

## به کارگیری دستگاه شخصی در بیمارستان: یک مطالعه کیفی

معصومه شهبازی<sup>۱</sup> (M.Sc.)، مصطفی امینی رارانی<sup>۲</sup> (Ph.D.)، مریم جهانبخش<sup>۳\*</sup> (Ph.D.)، شهرام طهماسبیان<sup>۴</sup> (Ph.D.)

۱- گروه مدیریت و فناوری اطلاعات سلامت، دانشگاه علوم پزشکی اصفهان، اصفهان، ایران

۲- مرکز تحقیقات عوامل اجتماعی موثر بر سلامت، دانشگاه علوم پزشکی اصفهان، اصفهان، ایران

۳- مرکز تحقیقات فناوری اطلاعات در امور سلامت، دانشگاه علوم پزشکی اصفهان، اصفهان، ایران

۴- گروه انفورماتیک پزشکی، دانشکده فناوری‌های نوین، دانشگاه علوم پزشکی شهرکرد، شهرکرد، ایران

تاریخ دریافت: ۱۴۰۱/۱۲/۲۰ تاریخ پذیرش:

jahanbakhsh.him@gmail.com

نویسنده مسئول، تلفن: ۰۹۱۳۳۲۱۵۳۵۱

### چکیده

هدف: رویکرد دستگاه خود را بیاورید یا Bring Your Own Device (BYOD) استفاده از دستگاه‌های همراه شخصی را در جهت انجام اهداف سازمانی و شغلی ترویج داده است اما استفاده از این رویکرد می‌تواند چالش‌ها و مخاطرات مختلفی را برای سازمان‌های سلامت به همراه داشته باشد. این پژوهش با هدف شناسایی مولفه‌های آمادگی بیمارستان‌ها در استفاده از BYOD انجام شده است که می‌تواند در جهت تدوین سیاست‌های مناسب و در نهایت کنترل چالش‌های مرتبط مورد استفاده قرار گیرد. مواد و روش‌ها: پژوهش حاضر از انواع مطالعات کیفی می‌باشد. مصاحبه‌شوندگان با استفاده از نمونه‌گیری هدفمند و با رویکرد گلوله برفی تا رسیدن به سطح اشباع انتخاب شدند. جمع‌آوری داده‌ها از طریق مصاحبه نیمه‌ساختارمند با ۱۵ نفر از خبرگان حوزه BYOD انجام شد. داده‌های کیفی با روش تحلیل مضمون (تماتیک) و به کمک نرم‌افزار MAXQDA نسخه ۱۲ تحلیل شد.

یافته‌ها: بر اساس نتایج ۶ مضمون اصلی و ۲۳ زیرمضمون شناسایی شد. اصول مدیریتی، منابع انسانی، هزینه، زیرساخت فنی، ملاحظات قانونی و ملاحظات اخلاقی به عنوان ۶ مضمون اصلی در آمادگی بیمارستان‌ها در رابطه با BYOD نقش دارند. نتیجه‌گیری: تمرکز بر موضوعات شناسایی شده در قالب تدوین و پیاده‌سازی برنامه‌های رسمی و همچنین سیاست‌گذاری‌های مناسب توسط مدیران و ذی‌نفعان سازمان‌ها می‌تواند به بهره‌مندی مناسب از مزایای BYOD و کاهش هر چه بیش تر چالش‌های مرتبط به آن بی‌انجامد.

واژه‌های کلیدی: فن‌آوری‌های اطلاعات، پیاده‌سازی فن‌آوری اطلاعات سلامت، دستگاه شخصی خود را بیاورید، سازمان‌های مراقبت بهداشتی

### مقدمه

در سال‌های اخیر سلامت یکی از صنایع پیشرو در استفاده از رویکرد "دستگاه خود را بیاورید" یا "Bring Your Own Device (BYOD)" بوده است. این رویکرد به استفاده از دستگاه‌های همراه شخصی مانند تلفن‌های هوشمند، نوت بوک و تبلت در محل کار به منظور انجام اهداف شغلی اشاره دارد [۴-۱] و بیمارستان‌ها به عنوان یکی از سازمان‌های مهم صنعت سلامت به سرعت در حال اتخاذ سیاست‌های مدیریت دستگاه‌های همراه شخصی هستند [۵]. کارکنان سازمان‌ها برای توسعه کارهای خود به اطلاعات به هنگام نیاز دارند و BYOD فراهم‌کننده چنین موقعیت مهمی است [۶]. در سازمان‌های مراقبت بهداشتی عموماً از دستگاه‌های همراه شخصی برای انجام وظایفی مانند مستندسازی اطلاعات،

دسترسی به سوابق سلامت بیماران، مدیریت اطلاعات دارویی و نتایج اقدامات آزمایشگاهی و تصویربرداری، ارتباط با هم‌تایان یا بیماران و جست‌وجوی منابع مرجع استفاده می‌شود [۲].

به‌کارگیری این رویکرد مزایایی هم‌چون تحرک و پویایی کارکنان [۸،۷،۴،۳]، انعطاف‌پذیری بیشتر در ارائه خدمات [۹،۷،۴،۳]، صرفه‌جویی در هزینه سازمان [۹] و ایجاد فضای رقابتی [۸،۳] را به دنبال دارد. به دلیل مزایای ویژه که سیاست‌گذاری BYOD در حوزه سلامت به همراه دارد به طور مداوم در حال رشد است [۲،۱] به گونه‌ای که کارکنان سازمان‌ها به استفاده از دستگاه‌های همراه شخصی در محل کار ترغیب شده و حدود ۹۵ درصد آن‌ها از ابزارهای شخصی خود برای اهداف شغلی استفاده می‌کنند [۳،۲]. بدین ترتیب

در به‌کارگیری BYOD است. لذا در پژوهش حاضر به شناسایی مولفه‌های مرتبط با آمادگی بیمارستان‌ها در به‌کارگیری BYOD پرداخته شد. لازم به ذکر است این پژوهش تبیین هر چه بیشتر بخش کیفی از یک مطالعه ترکیبی است که در سال ۲۰۲۲ در مجله Proceedings of Singapore Healthcare به چاپ رسیده است [۲۰].

