امنیت سایبری در نظام سلامت و مراقبت از بیماران عفونی: پیامدها برای ایمنی بیمار و سلامت عمومی

رهام بنی فضل[1]*

۱-دانشجوی کارشناسی ارشد مهندسی کامپیوتر- گرایش شبکه، دانشگاه ازاد تهران شمال

*نویسنده مسئول : رهام بنی فضل نشانی برای مکاتبه: banifazr@gmail.com
دریافت مقاله: پاییز ۱۴۰۴ پذیرش برای چاپ: زمستان ۱۴۰۴

چکیده

با گسترش استفاده از فناوری‌های دیجیتال در نظام سلامت، سامانه‌های آزمایشگاهی و تصویربرداری، سامانه‌های ارتباطی و نسخه‌نویسی الکترونیک به اجزای مهم ارائه خدمات سلامت تبدیل شده‌اند. حملات سایبری، به‌ویژه حملات باج‌افزاری، صرفاً رخدادهایی فناورانه یا محدود به نقض محرمانگی اطلاعات نیستند، بلکه می‌توانند با مختل‌کردن دسترسی به نتایج تشخیصی، فرایندهای تجویز و تبادل اطلاعات، تداوم مراقبت و ایمنی بیمار را به خطر اندازند. این حملات همچنین ممکن است از طریق افشای غیرمجاز داده‌های بالینی و میکروب‌شناسی، اطلاعات مربوط به الگوهای مقاومت ضدمیکروبی و وضعیت اپیدمیولوژیک بیماری‌های واگیر در مناطق مختلف را در معرض دسترسی افراد غیرمجاز قرار دهند. اهمیت و شکل این پیامدها به میزان دیجیتالی‌شدن فرایندهای نظام سلامت وابسته است. در ایران، با وجود نگهداری عمدتاً کاغذی پرونده‌های بستری، نسخه‌نویسی الکترونیک در خدمات سرپایی و استفاده از سامانه‌های دیجیتال آزمایشگاهی، تصویربرداری و ارتباطی، وابستگی به زیرساخت‌های دیجیتال همچنان قابل توجه است. این مرور روایتی، شواهد منتشرشده درباره پیامدهای حملات سایبری بر دسترسی به اطلاعات بالینی، تداوم خدمات تشخیصی و درمانی و سلامت عمومی را بررسی می‌کند. با تمرکز بر متخصصان بیماری‌های عفونی، پیامدهای احتمالی اختلال در دسترسی به نتایج کشت و آزمون‌های حساسیت ضدمیکروبی، مدیریت مصرف آنتی بیوتیک ها، پایش عفونت‌ها و گزارش‌دهی بیماری‌ها نیز مورد توجه قرار می‌گیرد. شواهد موجود، که عمدتاً بر مطالعات مشاهده‌ای و گزارش‌های موردی و تجربه کشورهایی با زیرساخت‌های دیجیتال متفاوت استوارند، از اختلال در ارائه خدمات، تأخیر در فرایندهای تشخیصی و درمانی و انتقال بخشی از بار مراقبت به مراکز مجاور حکایت دارند. با این‌حال، میزان تعمیم این یافته‌ها به ایران نیازمند توجه به تفاوت‌های ساختاری نظام سلامت است. آمادگی متناسب با زیرساخت هر مرکز، شامل پیش‌بینی مسیرهای جایگزین ثبت و انتقال اطلاعات، تداوم مراقبت از بیماران بدحال، حفاظت از محرمانگی و صحت داده‌ها و بازیابی و تطبیق اطلاعات پس از رفع اختلال، باید در کنار اقدامات پیشگیرانه امنیت سایبری، بخشی از برنامه‌های ایمنی بیمار و تداوم خدمات سلامت باشد.

واژگان کلیدی :*حملات سایبری؛ باج‌افزار؛ ایمنی بیمار؛ بیماری‌های عفونی؛ مقاومت ضدمیکروبی؛ سلامت عمومی.*

مقدمه

تصمیم‌گیری روزمره در درمان عفونت‌ها، از انتخاب درمان تجربی با آنتی‌بیوتیک تا تنظیم دوز و تعیین مدت درمان، به اطلاعاتی وابسته است که از منابع مختلف به دست می‌آیند؛ از جمله پرونده کاغذی بیمار، نتایج آزمایشگاهی، تصاویر پزشکی، سامانه‌های نسخه‌نویسی و سوابق ثبت‌شده در سامانه‌های دیجیتال. در ایران، کاغذی‌بودن پرونده‌های بستری به این معنا نیست که مراقبت بیمارستانی از اختلال سایبری مصون است. ازکارافتادن سامانه اطلاعات آزمایشگاهی، تصویربرداری، ارتباطات، احراز هویت یا سایر زیرساخت‌های دیجیتال می‌تواند دسترسی به اطلاعات ضروری یا انتقال به‌موقع آن‌ها را مختل کند. در خدمات سرپایی نیز اختلال در نسخه‌نویسی الکترونیک یا سامانه‌های مرتبط ممکن است فرایند تجویز و

دریافت دارو را به تأخیر اندازد. در چنین شرایطی، امنیت سایبری باید نه‌فقط مسئله‌ای فنی یا حقوقی، بلکه عاملی مؤثر بر ایمنی بیمار و تداوم خدمات سلامت تلقی شود.

