می‌تواند ناشی از تغییرات در طول زمان، تفاوت‌های منطقه‌ای یا روش‌های ارزیابی متفاوت باشد.

با توجه به پایین‌ترین میزان انطباق در حیطه‌ی کنترل دستگاه و رسانه(۷۴/۹ درصد) پیشنهاد می‌شود که بیمارستان‌ها اقداماتی نظیر تدوین و اجرای سیاست‌های مشخص برای مدیریت دستگاه‌ها و رسانه‌ها شامل شناسایی، ردیابی، نگهداری و امحای امن دستگاه‌ها و رسانه‌های حاوی اطلاعات بهداشتی، آموزش کارکنان از طریق برگزاری دوره‌های آموزشی منظم برای کارکنان در مورد اهمیت مدیریت صحیح دستگاه‌ها و رسانه‌ها و آشنایی با پروتکل‌های مربوط و استفاده از فناوری‌های پیشرفته با به‌کارگیری سیستم‌های ردیابی الکترونیکی و نرم‌افزارهای مدیریت دارایی برای نظارت بر دستگاه‌ها و رسانه‌ها را برای بهبود این حوزه در نظر بگیرند. اجرای این اقدامات می‌تواند به بهبود انطباق بیمارستان‌ها با استانداردهای حفاظت فیزیکی HIPAA و افزایش امنیت اطلاعات بیماران منجر شود.

در بخش حفاظت فنی نیز ۸۶/۷ درصد از بیمارستان‌ها، استانداردهای مربوط را رعایت کرده بودند. بالاترین میزان تطابق در این بخش به احراز هویت فرد یا نهاد(۱۰۰٪) اختصاص داشت؛ درحالی‌که کمترین میزان انطباق در حیطه‌ی یکپارچگی(۵۰٪) مشاهده شد.

یافته‌های این مطالعه مبنی بر رعایت بالای استانداردهای حفاظت فنی در بیمارستان‌های مورد بررسی(۸۶/۷ درصد) و تطابق کامل در حیطه‌ی احراز هویت فرد یا نهاد(۱۰۰ درصد) با نتایج برخی مطالعات پیشین همخوانی دارد. در مطالعه‌ی ابراهیم‌پور صدقیانی و همکاران نتایج ارزیابی با استفاده از چک‌لیست‌های مبتنی بر استانداردهای HIPAA و ISO/IEC27001 نشان داد که استانداردهای فنی در بیمارستان ۲۲ بهمن نیشابور ۱۰۰ درصد رعایت شده و در بیمارستان حکیم، استانداردهای خط‌مشی امنیت اطلاعات نیز ۱۰۰ درصد و تشکیلات امنیت اطلاعات ۹۰ درصد بالاترین حد رعایت را داشتند. باوجود مطلوب بودن امنیت اطلاعات در بیمارستان‌های مورد مطالعه، ازآن‌جا که روزانه اطلاعات بسیار زیادی در بیمارستان‌ها تبادل می‌شوند، عدم رعایت امنیت در حد نانو می‌تواند زیان‌های جبران ناپذیری را متوجه بیمارستان‌ها کند. بنابراین، مدیران بخش‌های مدیریت اطلاعات سلامت و فناوری اطلاعات بیمارستان‌ها باید تلاش کنند تا نقاط آسیب‌پذیر را شناسایی کرده و برای بهبود کاستی‌های امنیت اطلاعات بیمارستان برنامه‌ریزی کنند(۲۹). در مطالعه‌ای که توسط Kwon و Johnson (۳۰) انجام شد، مشخص شد که بسیاری از بیمارستان‌ها به‌دلیل الزام‌های قانونی و با هدف جلوگیری از دسترسی غیرمجاز، پروتکل‌های احراز هویت کاربران را به‌طور کامل رعایت می‌کنند، به‌ویژه استفاده از نام کاربری و رمز عبور منحصربه‌فرد یا سیستم‌های احراز هویت چندعاملی که امنیت را افزایش می‌دهد. با این حال، میزان انطباق پایین در بخش یکپارچگی(۵۰٪) با یافته‌های Appari و Johnson (۳۱) متفاوت است. آن‌ها در مطالعه‌ی خود نشان دادند که بسیاری از بیمارستان‌های ایالات متحد آمریکا، مکانیزم‌های خودکار سنجش یکپارچگی داده‌ها مانند امضای دیجیتال را به‌طور کامل اجرا کرده‌اند و میزان تطابق در این زمینه بالاتر از ۸۰ درصد بوده است. این تفاوت می‌تواند ناشی از تفاوت در زیرساخت‌های فناوری اطلاعات، سطح بودجه یا سیاست‌های حاکم بر بیمارستان‌های کشورهای مختلف باشد. برای بهبود انطباق در حیطه‌ی یکپارچگی، پیشنهاد می‌شود که بیمارستان‌ها از ابزارهای پیشرفته‌ی رمزنگاری و الگوریتم‌های Hashing برای تضمین یکپارچگی داده‌ها بهره بگیرند. همچنین، اجرای دوره‌های آموزشی مستمر برای کارکنان فناوری اطلاعات جهت آشنایی با شیوه‌های پیشرفته‌ی حفاظت از داده‌ها می‌تواند به ارتقای امنیت سیستم‌های اطلاعاتی کمک کند.