## مواد و روش‌ها

پژوهش حاضر با کد اخلاقی

IR.MUI.RESEARCH.REC.1398.743 یک مطالعه کیفی

است که در آن داده‌ها با استفاده از مصاحبه‌های نیمه ساختاریافته گردآوری شده‌اند. مصاحبه‌شوندگان با استفاده از نمونه‌گیری هدفمند انتخاب شدند و به منظور تکمیل شبکه انسانی از نمونه‌گیری گلوله برفی نیز استفاده شد. معیارهای ورود برای مصاحبه‌شوندگان شامل آشنا بودن با مفهوم BYOD، داشتن سابقه کاری مرتبط با بخش فن‌آوری اطلاعات سلامت و آشنایی با ویژگی‌های فنی دستگاه‌های همراه شخصی (چرخه حیات یک فن‌آوری از امکان‌سنجی تا نگاه‌داشت آن) مانند تلفن‌های هوشمند، نوت بوک و تبلت بود. از آن‌جا که چارچوب مشخصی در خصوص آمادگی بیمارستان در به‌کارگیری از BYOD وجود نداشت به منظور تدوین راهنمای مصاحبه مطالعات مرتبط با آمادگی بیمارستان‌ها در خصوص سایر فن‌آوری‌های اطلاعات در صنعت سلامت بررسی شد و مولفه‌های اصلی آمادگی بیمارستان در استفاده یک فن‌آوری استخراج گردید. در نهایت طی سه جلسه بحث و مذاقه توسط تیم پژوهش، سؤال اصلی و سؤالات فرعی مرتبط با BYOD در قالب راهنمای مصاحبه تدوین شد.

جمع‌آوری داده‌ها، داده‌ها از طریق مصاحبه‌های نیمه ساختاریافته به صورت حضوری و تلفنی تا رسیدن به سطح اشباع داده‌ها انجام شد. لازم به ذکر است ۷ مصاحبه به صورت حضوری و چهره به چهره انجام شد اما به دلیل ابیهدمی کرونا و رعایت فاصله‌گذاری اجتماعی سایر مصاحبه‌ها به شکل تلفنی انجام پذیرفت. برای انجام مصاحبه ابتدا مصاحبه‌شوندگان مشخص شده و بعد از هماهنگی با فرد مذکور، کسب رضایت و تمایل وی برای شرکت در مصاحبه، مصاحبه توسط نویسنده اول به صورت حضوری و یا تلفنی در زمان و مکان مورد نظر مصاحبه‌شوندگان انجام شد. قبل از مصاحبه، راهنمای مصاحبه در اختیار مصاحبه‌شوندگان قرار داده شد و پس از آگاهی آن‌ها به موضوع مصاحبه و ارائه توضیحات در خصوص هدف پژوهش، مصاحبه‌ها آغاز

امروزه BYOD دیگر انتخابی برای سازمان‌ها نیست و به یک استاندارد برای کسب و کار در عصر دیجیتال تبدیل شده است [۱۰]. اما علی‌رغم مزایای نام برده شده، اجرای رویکرد BYOD برای سازمان‌ها چالش‌های امنیتی [۱۱-۱۴]، قانونی [۱۱] و مالی [۱۵] را به همراه دارد که هنگام کاربرد آن در حوزه سلامت افزایش می‌یابد چرا که محرمانه بودن اطلاعات سلامت از اهمیت ویژه‌ای برخوردار است. مارشال در مطالعه خود امنیت داده‌ها، پروتکل‌های استاندارد و دستورالعمل‌های شفاف، مباحث قانونی مرتبط با داده‌های شخصی افراد، نوع دستگاه مورد استفاده و وابستگی به اینترنت دستگاه‌ها را از چالش‌های کلیدی کاربرد BYOD در سازمان‌های مراقبت بهداشتی معرفی کرده است [۱۴].

با فراگیر شدن BYOD انتظار می‌رود سیاست‌های مرتبط با این رویکرد توسط ذینفعان و مدیران سازمان‌ها از جمله سازمان‌های مراقبت بهداشتی اتخاذ گردد [۱۶]. اما سیاست‌های موجود مبهم بوده و در موارد بسیاری حتی سیاست‌های به‌کارگیری آن توسط سازمان‌ها اتخاذ نشده است [۱۷]. بسیاری از بیمارستان‌ها برای ایجاد سیاست‌های موثر در خصوص کاهش خطرات BYOD با چالش روبرو هستند [۱۰] و می‌توان گفت اجرای این رویکرد از بزرگ‌ترین چالش‌های فن‌آوری اطلاعات برای مدیران بیمارستان‌ها محسوب می‌شود [۲].

پذیرش و کنترل تهدیدات BYOD مستلزم تدوین استراتژی‌ها و سیاست‌های مرتبط قبل از استفاده از آن در سازمان است [۱۸]. زیرا اگرچه به‌کارگیری این فن‌آوری مزایای خاصی را برای کارکنان فراهم کرده به گونه‌ای که تماماً آن را برای اهداف شخصی و کاری استفاده کنند اما موضوعاتی همچون حفاظت از حریم خصوصی کارکنان و داده‌های ذخیره شده آن‌ها بر دستگاه‌های همراه شخصی تهدیدی چالش برانگیز می‌باشد [۱۹،۲]. این مشکل در صنعت سلامت که داده‌های شخصی بیمارمان مطرح است پررنگ‌تر بوده و استفاده از دستگاه‌های همراه شخصی در مراکز مراقبت بهداشتی خطرات و چالش‌های مضاعفی را برای متخصصان فن‌آوری اطلاعات سلامت که مسئول امنیت داده‌های سازمان هستند، به همراه دارد [۲۰] که خود مستلزم توانمندی سازمان‌ها در کنترل ویژگی‌های و پیچیدگی‌های این رویکرد و کاهش یا مهار مخاطرات پیش رو می‌باشد [۱۰،۱۶]. به نظر می‌رسد اولین قدم در دستیابی به این مهم با توجه به خلاء تحقیقاتی و عملیاتی موضوع BYOD در صنعت سلامت ایران و نیز تمرکز مطالعات انجام شده در خارج از ایران بر موضوع سائیری و امنیتی آن، شناسایی مولفه‌های آمادگی بیمارستان‌ها

منظور مدیریت، دسته‌بندی و کدگذاری داده‌ها از نرم‌افزار MAXQDA نسخه ۱۲ استفاده شد.