ابعاد این مسئله قابل‌توجه است. در یک مطالعه درباره حملات باج‌افزاری علیه مراکز ارائه‌دهنده خدمات سلامت در ایالات متحده طی سال‌های ۲۰۱۶ تا ۲۰۲۱، در مجموع ۳۷۴ حمله شناسایی شد که افشای اطلاعات سلامت حدود ۴۲ میلیون نفر را در پی داشت. تعداد سالانه حملات نیز از ۴۳ مورد به ۹۱ مورد افزایش یافت. در ۴۴ درصد حملات (۱۶۶ مورد)، اختلال در ارائه خدمات مراقبتی گزارش شد (۱).

مقاله حاضر با هدف آگاهی‌بخشی به متخصصان بیماری‌های عفونی، به بررسی پیامدهای بالینی و عملیاتی حملات سایبری و اختلال در سامانه‌های دیجیتال سلامت می‌پردازد و راهکارهای مرتبط با حفظ ایمنی بیمار و تداوم مراقبت را تبیین می‌کند.

روش کار

این مقاله به روش مرور روایتی تدوین شده است. منابع از طریق جست‌وجوی هدفمند مقالات داوری شده و گزارش‌های رسمی درباره حملات سایبری علیه مراکز ارائه‌دهنده خدمات سلامت، منتشرشده تا دی ماه ۱۴۰۴، گردآوری شدند. مطالعاتی در اولویت قرار گرفتند که پیامدهای بالینی یا عملیاتی این حملات را گزارش کرده بودند. بنابراین، این مقاله با رویکرد مرور روایتی و با هدف ارائه جمع‌بندی تحلیلی از شواهد موجود، تبیین ابعاد مختلف تهدیدات سایبری و بررسی پیامدهای آن‌ها بر ایمنی بیماران و تداوم خدمات سلامت تدوین شده است.

پیامدها برای سلامت عمومی

پیامدهای حمله سایبری به یک بیمارستان ممکن است فراتر از همان مرکز گسترش یابد و بر دسترسی بیماران به خدمات درمانی در مراکز مجاور و نیز افزایش مرگ‌ومیر بیمارستانی اثر بگذارد (۲). در مطالعه‌ای درباره حمله باج‌افزاری در ماه مه ۲۰۲۱ به چهار بیمارستان و دو بخش اورژانس مجاور، میانگین مراجعات روزانه از ۲۱۸۴ به ۲۵۱۴ نفر افزایش یافت. تعداد ورود بیماران با آمبولانس از ۱۷۴۱ به ۲۳۵۴ رسید، میانه زمان انتظار برای ورود به اتاق معاینه از ۲۱ به ۳۱ دقیقه افزایش یافت و تعداد بیمارانی که قبل از معاینه مرکز را ترک کردند، از ۱۵۸ به ۳۶۰ نفر رسید. در این مطالعه، تعداد موارد تأیید شده سکته مغزی در دو اورژانس مجاور بیمارستان‌های آسیب‌دیده نیز از ۲۲ مورد پیش از حمله به ۴۷ مورد در دوره حمله و بازیابی افزایش یافت. نویسندگان این افزایش را عمدتاً به اختلال در فعالیت مراکز تخصصی سکته مغزی در بیمارستان‌های هدف و انتقال بیماران به تعداد کمتری از مراکز فعال منطقه نسبت دادند. با وجود افزایش حجم بیماران، زمان انجام سی‌تی‌اسکن و زمان شروع درمان حاد سکته مغزی افزایش معنی‌داری نداشت.(3) در یک مطالعه مبتنی بر داده‌های بیمه Medicare در ایالات متحده که پیامدهای حملات باج‌افزاری را در بیمارستان‌های هدف بررسی کرد، حجم پذیرش بیماران بستری در هفته نخست حمله حدود ۱۷ تا ۲۵ درصد کاهش یافت. در مقابل، در بیمارانی که در زمان آغاز حمله از قبل در بیمارستان بستری بودند، مرگ‌ومیر داخل بیمارستان افزایش نشان داد؛ به‌طوری‌که برآوردها حاکی از افزایش نسبی حدود ۲۱ تا ۳۶ درصدی این پیامد بود. این افزایش در بیمارستان‌هایی که حملات شدیدتری را تجربه کرده بودند، بیشتر گزارش شد (۲). یافته‌ها نشان می‌دهند که حملات باج‌افزاری علاوه بر کاهش ظرفیت ارائه خدمات و پذیرش بیماران، ممکن است با افزایش خطر مرگ در بیمارانی که هنگام وقوع حمله در بیمارستان بستری هستند، همراه باشند.(2)

در یک مرور نظام‌مند که در سال ۲۰۲۶ منتشر شد، گزارش شد که در مراکز درمانی نزدیک به بیمارستانی که هدف حمله سایبری قرار گرفته بود، میزان زنده‌ماندن بیماران پس از ایست قلبی خارج از بیمارستان، همراه با وضعیت عصبی مطلوب، از ۴۰ درصد به ۴/۵ درصد کاهش یافته بود. همچنین، در مطالعه‌ای دیگر مشخص شد که در مناطق روستایی، رسیدن به نزدیک‌ترین بیمارستانی که از حمله باج‌افزاری آسیب ندیده بود، ۴ تا ۷ برابر بیشتر از مناطق شهری زمان می‌برد .(4)