در ایران هنوز قانون جامع و یکپارچه‌ای برای حفاظت از داده‌های شخصی، از جمله داده‌های سلامت، وجود ندارد؛ اما مجموعه‌ای از مقررات پراکنده

به‌طور غیرمستقیم از این اطلاعات حمایت می‌کنند. مهم‌ترین این مقررات شامل اصل‌های ۲۲ و ۲۵ قانون اساسی، ماده ٦٤٨ قانون مجازات اسلامی درباره جرم‌انگاری افشای اسرار پزشکی، قانون جرایم رایانه‌ای در زمینه‌ی دسترسی و افشای غیرمجاز داده‌های الکترونیکی، و مواد ۵۸ تا ٦١ قانون تجارت‌الکترونیکی درباره حفاظت از داده‌های شخصی است. همچنین وزارت بهداشت از طریق دستورالعمل‌های داخلی و منشور حقوق بیمار بر محرمانگی اطلاعات پزشکی تأکید می‌کند. با این‌حال، به دلیل فقدان چارچوب جامع مشابه مقررات بین‌المللی مانند (HIPAA و (GDPR: General data protection regulations))، موضوعاتی مانند نحوه جمع‌آوری، نگهداری، پردازش، اشتراک‌گذاری و انتقال داده‌های سلامت هنوز با چالش‌ها و ابهام‌های جدی حقوقی مواجه است. پژوهش حاضر، با ارایه داده‌های کمی درباره انطباق بیمارستان‌ها با استانداردهای حفاظت فیزیکی(مانند عملکرد قوی در امنیت ایستگاه‌های کاری) و فنی(مانند احراز هویت قوی)، نقشه راه دقیقی از نقاط ضعف و قوت در اختیار مدیران قرار داده است. یافته‌های کلیدی، شکاف‌های حیاتی در حوزه‌های«کنترل دستگاه و رسانه» و «یکپارچگی اطلاعات» را برجسته می‌کند. این داده‌ها بلافاصله برای تخصیص مؤثر منابع به سمت آموزش مدون کارکنان، تدوین دستورالعمل‌های شفاف برای امحای امن دستگاه‌ها، و تهیه نرم‌افزارهای ردیابی قابل استفاده هستند تا ریسک‌های امنیتی ناشی از عدم انطباق را به‌صورت عملی کاهش داده و اعتماد بیماران به محرمانگی داده‌ها را تقویت کنند. از طرفی این مطالعه با محدودیت‌هایی چون کوچک بودن جامعه پژوهش، ماهیت خودگزارشی داده‌ها و تمرکز صرف بر استانداردهای حفاظت فیزیکی و فنی HIPAA در یک دانشگاه خاص مواجه است. ازاین‌رو برای دستیابی به درکی جامع‌تر و تعمیم پذیری نتایج، مطالعات آینده باید با نمونه‌های بزرگ‌تر، استفاده از روش‌های ترکیبی(مانند مشاهده مستقیم) و بررسی تأثیر عوامل سازمانی(نظیر بودجه و فرهنگ امنیتی) بر انطباق، انجام شوند. نتایج این مطالعات در سطح کلان به‌عنوان اولین گام سیاستی می‌تواند مبنایی برای طراحی و استقرار دستورالعمل‌های بومی امنیت اطلاعات سلامت در غیاب یک چارچوب ملی جامع باشد و دانشگاه‌های علوم پزشکی با ایجاد چارچوب امنیتی واحد و نظام پایش دوره‌ای می‌توانند هماهنگی و بهبود مستمر در کاهش ریسک نقص داده‌ها را در بیمارستان‌های خود تضمین کنند.