قابلیت اعتماد داده‌های کیفی. بدین منظور، از ۴ معیار ارزیابی پژوهش‌های کیفی پیشنهاد شده توسط لینکون و گوبا [۲۰] استفاده شد. جهت افزایش قابل قبول بودن داده‌ها، علاوه بر اشتغال ذهنی پژوهشگر به مطالعه، از تلفیق در تمام مراحل تحقیق از جمله تلفیق روش‌های گردآوری داده‌ها (مصاحبه، مشاهده نوشتار و حاشیه‌نویسی، مشاهده اسناد) استفاده شد. در خصوص انتقال‌پذیری سعی شد علاوه بر توصیف پرمایه (Thick description) فرایند تحقیق و یافته‌ها از نمونه‌گیری هدفمند نیز استفاده شود. قابلیت اطمینان با استفاده از نظرات تکمیلی اساتید راهنما و مشاور در کدگذاری و تحلیل متن مصاحبه‌ها به دست آمد. همچنین متن‌های پیاده شده در اختیار مصاحبه‌شوندگان قرار گرفت و بازخوردهای لازم از آن‌ها دریافت شد. برای افزایش تاییدپذیری سعی شد، تمامی فرایندها انجام پژوهش بدون جهت‌گیری و فارغ از ارزش‌های شخصی انجام شود.

ملاحظات اخلاقی. ضمن اخذ کد اخلاق از دانشگاه، هر یک از مصاحبه‌ها بعد از توضیح اهداف پژوهش و رضایت مصاحبه‌شوندگان انجام شد و هر زمان که تمایلی به ارائه جزئیات بیشتر از سمت ایشان نبود مصاحبه اتمام می‌یافت. همچنین به منظور ضبط مصاحبه‌ها از آن‌ها اجازه کسب شد.

## نتایج

مشخصات مصاحبه‌شوندگان. جامعه پژوهش شامل ۱۵ نفر مصاحبه‌شونده می‌باشد. ۲ نفر از مصاحبه‌شوندگان زن و سایر افراد مرد بودند. افراد مورد مصاحبه دارای سابقه کار در سطوح اجرایی و دانشگاهی بودند. سابقه کاری افراد حداقل ۳ سال و حداکثر ۲۰ سال می‌باشد. مشخصات این افراد به تفکیک هر یک در جدول ۱ ارائه شده است.

پس از انجام مصاحبه‌ها ۶ مضمون و ۲۲ زیرمضمون از تحلیل داده‌های کیفی حاصل شد. این مضامین و زیرمضمون‌ها به همراه کدهای مرتبط با هر یک در جدول ۲ نمایش داده شده است.

می‌شدند. قبل از شروع مصاحبه با مصاحبه‌شوندگان رابطه مناسب (معرفی محقق، ذکر انگیزه و هدف از انجام پژوهش، اخذ رضایت شفاهی برای شرکت در مصاحبه، محرمانه ماندن نام مصاحبه‌شونده و مکالمات ضبط شده، علت انتخاب فرد مصاحبه‌شونده و اخذ رضایت جهت ضبط مکالمات) برقرار شد که این امر جلب اعتماد شرکت‌کننده و علاقه بیشتر وی به شرکت در مطالعه را به دنبال داشت. در پایان مصاحبه نیز اطلاعات دموگرافیک مصاحبه‌شوندگان مانند سابقه کاری، میزان تحصیلات، سطح سازمانی و سمت فعلی جمع‌آوری گردید. برای ثبت مصاحبه‌ها با کسب اجازه از مصاحبه‌شوندگان از دستگاه ضبط صدا استفاده شد و هم‌زمان با آن نیز یادداشت‌برداری و ثبت نکات مهم و کلیدی توسط پژوهشگر انجام شد. سپس مصاحبه‌های ضبط شده بدون هیچ‌گونه دخل و تصرفی در فاصله زمانی کوتاهی بعد از انجام مصاحبه پیاده‌سازی شد و توسط خود محقق به صورت متن نوشتاری در قالب فایل Word در آمد. همچنین فایل پیاده‌سازی مصاحبه‌ها برای مصاحبه‌شوندگان ارسال شد تا در صورت نیاز تصحیح و تکمیل گردد. در نهایت پس از انجام ۱۵ مصاحبه اشباع داده‌ها حاصل شد. مصاحبه‌ها در بازه زمانی خرداد ۱۳۹۸ تا مرداد ماه ۱۳۹۹ انجام شد و مدت زمان هر یک از ۱۵ دقیقه تا یک ساعت متغیر بود.

تحلیل داده‌ها. داده‌های گردآوری شده با استفاده از روش تحلیل مضمون بر اساس الگوی گام به گام تحلیل تماتیک ارائه شده توسط براون و کلارک انجام شد [۱۸]: آشناسازی با داده‌ها از طریق گوش دادن به مصاحبه‌های ضبط شده، پیاده‌سازی آن‌ها، خواندن و بازخوانی متن مصاحبه‌ها و خواندن یادداشت‌های مصاحبه‌کننده انجام شد. در این مرحله معانی و الگوهای خاصی که ممکن بود مرتبط با مولفه‌های آمادگی بیمارستان‌ها در به‌کارگیری BYOD باشد شناسایی شدند. بعد از مطالعه داده‌ها و آشنا شدن با آن‌ها فهرستی از اطلاعات مرتبط با آمادگی بیمارستان‌ها که به نظر حائز اهمیت و کلیدی بودند انتخاب شده و کدگذاری گردید. کدهای به دست آمده از مرحله قبل در قالب زیر مضمون‌های مولفه‌های آمادگی بیمارستان‌ها دسته‌بندی شدند. سپس چندین زیرمضمون که حاوی مفاهیم و معانی یکسانی در ارتباط با BYOD بودند در قالب مضامین اصلی طبقه‌بندی شدند. هر یک از مضامین و زیر مضمون‌ها، با توجه به محوریت موضوعشان در ارتباط با آمادگی بیمارستان‌ها برای بایود نام‌گذاری شدند. در نهایت گزارش حاصل از تحلیل داده‌های کیفی در قالب مقاله علمی نوشته شد. شایان ذکر است، به