از منظر سلامت عمومی عفونی، دست‌کم دو پیامد بالقوه اهمیت دارند. نخست، انتقال بیماران به مراکز مجاور و افزایش ازدحام در اورژانس ممکن است ارزیابی بیماران مشکوک به بیماری‌های واگیر را به تأخیر اندازد و اجرای به‌موقع اقدامات احتیاطی و کنترل عفونت را دشوارتر کند. از آنجا که این پیامد در منابع مورد استناد مستقیماً در ایران بررسی نشده است، باید آن را استنباطی محتمل، و نه یافته‌ای اثبات‌شده در کشور، تلقی کرد. دوم، اختلال در سامانه‌های آزمایشگاهی، ارتباطات و ثبت و انتقال داده‌ها می‌تواند تجمیع و گزارش به‌موقع اطلاعات میکروب‌شناسی را مختل کند و در نتیجه،

پایش مقاومت ضدمیکروبی یا شناسایی خوشه‌های بیماری را به تأخیر اندازد.

در ایران، هرچند پرونده‌های بستری عمدتاً به‌صورت کاغذی نگهداری می‌شوند، خلاصه‌ای از اطلاعات بیماران در سامانه‌های رایانه‌ای ثبت می‌شود. بنابراین، کاغذی‌بودن پرونده‌ها به معنای مصون‌بودن فرایندهای درمانی و نظارتی از پیامدهای حملات سایبری نیست؛ اختلال در سامانه‌های ثبت اطلاعات، آزمایشگاهی یا ارتباطی همچنان می‌تواند بر دسترسی به داده‌ها، انتقال نتایج و گزارش‌دهی اثر بگذارد. ازاین‌رو، پیش‌بینی روش‌های جایگزین برای ثبت و بازیابی اطلاعات، انتقال نتایج حیاتی آزمایشگاهی و تداوم گزارش‌دهی در زمان اختلال، می‌تواند به حفظ ایمنی بیماران و تداوم فعالیت‌های مراقبت و پایش سلامت عمومی کمک نماید.

اختلال در دسترسی به اطلاعات بیمار و سامانه‌های دیجیتال

در کشورهایی که پرونده الکترونیک سلامت در بیمارستان‌ها به‌طور گسترده استفاده می‌شود، ازکارافتادن این پرونده‌ها ممکن است کارکنان را ناگزیر به استفاده از روش‌های کاغذی نماید؛ آمادگی ناکافی برای این وضعیت می‌تواند خود منشأ اختلال باشد. مرور نظام‌مند اخیر شامل ۵۹ مطالعه نشان داد که قطعی سامانه‌های پرونده الکترونیک با تأخیر در تجویز و اجرای دستورات دارویی، افزایش خطر خطاهای دارویی در بخش‌های مراقبت ویژه و تأخیر در تصمیم‌گیری‌های مربوط به مراقبت پایان عمر همراه بوده است (4). این یافته‌ها را نمی‌توان بدون تعدیل به بیمارستان‌های ایران تعمیم داد؛ زیرا پرونده‌های بستری در ایران عمدتاً کاغذی‌اند. با این‌حال، گزارش حمله سایبری به یک بیمارستان دانشگاهی ۵۰۰ تخت‌خوابی در ایالت ورمونت آمریکا در اکتبر ۲۰۲۰ نشان داد که اختلال اینترنت، پرونده الکترونیک سلامت و سامانه‌های پست الکترونیک به مدت ۲۶ روز، ارتباطات و سامانه پیجینگ را نیز تحت تأثیر قرار داد و هماهنگی بالینی را دشوار کرد (۵). این نمونه بر وابستگی مراقبت به مجموعه‌ای از زیرساخت‌های دیجیتال، فراتر از پرونده بیمار، تأکید می‌کند.

در بیماران مبتلا به عفونت، پیامد اختلال سایبری می‌تواند تأخیر در دسترسی یا انتقال اطلاعاتی باشد که مستقیماً بر تصمیم‌گیری تشخیصی و درمانی اثر می‌گذارند؛ از جمله سابقه عفونت ناشی از میکروارگانیسم‌های مقاوم به آنتی بیوتیک ها، سوابق حساسیت یا واکنش‌های نامطلوب دارویی، ضرورت رعایت احتیاطات تماسی یا هوابرد و رژیم ضدمیکروبی فعلی بیمار. در محیطی که پرونده بستری کاغذی است، این اطلاعات ممکن است در پرونده فیزیکی ثبت شده باشند، اما نتایج آزمایشگاهی و تصویربرداری، سامانه‌های نسخه‌نویسی، ارتباطات داخلی یا دسترسی به اطلاعات قبلی همچنان ممکن است به زیرساخت‌های دیجیتال وابسته باشند. بنابراین، اختلال سایبری لزوماً به معنای ناپدیدشدن پرونده کاغذی نیست؛ ممکن است به تأخیر در تولید، انتقال، مشاهده یا تطبیق اطلاعات مکمل بینجامد. وجود روش‌های جایگزین برای ثبت و انتقال نتایج و دستورات می‌تواند خطر تأخیر یا خطا در تصمیم‌گیری بالینی را کاهش دهد.