نتیجه‌گیری

نتایج این مطالعه نشان‌دهنده‌ی انطباق کلی بالا و قابل قبول بیمارستان‌های مورد بررسی با الزامات امنیتی استاندارد HIPAA به‌عنوان یک استاندارد معتبر جهانی است؛ به‌طوری‌که بیش از ۸۰ درصد بیمارستان‌ها، استانداردها در هر دو حوزه‌ی حفاظت فیزیکی(۸۱/۷ درصد) و حفاظت فنی(۸٦/۷ درصد) را رعایت کرده‌اند. این نزدیکی درصدها، حاکی از توازن نسبی در توجه به زیرساخت‌ها و کنترل‌های فنی است. با این‌حال، وجود شکاف حدود ١٤ تا ١٩ درصدی در انطباق کامل، ضرورت تمرکز بر حیطه‌های جزیی‌تر و برنامه‌ریزی برای رفع نواقص باقی‌مانده را گوشزد می‌کند تا امنیت داده‌های سلامت به‌طور کامل تضمین شود.

تشکر و قدردانی

از کلیه مدیران واحد فناوری اطلاعات در بیمارستان‌های مورد مطالعه جهت همکاری و همراهی سودمندشان تشکر و قدردانی می‌گردد. این مطالعه بر اساس ملاحظات اخلاقی کمیته اخلاق معاونت تحقیقات و فناوری دانشگاه علوم پزشکی بیرجند با کد اخلاق IR.BUMS.REC.1403.012 و شماره طرح پژوهشی ٦٥٥٤ انجام شد.

References

1. Dehnavieh R, Haghdoost A, Khosravi A, Hoseinabadi F, Rahimi H, Poursheikhali A, et al. The district health information system (DHIS2): A literature review and meta-synthesis of its strengths and operational challenges based on the experiences of 11 countries. Health Information Management Journal 2019; 48(2): 62-75.

2. Armstrong S. The computer will assess you now. British Medical Journal 2016; 355(1): i5680.

3. Bates DW, Saria S, Ohno-Machado L, Shah A & Escobar G. Big data in health care: Using analytics to identify and manage high-risk and high-cost patients. Health Affairs 2014; 33(7): 1123-31.

4. Balestra ML. Electronic health records: Patient care and ethical and legal implications for nurse practitioners. The Journal for Nurse Practitioners 2017; 13(2): 105-11.

5. Eslami-Andargoli A, Scheepers H, Rajendran D & Sohal A. Health information systems evaluation frameworks: A systematic review. International Journal of Medical Informatics 2017; 97(1): 195-209.

6. Martin NL, Imboden T & Green DT. HIPAA security rule compliance in small healthcare facilities: A theoretical framework. Issues in Information Systems 2015; 16(1): 1-10.

7. U.S. Department of Health and Human Services. Summary of the HIPAA security rule. Available at: https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html. 2024.

8. Sharifian R, Nematollahi M, Monem H & Ebrahimi F. Evaluating the security safeguards in hospital information system according to the health insurance portability and accountability act of university hospitals in shiraz university of medical sciences, Iran. Health Information Management 2013; 10(1): 35-46[Article in Persian].

9. Givachi S, Malek-Mohammadi B & Jalili M. Emergency key operational plan in emergency planning, Iran, Tehran: 3rd Conference on Environmental Planning and Management, 2013.

10. Nasiri S, Sadoughi F, Tadayon MH & Dehnad A. Security and privacy mechanisms of Internet of things in healthcare and non-healthcare industry. Journal of Health Administration 2019; 22(4): 86-105.