## جدول ۱. ویژگی‌های مصاحبه‌شوندگان

شماره کد	جنسیت	تحصیلات	سابقه کاری	سابقه سطوح سازمانی
۱	مرد	دانشجوی دکترای تخصصی انفورماتیک پزشکی	۶ سال در حوزه فن‌آوری اطلاعات	اجرایی - دانشگاهی
۲	مرد	دکترای تخصصی انفورماتیک پزشکی	۱۲ سال در حوزه فن‌آوری اطلاعات/ ۴ سال در حوزه سلامت	دانشگاهی
۳	مرد	دکترای تخصصی انفورماتیک پزشکی	۱۷ سال	دانشگاهی
۴	مرد	دکترای تخصصی انفورماتیک پزشکی	۲۰ سال در حوزه فن‌آوری اطلاعات سلامت	اجرایی - دانشگاهی
۵	مرد	دکترای تخصصی انفورماتیک پزشکی	۴ سال در حوزه فن‌آوری اطلاعات/ ۵ سال در حوزه فن‌آوری اطلاعات سلامت	اجرایی - دانشگاهی
۶	مرد	دکترای تخصصی انفورماتیک پزشکی	۱۵ سال در حوزه فن‌آوری اطلاعات سلامت	اجرایی - دانشگاهی
۷	مرد	دکترای تخصصی انفورماتیک پزشکی	۲۰ سال	دانشگاهی
۸	مرد	دکترای تخصصی انفورماتیک پزشکی	۱۳ سال در حوزه فن‌آوری اطلاعات سلامت	اجرایی
۹	مرد	دکترای تخصصی انفورماتیک پزشکی	۲۰ سال در حوزه فن‌آوری اطلاعات سلامت	دانشگاهی
۱۰	زن	دکترای تخصصی انفورماتیک پزشکی	۹ سال در حوزه انفورماتیک/ ۲۰ سال در حوزه سلامت	دانشگاهی
۱۱	مرد	کارشناس ارشد نرم افزار	۱۹ سال در حوزه فن‌آوری اطلاعات سلامت	اجرایی
۱۲	مرد	کارشناس ارشد نرم افزار	۲۸ سال در حوزه فن‌آوری اطلاعات سلامت	اجرایی - دانشگاهی
۱۳	مرد	کارشناس ارشد نرم افزار	۱۲ سال در حوزه فن‌آوری اطلاعات	اجرایی - دانشگاهی
۱۴	مرد	کارشناسی ارشد مهندسی شیمی	۳ سال در حوزه فن‌آوری اطلاعات سلامت	اجرایی
۱۵	زن	دانشجوی دکترای تخصصی نرم افزار	۱۰ سال در حوزه فن‌آوری اطلاعات سلامت	اجرایی

پس از انجام مصاحبه‌ها ۶ مضمون و ۲۲ زیرمضمون از تحلیل داده‌های کیفی حاصل شد. این مضامین و زیرمضمون‌ها به همراه کدهای مرتبط با هر یک در جدول ۲ نمایش داده شده است.

## جدول ۲. مضامین، زیرمضمون‌ها و کدهای مرتبط با آمادگی بیمارستان‌ها در بکارگیری BYOD

مضمون	زیرمضمون (فراوانی نظرات)	کد	
۱: اصول مدیریتی	۱۱: تدوین استراتژی (۱۰)	۱۱۱: عملیاتی	
		۱۱۲: فنی	
	۱۲: استقرار کمیته راهبردی BYOD (۱)	۱۲۱: تعیین کارگروه و اعضای تیم	
		۱۲۲: تعیین مدیر پروژه	
	۱۳: امکان‌سنجی (۷)	۱۳۱: عملیاتی	
		۱۳۲: فنی	
	۱۴: ارتباطات بین بخشی (۱)	۱۴۱: ایجاد ارتباط موثر مابین وزارتخانه‌های مرتبط	۱۴۲: ایجاد ارتباط پایدار مابین وزارتخانه‌های مرتبط
			۱۴۳: ایجاد ارتباط موثر مابین سازمان و نهادهای خصوصی و دولتی
			۱۴۴: ایجاد ارتباط پایدار مابین سازمان و نهادهای خصوصی و دولتی
			۲۱: نوع کاربر (۱۵)
	۲: منابع انسانی	۲۲: ایجاد انگیزه (۱۰)	۲۲۱: مالی
			۲۲۲: غیرمالی
		۲۳: حفظ ایمنی (۱)	۲۳۱: جلوگیری از انتقال آلودگی‌های بیمارستانی توسط وسایل شخصی
			۲۳۲: پاک کردن تجهیزات شخصی با شوینده‌های مجاز
۲۴: فرهنگ (۸)		۲۴۱: فرهنگ سازی	
		۲۴۲: کاهش مقاومت در برابر تغییر	
۲۵: آموزش (۳)		۲۵۱: شیوه‌های صحیح بکارگیری دستگاه‌های شخصی	
		۲۵۲: روش‌های اجتماعی مقابله با خطرات امنیتی	
۳: هزینه		۳۱: مستقیم (۱۴)	۳۱۱: نحوه بازپرداخت
			۳۱۲: راه اندازی
	۳۲: غیرمستقیم (۷)	۳۲۱: استهلاك	