اختلال در خدمات آزمایشگاهی

آزمایشگاه نقطه‌ای است که قطع سامانه‌ها بیشترین اثر را بر تشخیص بیماری های عفونی می‌گذارد. حمله باج‌افزار BlackSuit به سرویس ملی آزمایشگاه‌های سلامت آفریقای جنوبی در ۲۲ ژوئن ۲۰۲۴، که تشخیص آسیب‌شناسی بیش از ۸۰ درصد جمعیت آن کشور را بر عهده دارد، سامانه اطلاعات آزمایشگاهی و اینترنت را ۴۰ روز غیرقابل‌دسترس کرد. تست ها به موارد فوری محدود شد، زمان پاسخ‌دهی در بیشتر موارد دو برابر شد (شمارش کامل سلولی از کمتر از ۲ ساعت به ۴ ساعت) و نتایج از راه تلفن، پیام‌رسان، نمابر و پیک منتقل گردید (6). نویسندگان آن گزارش درباره تست های اختصاصی بیماری های عفونی (مانند HIV یا سل) داده‌ای ارائه نکرده‌اند و احتمال افزایش عوارض و مرگ را فرضیه‌ای می‌دانند که نیازمند مطالعه است (6).

در لندن، حمله باج‌افزار Qilin به شرکت ارائه‌دهنده خدمات آسیب‌شناسی Synnovis در ۲۰۲۴ به لغو هزاران قرار و عمل انجامید. بر پایه گزارش‌ها، ۱۷۰ بیمار دچار آسیب شدند که بیشتر آن‌ها «آسیب کم» طبقه‌بندی شد، و در بررسی ایمنی مرگ یک بیمار، انتظار طولانی برای پاسخ آزمایش خون یکی از عوامل مؤثر شناخته شد (7). هرچند این داده‌ها از گزارش‌های خبری است و نه مقاله داوری‌شده، نشان می‌دهد تأخیر آزمایشگاهی می‌تواند مستقیماً به پیامد بالینی منتهی شود. برای عفونت‌های تهدیدکننده حیات مانند باکتریمی و منتژیت که تصمیم درمانی به کشت خون و رنگ‌آمیزی گرم وابسته است، چنین تأخیرهایی اهمیت ویژه دارد.

تجهیزات پزشکی متصل به شبکه

بسیاری از تجهیزات پزشکی، از دستگاه‌های تصویربرداری مانند MRI و CT و تحلیل‌گرهای آزمایشگاهی تا پمپ‌های

انفوزیون و مانیتورهای پایش علائم حیاتی، برای تبادل داده، ارسال نتایج یا دریافت اطلاعات و دستورهای مرتبط، به شبکه‌ها و سامانه‌های دیجیتال بیمارستان متصل هستند. برخی از این تجهیزات عمر طولانی دارند و از سیستم‌عامل‌ها یا نرم‌افزارهای قدیمی استفاده می‌کنند که به‌روزرسانی یا پشتیبانی امنیتی آن‌ها ممکن است با محدودیت‌هایی همراه باشد. در چنین شرایطی، حمله سایبری می‌تواند به آلودگی دستگاه، بهره‌برداری از آسیب‌پذیری‌های امنیتی آن یا اختلال در عملکرد سامانه‌های مرتبط و دسترسی به خروجی‌های تشخیصی منجر شود.

در جریان حمله باج‌افزاری WannaCry در سال ۲۰۱۷، آلودگی برخی تجهیزات پزشکی در مراکز درمانی آمریکا گزارش شد و شرکت Siemens Healthineers نیز با انتشار اطلاعیه‌های امنیتی، درباره احتمال تأثیر این بدافزار بر برخی تجهیزات تصویربرداری و تشخیصی خود هشدار داد (۸). همچنین، سازمان غذا و داروی آمریکا (FDA) در سال ۲۰۱۵ درباره آسیب‌پذیری امنیتی احتمالی پمپ انفوزیون Hospira Symbiqو امکان دسترسی غیرمجاز به آن از طریق شبکه هشدار داد؛ بااین‌حال، این هشدار به معنای اثبات سوءاستفاده عملی از این آسیب‌پذیری نبود.(9)

اختلال در مراقبت از بیمار لزوماً به آسیب مستقیم یا ازکارافتادن خود دستگاه محدود نمی‌شود. حتی اگر تجهیزات پزشکی همچنان از نظر فنی قابل استفاده باشند، اختلال در سرورهای ذخیره و بازیابی تصاویر، سامانه‌های اطلاعات آزمایشگاهی، زیرساخت شبکه یا سامانه‌های احراز هویت می‌تواند دسترسی کارکنان درمانی به نتایج و اطلاعات ضروری را مختل کند یا ضرورت قطع موقت اتصال برخی تجهیزات به شبکه را در پی داشته باشد. این مسئله به‌ویژه در مراقبت از بیماران بدحال اهمیت دارد؛ زیرا اختلال در دسترسی به داده‌های پایش، نتایج آزمایشگاهی یا اطلاعات موردنیاز برای تصمیم‌گیری درمانی ممکن است بر ارزیابی وضعیت بیمار و تداوم مراقبت اثر بگذارد.

در بیمارستان‌های ایران نیز، با وجود نگهداری عمده پرونده‌های بستری به‌صورت کاغذی و ثبت رایانه‌ای خلاصه‌ای از اطلاعات بیماران، وابستگی تجهیزات پزشکی و سامانه‌های تشخیصی به زیرساخت‌های دیجیتال می‌تواند همچنان منشأ آسیب‌پذیری باشد. بنابراین، ارزیابی امنیت سایبری مراکز درمانی باید علاوه بر سامانه‌های ثبت اطلاعات، ارتباطات و ذخیره‌سازی داده‌ها، تجهیزات پزشکی متصل به شبکه و پیامدهای احتمالی اختلال در آن‌ها برای ایمنی بیمار را نیز در بر گیرد.