11. Zarei J & Sadoughi F. Information security risk management for computerized health information systems in hospitals: A case study of Iran. Risk Management and Healthcare Policy 2016; 9(1): 75-85.

12. Moore W & Frye S. Review of HIPAA, part 1: History, protected health information, and privacy and security rules. Journal of Nuclear Medicine Technology 2019; 47(4): 269-72.

13. Hajavi A, Khoushgam M & Hatami M. A comparative study on regarding rate of the privacy principles in legal issues by WHO manual at teaching hospitals of Iran, Tehran and Shahid Beheshti medical sciences universities, 2007. Journal of Health Administration 2008; 11(33): 7-16[Article in Persian].

14. Clipper B. The influence of the COVID-19 pandemic on technology: Adoption in health care. Nurse Leader 2020; 18(5): 500-3.

15. Kruse CS, Smith B, Vanderlinden H & Nealand A. Compliance with physical security standards in healthcare organizations: A national survey. Journal of Medical Systems 2017; 41(8): 1-9.

16. Davis DC & Having KM. Compliance with HIPAA security standards in U.S. Hospitals. Journal of Healthcare Information Management 2006; 20(2): 108-15.

17. Anthony D, Appari A & Johnson ME. Institutionalizing HIPAA compliance: Organizations and competing logics in U.S. health care. Journal of Health and Social Behavior 2014; 55(1): 108-24.

18. Chen JQ & Benusa A. HIPAA security compliance challenges: The case for small healthcare providers. International Journal of Healthcare Management 2017; 10(2): 135-46.

19. Galloway L. Understanding the health insurance portability and accountability act. Available at: https://pabau.com/blog/hipaa-compliance-simplified-guide/. 2023.

20. Warkentin M, Johnston A & Adams A. User interaction with healthcare information systems: Do healthcare professionals want to comply with HIPAA? Americas Conference on Information System in Acapulco, México, 2006.

21. Sari PK, Prasetio A, Candiwan C, Handayani PW, Hidayanto AN, Syauqina S, et al. Information security cultural differences among health care facilities in Indonesia. Heliyon 2021; 7(6): e07248.

22. Brady JW. An investigation of factors that affect HIPAA security compliance in academic medical centers [Thesis]. USA, Florida: Nova Southeastern University; 2010.

23. Nebergall J. Breaking down healthcare's hidden data silos: Expert tips. Available at: https://www.consensus.com/blog/breaking-down-healthcares-hidden-data-silos-expert-tips/. 2023.

24. Ibrahim AM, Abdel-Aziz HR, Mohamed HA, Zaghamir DE, Wahba NMI, Hassan GhA, et al. Balancing confidentiality and care coordination: Challenges in patient privacy. BMC Nursing 2024; 23(564): 1-14.

25. Brady JW. Securing health care: Assessing factors that affect HIPAA security compliance in academic medical centers. Available at: https://scispace.com/pdf/securing-health-care-assessing-factors-that-affect-hipaa-1payi8xo7i.pdf. 2011.

26. Bravo KM & Gustavon FG. Available at: https://www.semanticscholar.org/paper/A-model-for-hipaa-security-compliance-Bravo-Gustavson/5fd48e8a955e0af6e39008ec907f24ab49430171. 2005

27. Abbasi N & Smith DA. Cybersecurity in healthcare: Securing patient health information (PHI), HIPPA compliance framework and the responsibilities of healthcare providers. Journal of Knowledge Learning and Science Technology 2024; 3(3): 278-87.

28. Kwon J & Johnson ME. Security practices and regulatory compliance in the healthcare industry. Journal of the American Medical Informatics Association 2013; 20(1): 44-51.

29. Ebrahimpour-Sadagheyani H & Heydarpour F. Information security standards in the information system of hospitals of Neyshabur University of Medical Sciences. Journal of Neyshabur University of Medical Sciences 2022; 10(34): 133-42[Article in Persian].

30. Kwon J & Johnson ME. Proactive versus reactive security investments in the healthcare sector. Management Information Systems Quarterly 2014; 38(2): 451-71.

31. Appari A & Johnson ME. Information security and privacy in healthcare: Current state of research. International Journal of Internet and Enterprise Management 2010; 6(4): 279-314.