۳۲۲: نگهداشت	
۴۱۱: پشتیبانی از اتصال دستگاه ها به شبکه سازمان	
۴۱۲: پشتیبانی از بروز رسانی نرم افزارهای دستگاههای شخصی	
۴۱۳: پشتیبانی از خرید دستگاه های همگن	
۴۱۴: پشتیبانی از الزامات نرم افزاری	۴۱: پشتیبانی (۶)
۴۱۵: پشتیبانی از الزامات سخت افزاری	
۴۱۶: پشتیبانی از تهیه تجهیزات مورد نیاز برای اتصال دستگاههای شخصی	
۴۲۱: یکپارچگی داده ها و اطلاعات	
۴۲۲: یکپارچگی نرم افزارها	۴۲: یکپارچگی (۳)
۴۲۳: یکپارچگی پایگاه های داده	
۴۳۱: محل ذخیره اطلاعات	
۴۳۲: گواهی امنیتی نرم افزار	
۴۳۳: شناسنامه سخت افزاری و نرم افزاری	
۴۳۴: آنتی ویروس ها و بدافزارها	
۴۳۵: مفقود شدن دستگاه شخصی	
۴۳۶: تعریف سطوح دسترسی	
۴۳۷: حفاظت از اطلاعات شخصی کاربر	
۴۳۸: لاگ فایل ها	
۴۳۹: پایش و نظارت شبکه	۴۳: امنیت داده ها (۱۵)
۴۳۱۰: فایروال	
۴۳۱۱: کنترل تجهیزات فیزیکی قبل از اتصال	
۴۳۱۲: بکارگیری اسکریپت رکورد	
۴۳۱۳: احراز هویت	
۴۳۱۴: پروتکل های امنیت شبکه	
۴۳۱۵: تعیین سطح حساسیت داده ها	
۴۳۱۶: بستر ارتباطی با محل ذخیره سازی	
۴۴۱: راه اندازی شبکه خصوصی	
۴۴۲: پایگاه داده های ابری	۴۴: شبکه و ارتباطات (۱۰)
۴۴۳: مدیریت دسترسی به شبکه	
۴۴۴: تداوم فرآیندها	
۴۵۱: تعیین حداقل های نرم افزاری	
۴۵۲: طراحی تحت وب	
۴۵۳: مدیریت کیفیت	۴۵: نرم افزاری (۹)
۴۵۴: تهیه نسخه همراه نرم افزار	
۴۵۵: ماهیت نرم افزارها	
۴۶۱: محدودیت بکارگیری سخت افزارها	
۴۶۲: تعیین حداقل های سخت افزاری	۴۶: سخت افزاری (۶)
۴۶۳: شناسایی سخت افزارها	
۵۱۱: اخذ رضایت از کاربر برای استفاده از دستگاه شخصی	
۵۱۲: اخذ رضایت از کاربر برای اتصال به وسیله شخصی وی	۵۱: رضایتنامه ها (۲)
۵۲۱: قرارداد برای تعیین سرور	
۵۲۲: قرارداد مربوط به آموزش نرم افزار	۵۲: قراردادها (۱)
۵۲۳: قرارداد مربوط به پشتیبانی نرم افزار	
۵۳۱: عدم دسترسی به اطلاعات شخصی کاربر	
۵۳۲: تعهدات کاربر	۵۳: تعهدات (۵)
۵۳۳: کسب اجازه از مراجع قانونی	
۵۴۱: بخشنامه های بازپرداخت	
۵۴۲: قوانین حفاظت اطلاعات	۵۴: بخشنامه و آیین نامه (۹)
۵۴۳: قوانین سطوح دسترسی	
۵۴۴: سطوح تدوین قوانین	
۶۱۱: کارکنان سازمان	
۶۱۲: بیمار	۶۱: حریم خصوصی (۶)
۶۲۱: عدم انتشار اطلاعات توسط کاربر	
۶۲۲: عدم دسترسی افراد غیر مجاز به اطلاعات بیمار	۶۲: محرمانگی (۶)
۶۲۳: حفاظت از اطلاعات شناسایی کننده بیمار	

۴: زیرساخت فنی

۵: ملاحظات قانونی

۶: ملاحظات اخلاقی

از سوی دیگر ایجاد انگیزه‌های مثبت مالی و غیرمالی برای کاربران رویکرد BYOD ضروری عنوان شد به طوری که یکی از افراد اظهار داشت:

"مثلاً کسانی که لپ‌تاپ شخصی‌شان را می‌ارند به جای استفاده از کامپیوتر سازمانی آخر ماه یک سفر بهشون داده بشه. یک جوری تشویق کنند که جبران کنند این آورده اون فرد رو". (مصاحبه‌شونده ۱۳)

حفظ ایمنی افراد به منظور جلوگیری از انتقال آلودگی‌های بیمارستانی از طریق دستگاه‌های شخصی به خانه در زمان به‌کارگیری BYOD یکی از موارد مورد توجه در مصاحبه‌ها بود که نیازمند خط‌مشی‌های مربوطه برای کاهش آلودگی و تامین امنیت نیروی انسانی می‌باشد. یکی از افراد در این باره بیان داشت:

"ایمنی هم در وسایل سازمانی هم در وسایل شخصی و پاک کردن آن با شوینده‌های مجاز انجام بشه". (مصاحبه‌شونده ۱۱)

مورد دیگری که توسط مصاحبه‌شوندگان بیان شد توجه به مسائل فرهنگ سازمانی از جمله فرهنگ‌سازی و کاهش مقاومت در برابر تغییر بود؛ علی‌الخصوص که این شیوه به دلیل ایجاد حالت مانیتورینگ برای کاربران مقاومت بیشتری را می‌تواند به وجود بیاورد. مورد دیگر آموزش و آگاهی کارکنان و نیروی انسانی است که اهمیت ویژه‌ای در به‌کارگیری رویکرد BYOD دارد. طبق نظر یکی از افراد: "از همه مهم‌تر شاید بحث آموزش و آگاه‌سازی پرسنل باشه". (مصاحبه‌شونده ۷)

هزینه. طبق نظرات مصاحبه‌شوندگان هزینه‌های مرتبط با به‌کارگیری BYOD را می‌توان در دو دسته مستقیم و غیرمستقیم دسته‌بندی کرد. طبق این تقسیم‌بندی هزینه‌های مربوط به راه‌اندازی و نحوه بازپرداخت‌ها جزو هزینه‌های مستقیم بوده و هزینه‌های استهلاک و نگهداشت دستگاه‌های شخصی در حوزه هزینه‌های غیرمستقیم طبقه‌بندی می‌شود. یکی از نقل‌قول‌ها در این حوزه آورده شده است: "عمر مفید وسایل الکترونیکی دوتا فاکتور داره یکی مدت زمان و دیگری میزان استفاده. وقتی من به عنوان کاربر وسیله الکترونیکی شخصی خودم رو میارم و در سازمان استفاده می‌کنم طبیعتاً از مدت زمان عمرش کم میشه. پس از لحاظ مالی باید یک gain برای من داشته باشه". (مصاحبه‌شونده ۲)

زیرساخت فنی. رویکرد BYOD به طور غیر قابل انکاری با موضوعات فنی چه در ارتباط با ساختارهای سازمانی و چه در ارتباط با دستگاه‌های شخصی در ارتباط است و مصاحبه‌شوندگان به حوزه‌های مختلفی از آن اشاره نموده‌اند. به طور مثال مصاحبه‌شوندگان به ضرورت پشتیبانی فنی برای