توجه ویژه به بیماران بدحال و وابسته به تجهیزات حیاتی

بیماران بستری مبتلا به عفونت‌های شدید، به‌ویژه افراد دارای بیماری‌های زمینه‌ای متعدد و نارسایی هم‌زمان چند عضو، ممکن است به مراقبت در بخش مراقبت‌های ویژه، تهویه مکانیکی، پایش مداوم علائم حیاتی و نظارت مستمر بر وضعیت قلبی نیاز داشته باشند. در برخی بیماران، اختلال در عملکرد تجهیزات پایش قلبی یا سامانه‌های مرتبط با حمایت همودینامیک و تنفسی، از جمله تجهیزات تهویه مکانیکی و در موارد مقتضی دستگاه‌های ضربان‌ساز، می‌تواند پیامدهای بالینی جدی به دنبال داشته باشد. ازاین‌رو، ارزیابی خطر حملات سایبری نباید صرفاً به سامانه‌های ثبت اطلاعات، تصویربرداری یا انتقال نتایج آزمایشگاهی محدود شود، بلکه باید وابستگی تجهیزات پزشکی حیاتی و زیرساخت‌های پشتیبان آن‌ها به شبکه‌ها و سامانه‌های دیجیتال نیز در نظر گرفته شود. مراکز درمانی باید با همکاری تیم‌های بالینی، مهندسی پزشکی و فناوری اطلاعات مشخص کنند که اختلال در هر سامانه چه پیامدی برای مراقبت از بیمار دارد و چه اقدامات جایگزینی برای حفظ پایش، حمایت تنفسی و قلبی‌عروقی و تداوم درمان لازم است. همچنین، برنامه‌های آمادگی و پاسخ باید شامل اولویت‌بندی بیماران وابسته به تجهیزات حیاتی، تداوم تأمین برق و خدمات پشتیبان، پیش‌بینی روش‌های ایمن جایگزین برای پایش و مراقبت و تعیین مسئولیت کارکنان در شرایط اختلال باشد.

پیامدها بر تشخیص و درمان؛ نمونه‌ای از اختلال در مدیریت مصرف آنتی بیوتیک ها

گزارش بیمارستان ورمونت، نمونه‌ای از پیامدهای حمله سایبری بر مراقبت از بیماران مبتلا به عفونت است. در جریان این حمله، به‌دلیل اختلال در ارتباطات، فرایند تأیید مصرف آنتی بیوتیک های محدودشده با وقفه مواجه شد و یادآورهای الکترونیک مربوط به مدت درمان از دسترس خارج شدند. همچنین، بازبینی به‌موقع بیماران مبتلا به باکتریمی دشوار شد و نتایج آزمایشگاهی از طریق نمابر یا به‌صورت دستی به بخش‌های بیمارستان انتقال یافتند. اختلال در دسترسی به ابزارهای دوز بندی مبتنی بر فارماکوکینتیک و دشواری پایش غلظت خونی وانکومایسین نیز مدیریت درمان را با چالش مواجه کرد. در واکنش به این شرایط، اعضای تیم مدیریت

مصرف آنتی بیوتیک ها هر روز به آزمایشگاه مراجعه می‌کردند، کشت‌های خون مثبت را بررسی می‌کردند و نتایج را به‌صورت حضوری در اختیار تیم‌های درمانی قرار می‌دادند. حتی پس از بازیابی سامانه‌ها، بخشی از داده‌های میکروب‌شناسی قابل بازیابی نبود، آنتی‌بیوگرام‌ها ناقص ماندند و اطلاعات مصرف آنتی بیوتیک ها برای ارسال به سامانه ثبت ملی در دسترس نبود.(5)

اگرچه این گزارش مربوط به بیمارستانی با پرونده الکترونیک بستری است، تجربه آن برای نظام سلامت ایران نیز آموزنده است. در بیمارستان‌های ایران که پرونده‌های بستری عمدتاً به‌صورت کاغذی نگهداری می‌شوند، اختلال در سامانه‌های آزمایشگاهی و ارتباطی همچنان می‌تواند دسترسی به نتایج تشخیصی و انتقال به‌موقع آن‌ها به تیم درمان را مختل کند. ازاین‌رو، پیش‌بینی روش‌های جایگزین برای اعلام نتایج حیاتی، ارتباط مستمر آزمایشگاه با بخش‌های بالینی و ثبت دقیق اطلاعات در دوره اختلال، از اقدامات مهم برای حفظ ایمنی بیمار به شمار می‌روند.