اصول مدیریتی. مصاحبه‌شوندگان در خصوص اصول مدیریتی مرتبط با به‌کارگیری BYOD به مواردی از جمله تدوین استراتژی، استقرار کمیته راهبردی BYOD، امکان‌سنجی و ارتباطات بین بخشی اشاره نموده‌اند. در تدوین استراتژی توجه به استراتژی‌های فنی و عملیاتی مهم ذکر شده به گونه‌ای که یکی از مصاحبه‌شوندگان بیان داشت:

"داشتن یک استراتژی یا شیوه‌نامه که بر مبنای آن بتوانند تصمیم‌گیری کنند از نظر من خیلی مهم است". (مصاحبه‌شونده ۷)

از سوی دیگر به منظور نظارت بر فعالیت‌های مرتبط با رویکرد BYOD استقرار کمیته اختصاصی برای تعیین چشم‌انداز و مأموریت‌ها، تعیین مدیر پروژه و اعضای تیم و در نهایت تدوین برنامه استراتژیک از وظایف این کمیته نام برده شده است. ضرورت انجام امکان‌سنجی به خصوص در حوزه‌های عملیاتی، فنی و مالی پیش از شروع پروژه در اکثریت مصاحبه‌ها ذکر شده است. نظر یکی از افراد بدین شرح بود:

"قبلش باید یک مطالعه امکان‌سنجی یا feasibility study داشته باشید و ببینید چند درصد کادر شما سخت‌افزاری که دارند که قابل قبول است و چقدر حاضرند که از device خودتون استفاده کنند". (مصاحبه‌شونده ۶)

در مبحث ارتباطات بین بخشی مصاحبه‌شوندگان وجود ارتباطات موثر و پایدار مابین بخش‌های مختلف از جمله وزارت‌خانه‌ها و نهادهای خصوصی مرتبط را مورد نیاز دانستند. به طور مثال نظر یکی از افراد بدین شرح بود:

"وزارت بهداشت باید با سازمان‌های دیگه‌ای که روی این قضیه تاثیرگذار هستند مثل وزارت اطلاعات و ارتباطات در ارتباط باشه و با آنها ارتباطات خوبی برقرار کنه". (مصاحبه‌شونده ۱۰)

منابع انسانی. منابع انسانی از اصلی‌ترین بخش‌های هر سازمان می‌باشد که به منظور ایجاد هرگونه تغییری نیازمند توجه ویژه است. بر اساس دیدگاه مصاحبه‌شوندگان تعیین نوع کاربران که لازمه آن شناسایی فرآیندها و بخش‌های بیمارستان و هم‌چنین شناسایی و دسته‌بندی کارکنان بیمارستان (مکانیسم‌های فرآیند محور و نقش محور) است پیش از به‌کارگیری رویکرد BYOD از اهمیت بالایی برخوردار است. در این خصوص یکی از نظرات بدین شکل بود:

"باید segmentation داشته باشیم که قاعدتاً این هم بر اساس role base باشه. یا می‌تونه بر اساس یک فرآیند خاص یا یک بخش خاص توی بیمارستان باشه". (مصاحبه‌شونده ۱۴)

است در سطح خود دیتابیس هم مطرح است". (مصاحبه‌شونده ۱۲)

علاوه بر این موارد مصاحبه‌شوندگان به منظور استفاده کارآمد از BYOD تطابق کلیه سخت‌افزارهایی که با نرم‌افزارهای سیستمی در ارتباطند را با پیش‌نیازهای آن سیستم مهم دانسته و به اهمیت ثبت دستگاه‌ها نیز اشاره نموده‌اند. یکی از افراد در این باره بیان داشت:

"هر وسیله شخصی که شخص با خودش میاره باید رجیستر بشه و مثلاً شماره مک آدرسش ثبت بشه". (مصاحبه‌شونده ۲)

ملاحظات قانونی. در زمان اجرای یک فرآیند جدید در هر سازمان موارد قانونی مهمی وجود دارد که عدم توجه به آن‌ها پیش از اجرا می‌تواند در عدم اجرای موفق آن تأثیرگذار باشد. از جمله این موارد اخذ رضایت‌نامه از افراد است که طبق نظر خبرگان از اهمیت بالایی برخوردار است و سازمان‌ها ملزم هستند تا اطلاعات مرتبط و شرایط خاص از جمله دسترسی به ابزار شخصی افراد را در صورت نیاز به طور کامل برای افراد شرح داده و در این خصوص از آن‌ها کسب اجازه نماید. علاوه بر این کارکنان نیز باید به طور آزادانه امکان تصمیم‌گیری در جهت تکمیل نمودن فرم رضایت‌نامه را داشته باشند. مورد مهم دیگر بحث قراردادها است. قرارداد یک توافق الزام‌آور میان اشخاص یا سازمان‌هاست که در آن حقوق و تکالیف هر دو طرف در موضوعی معین مشخص شده است. بر همین اساس مصاحبه‌شوندگان ایجاد قرارداد مناسب مطابق با فعالیت‌های مورد نظر را لازم و ضروری دانسته‌اند. در این رابطه یکی از افراد بیان داشت:

"بحث قرارداد که شامل مباحث پشتیبانی و خرید آموزش نرم‌افزار و مسئله تعیین سرور". (مصاحبه‌شونده ۱۵)

علاوه بر این مصاحبه‌شوندگان ذکر نمودند که در هنگام استفاده از BYOD سازمان‌ها موظفند تعهدات مشخصی را در ارتباط با کارکنانشان و همچنین با وزارتخانه در جهت حفظ کیفیت اجرای این فرآیند ایجاد نمایند. علاوه بر این، تعهدات کاربر مبنی بر حفظ امنیت و استفاده از ابزار شخصی برای اهداف کاری نیز ضرورت دارد. یکی از نظرات بدین شرح است:

"چیزی که مهمه تعهدهای عدم افشای اطلاعاته که باید به طور جدی‌تر به اون‌ها پرداخته بشه". (مصاحبه‌شونده ۲)