این تجربه همچنین نشان می‌دهد که پیامدهای حمله سایبری ممکن است به دوره اختلال محدود نمانند و با ایجاد نقص در داده‌های میکروب‌شناسی و اطلاعات مصرف آنتی بیوتیک ها، فرایندهای پایش و ارزیابی را در دوره‌های بعد نیز تحت تأثیر قرار دهند. در خدمات سرپایی، اختلال در سامانه‌های دیجیتال، به‌ویژه نسخه‌نویسی الکترونیک، می‌تواند ثبت خدمات، تجویز دارو و تداوم دریافت درمان را با مشکل مواجه کند. در برخی گزارش‌ها، اختلال ناشی از حملات سایبری با کاهش مراجعات بیماران به مراکز درمانی و کاهش ارائه خدمات درمانی، از جمله تجویز و تزریق دارو، همراه بوده است (۴)؛ بااین‌حال، میزان و نوع این پیامدها به ساختار خدمات سلامت و میزان وابستگی فرایندهای ارائه خدمت به سامانه‌های دیجیتال بستگی دارد. در ایران، تدوین دستورالعمل‌های جایگزین برای نسخه‌نویسی و ثبت خدمات سرپایی، همراه با پیش‌بینی روش‌های ایمن برای مستندسازی و پیگیری درمان در زمان اختلال، می‌تواند به کاهش وقفه در ارائه خدمات کمک کند.

افشای اطلاعات راهبردی سلامت عمومی

پیامدهای حملات سایبری به مراکز درمانی ممکن است فراتر از اختلال در ارائه خدمات و نقض محرمانگی اطلاعات بیماران باشد و به افشای داده‌های راهبردی سلامت عمومی نیز منجر شود. دسترسی غیرمجاز به نتایج میکروب‌شناسی،

آنتی‌بیوگرام‌ها، اطلاعات مصرف آنتی بیوتیک ها و داده‌های ثبت و پایش بیماری‌ها می‌تواند اطلاعات ارزشمندی درباره الگوهای مقاومت ضدمیکروبی، پراکندگی عوامل بیماری‌زا و وضعیت اپیدمیولوژیک بیماری‌های واگیر در مناطق مختلف فراهم کند. در صورت دسترسی به داده‌های کافی و به‌روز، این اطلاعات ممکن است تصویری از روندهای محلی مقاومت میکروبی یا شناسایی و افزایش موارد برخی بیماری‌ها در شهرها و مناطق مشخص ارائه دهد. چنین داده‌هایی، افزون بر حساسیت ناشی از اطلاعات فردی بیماران، از نظر راهبردی نیز اهمیت دارند؛ زیرا می‌توانند وضعیت آسیب‌پذیری نظام سلامت و چالش‌های تشخیصی و درمانی یک منطقه را آشکار کنند. در هر حال، امکان استنباط الگوهای منطقه‌ای یا ملی به گستره، کیفیت و نمایندگی داده‌های در دسترس بستگی دارد. از این رو، حفاظت از این اطلاعات، محدودسازی دسترسی بر اساس نقش شغلی، ثبت و پایش دسترسی‌ها و پیش‌بینی سازوکارهای امن برای ذخیره‌سازی و تبادل داده‌ها باید بخشی از راهبرد امنیت سایبری مراکز درمانی و سامانه‌های مراقبت سلامت عمومی باشد

جدول ۱. خلاصه‌ای از شواهد منتخب درباره پیامد حملات سایبری بر مراقبت بالینی

منبع	رخداد / طراحی	یافته کلیدی
(1)	۳۷۴ حمله باج‌افزاری به مراکز درمانی آمریکا، ۲۰۱۶ تا ۲۰۲۱	۴۴ درصد با اختلال در مراقبت همراه بود؛ حملات سالانه از ۴۳ به ۹۱ رسید
(3)	چهار بیمارستان هدف و دو اورژانس مجاور، مه ۲۰۲۱	ورود با آمبولانس ۱٬۷۴۱ به ۲٬۳۵۴؛ ترک بدون ویزیت ۱۵۸ به ۳۶۰
(4)	مرور نظام‌مند ۵۹ مطالعه، سال ۲۰۲۶	۳۱۶ آسیب در سطح بیمار شامل تأخیر دارو، تأخیر آزمایش و بازتوزیع بیماران
(5)	بیمارستان دانشگاهی ورمونت، ۲۶ روز قطعی	تعلیق تأیید ضدمیکروب‌ها، آنتی‌بیوگرام ناقص، داده مصرف غیرقابل ارسال
(6)	سرویس ملی آزمایشگاه آفریقای جنوبی، ۴۰ روز قطعی	فقط آزمون‌های فوری؛ زمان پاسخ‌دهی در بیشتر موارد دو برابر
(7)	شرکت آسیب‌شناسی Synnovis در لندن، ۲۰۲۴	۱۷۰ بیمار دچار آسیب؛ مرگ یک بیمار با نقش تأخیر آزمایش خون

تهدید علیه صحت و یکپارچگی اطلاعات تشخیصی

پیامدهای حملات سایبری به مراکز درمانی ممکن است فراتر از ازکارافتادن سامانه‌ها یا تأخیر در دسترسی به اطلاعات باشد و صحت و یکپارچگی داده‌های تشخیصی را نیز تهدید کند. در صورت دسترسی غیرمجاز به سامانه‌های اطلاعات آزمایشگاهی یا تصویربرداری پزشکی، امکان تغییر، حذف یا انتساب نادرست نتایج آزمایشات و تصاویر یا گزارش‌های رادیولوژی وجود دارد. پژوهش‌های آزمایشی نیز، امکان دست‌کاری نتایج آزمایشگاهی در مسیر انتقال داده و تغییر تصاویر پزشکی در برخی سناریوهای تهدید سایبری را نشان داده‌اند (۱۰). چنین تغییراتی، در صورت شناسایی نشدن، می‌توانند به تفسیر نادرست وضعیت بیمار، تأخیر در تشخیص، انتخاب درمان نامناسب یا انجام اقدامات تشخیصی و درمانی غیرضروری منجر شوند. با این حال، باید میان امکان فنی این نوع دست‌کاری و وقوع مستند آن در حملات واقعی تمایز قائل شد. از این رو، حفاظت از صحت داده‌ها، ثبت و قابلیت پیگیری تغییرات، محدودسازی دسترسی‌های غیرمجاز و راستی‌آزمایی نتایج مشکوک باید در کنار اقداماتی که با هدف حفظ دسترس‌پذیری سامانه‌ها انجام می‌شوند، مورد توجه قرار گیرند (۱۰).