در بحث بخش‌نامه و آیین‌نامه ذکر شده است که قوانین مرتبط در به‌کارگیری BYOD می‌بایست در سطح مناسبی تدوین شده و راهنماهای مناسبی به شکل بخش‌نامه برای اجرای درست آن تعیین شود که مواردی از جمله سطوح

کاربران BYOD اشاره کرده و خدمات پشتیبانی سخت‌افزاری و نرم‌افزاری را مورد نیاز دانسته‌اند. در این باره یکی از افراد بیان داشت:

"تکنیکال ساپورت لازم برای این کار از سوی سازمان برای افراد مهیا باشه و بتونن این ساپورت را همان‌طور که دستگاه‌های سازمانی دریافت می‌کنند دستگاه‌های شخصی نیز دریافت کنند". (مصاحبه‌شونده ۷)

مورد بعدی موضوع یک‌پارچگی داده‌هاست که می‌بایست در تمام جنبه‌های کلیدی طراحی، پیاده‌سازی و استفاده از هر سیستمی که داده‌ها را ذخیره، پردازش یا بازیابی می‌کند وجود داشته باشد و در این خصوص مصاحبه‌شوندگان تأکید کردند که این یک‌پارچگی باید در داده‌ها، نرم‌افزارها و پایگاه‌های داده باشد و از جزیره‌ای کار کردن اجتناب شود. مبحث امنیت داده‌ها در حوزه بهداشت و درمان به دلیل آن‌که محرمانگی اطلاعات بیمار از اهمیت بالایی برخوردار است به کرات توسط مصاحبه‌شوندگان مورد توجه بوده و ایجاد راهکارهای استاندارد و مورد اعتماد را به منظور اجرای این فرآیند در بیمارستان ضروری دانسته‌اند. یکی از افراد در این باره بیان داشت:

"یکی از مهم‌ترین عوامل بحث امنیت اطلاعات هست. به نظر من بر اساس اون کاربرد نرم‌افزاری که روی این سیستم نصب میشه یک دسته‌بندی را انجام بدیم و هر نرم‌افزاری را اجازه ندهیم که بر روی سیستم افراد قابل نصب و استفاده باشه بسته به نوع کاربر. ما یک فضای مبتنی بر کلود را لازم داریم که حتماً بایستی ابزار مبتنی بر کلود ما پرایوت باشه". (مصاحبه‌شونده ۱۰)

در به‌کارگیری BYOD به دلیل وجود حجم وسیعی از دستگاه‌های شخصی کارکنان، موضوع شبکه و ارتباطات مورد توجه بسیاری از مصاحبه‌شوندگان بوده است. به طور مثال افراد بیان داشتند که نحوه اتصال بی‌سیم یا باسیم باید مشخص شده و برای هرکدام نیز به منظور اتصال دستگاه‌های شخصی امکاناتی پیش‌بینی شود. در حوزه نرم‌افزاری مصاحبه‌شوندگان بیان داشتند که تدوین مجموعه‌ای از ویژگی‌ها، رفتار و عملکرد نرم‌افزارهای مرتبط با رویکرد BYOD می‌بایست تعیین و مشخص شوند و برای سازگاری‌های نرم‌افزاری با انواع سیستم‌ها نیز فکری شود. یکی از نقل‌قول‌های مرتبط بدین شرح است:

"وقتی شما در یک سیستم windows base کار می‌کنید نمی‌تونید یک تبلت اندروید را بیاورید مگر این‌که نرم‌افزار و بانک اطلاعاتی که طراحی شده فارغ از نوع سیستم بوده یا برای آن‌ها هم فکری شده باشه. این در سطح سیستم عامل

ابتکاری در روال امور سازمان را ارائه کرده است. این سه اصل با نتایج مطالعه در حوزه اصول مدیریتی و به خصوص تدوین استراتژی‌های فنی و استقرار کمیته راهبردی مطابقت دارد. برودین و همکارانش نیز در پژوهش خود در ارتباط با چالش‌های مدیریت دستگاه خود را بیاورید [۲۲] به اهمیت تحلیل محیط اشاره نموده است که با نتایج به دست آمده در خصوص امکان سنجی در مطالعه مطابقت دارد. علاوه بر این برودین در مطالعه دیگری [۱۱] ضرورت وجود ارتباطات را در اجرای استراتژی‌های BYOD ذکر کرده که همسو با نتایج حاضر در خصوص ارتباطات بین بخشی می‌باشد. در مطالعه کری نیز چهار بعد فن‌آوری، امنیت، ذینفعان و سازمان به عنوان ابعاد اصلی چارچوب پذیرش BYOD نام برده شده‌اند [۲۳]. معرفی ذینفعان به عنوان یکی از ارکان اصلی اجرای این برنامه با نتایج این پژوهش مطابقت نداشته و اشاره‌ای بدان نشده است اما سایر مفاهیم موجود در ابعاد دیگر با معیارهای به دست آمده در این مطالعه تطابق دارد. البته لازم به ذکر است تاکید بر روی ایجاد ارتباطات پایدار و مناسب مابین سازمان‌های مرتبط با یک‌دیگر صورت گرفته اما به طور دقیق به ذینفعان اشاره‌ای نشده است.

توجه به نوع کاربر، ایجاد انگیزه و حفظ ایمنی کارکنان، فرهنگ‌سازی و آموزش به‌کارگیری BYOD و نیز تضمین هزینه‌های ایجاد تا نگاه‌داشت دستگاه‌های همراه از جمله جنبه‌های مدیریت منابع انسانی است که باید در بیمارستانی که به دنبال به‌کارگیری از دستگاه‌های همراه شخصی است مورد توجه قرار گیرد. طبق مطالعه وانی و همکارانش [۳] سیاست‌ها و اقدامات انجام شده در راستای مدیریت نیروی انسانی هم‌چون ترویج فرهنگ حفظ امنیت داده‌ها و آموزش مستمر آن به کارکنان موجب بهبود تعهدات سازمان در محافظت از داده‌های بیمارستان می‌شود که این نتایج با زیرمضمون‌های به دست آمده در منابع انسانی هماهنگی دارد. زاهدت و همکارانش در چارچوب ارائه شده خود در ارتباط با امنیت BYOD [۲۴] به نقش اصلی مردم یا همان نیروی انسانی در کنار مدیریت سیاست‌ها و فن‌آوری اشاره نموده‌اند که با یافته‌های مرتبط با نیروی انسانی در این مقاله همسو می‌باشد. طبق مطالعه مایر که در ارتباط با مدیریت دستگاه‌های همراه در بیمارستان‌ها انجام شده [۵]، رویکرد آموزش دادن به کاربران را نسبت به تلاش برای کنترل فن‌آوری در کوتاه مدت عملی‌تر دانسته و آن را به عنوان فرصتی برای در مدیریت هر چه بهتر استفاده از تلفن‌های همراه در بیمارستان‌ها معرفی کرده است. برودین نیز در چارچوب مدیریت BYOD [۱۱] به اهمیت وجود آموزش و ایجاد ارتباطات برای درک بهتر

دسترسی، حفاظت از اطلاعات و نحوه بازپرداخت‌ها را شامل شود.