راهبردهای پیشنهادی برای پزشکان معالج و مراکز درمانی

هر مرکز درمانی باید برنامه‌ای عملیاتی برای مواجهه با حملات سایبری و اختلال در سامانه‌های اطلاعاتی تدوین کند که با زیرساخت‌ها و فرایندهای واقعی آن مرکز متناسب باشد. این برنامه باید با مشارکت کارکنان بالینی و واحد فناوری اطلاعات تدوین و به‌طور دوره‌ای تمرین شود. در بیمارستان‌هایی که پرونده‌های بستری به‌صورت کاغذی نگهداری می‌شوند، لازم است دسترسی ایمن به پرونده‌های فیزیکی، فرم‌های جایگزین برای ثبت دستورات پزشکی و نتایج آزمایش‌ها، و روش‌های مشخص برای انتقال و پیگیری اطلاعات در زمان اختلال، پیش‌بینی شود.

همچنین، مسیرهای ارتباطی جایگزین میان آزمایشگاه میکروب‌شناسی و تیم‌های درمانی، به‌ویژه برای اعلام سریع نتایج حیاتی، کشت‌های خون مثبت و موارد باکتریمی، باید از پیش تعریف شوند. تهیه راهنماهای درمان تجربی و تعیین رویکردهای جایگزین برای مدیریت داروهایی که به پایش بالینی یا

آزمایشگاهی نیاز دارند نیز می‌تواند به تداوم درمان کمک نماید. افزون بر این، باید روش ثبت موقت نتایج آزمایشگاهی و میزان مصرف آنتی بیوتیک ها، همراه با سازوکار تطبیق، تکمیل و بازیابی مستندات پس از بازگشت سامانه‌ها، مشخص باشد.(5)

سناریوهای حمله سایبری باید در برنامه‌های مدیریت بحران بیمارستان و تمرین‌های آمادگی برای ارجاع بیماران فوری گنجانده شوند. مشارکت متخصصان بیماری‌های عفونی و اعضای کمیته کنترل عفونت در تدوین و ارزیابی این برنامه‌ها ضروری است؛ زیرا اختلال در ارتباطات، دسترسی به نتایج آزمایشگاهی و انتقال بیماران می‌تواند بر درمان عفونت‌ها و اجرای اقدامات کنترل عفونت اثر بگذارد. همچنین، اختلالات سایبری و پیامدهای بالینی ناشی از آن‌ها باید به‌عنوان رخدادهای مرتبط با ایمنی بیمار ثبت و بررسی شوند تا از تجربیات حاصل برای اصلاح برنامه‌های آمادگی و پاسخ استفاده شود.

در مراکز ارائه‌دهنده خدمات سرپایی نیز باید برای اختلال در نسخه‌نویسی الکترونیک، مسیر جایگزینی تعریف شود تا ثبت ایمن نسخه‌ها، دسترسی بیماران به داروهای موردنیاز و تداوم درمان تا زمان بازیابی سامانه‌ها امکان‌پذیر باشد.

محدودیت‌ها و نتیجه‌گیری

شواهد موجود درباره پیامدهای حملات سایبری در مراکز درمانی با محدودیت‌هایی همراه است. بخش عمده مطالعات منتشرشده از نوع مشاهده‌ای هستند و تفکیک اثر مستقیم حمله سایبری از سایر عوامل مؤثر بر پیامدهای بالینی، از جمله شدت بیماری بیماران و اختلالات هم زمان در ارائه خدمات، همیشه امکان‌پذیر نیست. افزون بر این، بخشی از شواهد از کشورهایی با زیرساخت‌های دیجیتال و الگوهای ثبت اطلاعات پزشکی متفاوت با ایران به دست آمده و برخی یافته‌ها نیز مبتنی بر گزارش‌های رسانه‌ای هستند. بنابراین، نتایج مربوط به اختلال در سامانه‌های اطلاعاتی و پیامدهای ناشی از آن‌ها باید با توجه به تفاوت‌های ساختاری نظام‌های سلامت تفسیر شوند و تعمیم مستقیم آن‌ها به شرایط ایران نیازمند احتیاط است. همچنین، میزان و نوع پیامدهای ناشی از دسترسی غیرمجاز به داده‌های سلامت، به گستره اطلاعات افشا شده، کیفیت و روزآمدی داده‌ها و امکان ارتباط دادن آن‌ها با مناطق جغرافیایی مشخص بستگی دارد.

در ایران، اگرچه پرونده‌های بستری عمدتاً به‌صورت کاغذی نگهداری می‌شوند و خلاصه‌ای از اطلاعات بیماران در سامانه‌های رایانه‌ای ثبت می‌شود، وابستگی فرایندهای درمانی به زیرساخت‌های دیجیتال همچنان قابل توجه است. نسخه‌نویسی الکترونیک در خدمات سرپایی و سامانه‌های آزمایشگاهی، تصویربرداری و ارتباطی می‌توانند در معرض اختلال قرار گیرند. ازاین‌رو، پیامد حملات سایبری را نباید صرفاً به ازکارافتادن پرونده الکترونیک بیمارستانی محدود دانست؛ اختلال در دسترسی به نتایج تشخیصی، انتقال اطلاعات، فرایندهای تجویز و ثبت داده‌ها نیز ممکن است بر تداوم مراقبت و ایمنی بیمار اثر بگذارد. افزون بر اختلال در دسترسی به اطلاعات، دسترسی غیرمجاز و افشای داده‌های سلامت نیز می‌تواند پیامدهای مهمی داشته باشد. داده‌های میکروب‌شناسی، الگوهای مقاومت ضدمیکروبی، اطلاعات مصرف آنتی بیوتیک ها و داده‌های مراقبت بیماری‌های واگیر، در صورت کفایت و روزآمدبودن، ممکن است تصویری از وضعیت اپیدمیولوژیک یا الگوهای مقاومت در مناطق مختلف ارائه دهند. افشای این اطلاعات، علاوه بر نقض محرمانگی بیماران، می‌تواند اطلاعاتی با اهمیت راهبردی درباره وضعیت سلامت عمومی و چالش‌های تشخیصی و درمانی مناطق مختلف در اختیار افراد غیرمجاز قرار دهد.

در مجموع، حملات سایبری می‌توانند از طریق تأخیر در دریافت نتایج آزمایشگاهی، اختلال در ارتباطات و فرایندهای درمانی، افزایش فشار بر مراکز درمانی مجاور و آسیب به صحت یا کامل‌بودن داده‌های ثبت‌شده، ایمنی بیمار و تداوم خدمات سلامت را تحت تأثیر قرار دهند.

گستره این پیامدها به نوع حمله، میزان وابستگی مرکز درمانی به سامانه‌های دیجیتال و توانایی آن در حفظ خدمات هنگام اختلال بستگی دارد. بنابراین، آمادگی برای مواجهه با این رخدادها باید متناسب با زیرساخت‌های هر مرکز طراحی شود و هم‌زمان، تداوم ارائه خدمات و حفاظت از محرمانگی، صحت و دسترس‌پذیری داده‌ها را در بر گیرد. حفظ دسترسی به پرونده‌های کاغذی، پیش‌بینی مسیرهای جایگزین برای انتقال و ثبت اطلاعات، تداوم مراقبت از بیماران بدحال، بازیابی و تطبیق داده‌ها پس از رفع اختلال، محدودسازی دسترسی بر اساس نقش شغلی و پایش دسترسی به اطلاعات، از اجزای مهم این آمادگی هستند. این اقدامات باید در کنار راهبردهای پیشگیرانه امنیت سایبری و نه به‌عنوان جایگزین آن‌ها اجرا شوند. در نهایت، امنیت سایبری مراکز درمانی نه‌تنها بخشی از برنامه‌ریزی برای ایمنی بیمار و تداوم خدمات، بلکه یکی از الزامات حفاظت از داده‌های حساس و پشتیبانی از نظام مراقبت و پایش سلامت عمومی است.

REFERENCE

1. Neprash HT, McGlave CC, Cross DA, et al. Trends in ransomware attacks on US hospitals, clinics, and other health care delivery organizations, 2016-2021. JAMA Health Forum. 2022;3(12):e224873.

2. Neprash H, McGlave C, Nikpay S. Hacked to Pieces? The Effects of Ransomware Attacks on Hospitals and Patients. Am Econ J Econ Policy. 2026;18(1):256-281.

3. Dameff C, Tully J, Chan TC, et al. Ransomware attack associated with disruptions at adjacent emergency departments in the US. JAMA Netw Open. 2023;6(5): e2312270. doi:10.1001/jamanetworkopen.2023.12270

4. Straw I, Kumar D, Kweon S, Selzer J, Dameff C, Tully J. Unveiling patient-level harms and at-risk clinical groups during hospital cyberattacks: systematic review of global case studies and social media data. J Med Internet Res. 2026;28: e88257. doi:10.2196/88257

5. Smith LM, Ahern JW. Antimicrobial stewardship during a cyberattack. Infect Control Hosp Epidemiol. 2022; 43:1275.

6. Cassim S, Chapanduka ZC. Cyberattack on the National Health Laboratory Service of South Africa: implications, response and recommendations. S Afr Med J. 2024;114(12): e2549.

7. Qilin ransomware attack on NHS supplier contributed to patient fatality. The Register. 2025 Jun 26. https://www.theregister.com/2025/06/26/qilin_ransomware_nhs_death/

8. Report: WannaCry attacks hit U.S. hospitals. AuntMinnie. 2017 May. https://www.auntminnie.com/imaging-informatics/enterprise-imaging/is/article/15617612/report-wannacry-attacks-hit-us-hospitals

9. Hospitals advised to stop using vulnerable computerized drug pumps (report on FDA safety communication on Hospira Symbiq). Help Net Security. 2015 Aug 3. https://www.helpnetsecurity.com/2015/08/03/hospitals-advised-to-stop-using-vulnerable-computerized-drug-pumps/

10. Eichelberg M, Kleber K, Kämmerer M. Cybersecurity challenges for PACS and medical imaging. Acad Radiol. 2020;27(8):1126-39.