**ملاحظات اخلاقی.** ملاحظات اخلاقی به حریم خصوصی افراد و محرمانگی اطلاعات اشاره دارد. طبق نظر مصاحبه‌شوندگان در به‌کارگیری BYOD حریم خصوصی افراد اهمیت به سزایی دارد چرا که از یک طرف با اطلاعات بیمار رو به رو هستیم و از سوی دیگر به دلیل استفاده از دستگاه‌های شخصی امکان انتشار فایل‌های شخصی کاربر وجود دارد. بر همین اساس موضوعات حریم خصوصی در هر دو حوزه بیماران و کارکنان می‌بایست مورد توجه باشد. طبق نظر یکی از افراد:

"اصول دو طرفه رعایت بشه یعنی هم از بحث بیمارستان حقوق آن رعایت بشه و هم از سطح فرد چون ممکنه در کامپیوتر فرد موارد شخصی وی هم باشه". (مصاحبه‌شونده ۱۲)

موضوع دیگر مورد توجه مصاحبه‌شوندگان بحث محرمانگی اطلاعات در حوزه بهداشت و درمان بود که به دلیل وجود داده‌های سلامت بیماران از اهمیت بالایی برخوردار است. یکی از نقل قول‌های مرتبط با این موضوع عبارتست از: "بیش‌ترین خطری که وجود داره اینه که محرمانگی افراد به هم بخوره. مثلاً فرض کنید که در موبایل من عکسی از بیمار وجود داره و بچه من در هنگام بازی با موبایل اشتباهی یکسری از اطلاعات موبایل منو انتقال بده". (مصاحبه‌شونده ۴)

## بحث و نتیجه‌گیری

مؤلفه‌های مرتبط با آمادگی بیمارستان‌ها در به‌کارگیری BYOD در ۶ موضوع اصلی اصول مدیریتی، منابع انسانی، هزینه، زیرساخت فنی، ملاحظات قانونی و ملاحظات اخلاقی دسته‌بندی شد. به منظور بیان جزئیات هر مفهوم زیرمضمون‌های مرتبط با آن ارائه و کدهای اختصاصی برای هر زیرمضمون با تکیه بر راهکارهای مناسب برای اجرای سیاست‌های مرتبط با BYOD بر اساس نظرات مصاحبه‌شوندگان ارائه گردید.

مطابق مضامین استخراج شده بیمارستان‌ها به منظور برآورد ساختن جنبه‌های مدیریتی BYOD نیازمند تدوین استراتژی، امکان سنجی، کمیته راهبردی و ارتباطات بین بخشی هستند. مارشال [۱۲] در مطالعه خود به منظور کمک به سازمان‌های مراقبت بهداشتی در توسعه و اجرای یک راهبرد موفق برای BYOD سه توصیه مشتمل بر همکاری مدیران ارشد و متخصصان فن‌آوری اطلاعات در ایجاد سیستم‌های امنیتی قوی، شناسایی مخاطرات احتمالی و پیش‌بینی تغییرات



دستگاه‌ها و امنیت اطلاعات اشاره شده که در این مطالعه نیز تایید شده است.

طبق نتایج مطالعه مارشال [۱۲] قانون در کنار مواردی هم چون امنیت، پروتکل‌ها و دستورالعمل‌ها، نوع دستگاه و وابستگی به اینترنت از چالش‌های اصلی BYOD در سلامت می‌باشد که می‌بایست مورد توجه سیاست‌گذاران قرار گیرد. در پژوهش کنونی نیز ملاحظات قانونی به عنوان یکی از ابعاد اصلی برنامه رسمی BYOD معرفی شد.

آگوشیم و همکارش [۲۱] استفاده از سیاست‌های موثر در خصوص BYOD و راه‌کارهای مدیریت دستگاه‌های همراه را در حفظ حریم خصوصی کاربر و محرمانگی اطلاعات دستگاه‌های شخصی کارکنان موثر دانسته‌اند. این نتایج با یافته‌های حاصل در خصوص حریم خصوصی کاربر و محرمانگی اطلاعات به عنوان ملاحظات اخلاقی کاملاً همسو می‌باشد.

از جمله محدودیت‌های این پژوهش می‌توان به عدم امکان مصاحبه حضوری به علت وقوع کرونا در مرحله انجام مصاحبه‌ها اشاره نمود.

با توجه به پیشرفت فن‌آوری اطلاعات و ارتباطات در دهه‌های اخیر، حرکت به سمت رویکردهایی مانند BYOD امری اجتناب‌ناپذیر است. لذا استفاده صحیح از این رویکرد و کاهش هر چه بیش‌تر چالش‌های مرتبط با آن به سیاست‌گذاری‌های مناسب نیازمند است. بر اساس پژوهش حاضر تمرکز بر اصول مدیریتی، نیروی انسانی، هزینه‌ها، زیرساخت‌های فنی و ملاحظات قانونی و اخلاقی به عنوان الزامات اصلی تدوین سیاست‌های برنامه BYOD در بیمارستان‌ها قلمداد شده و می‌تواند در ترسیم نقشه راه و تدوین سیاست‌ها به سیاست‌گذاران و متولیان امر کمک کند. به طور دقیق‌تر مدیران و سیاست‌گذاران می‌توانند با تدوین سیاست‌هایی در خصوص فرهنگ‌سازی، آموزش و ایجاد انگیزه در کارکنان، همچنین تدوین زیرساخت‌های مالی، قانونی و اخلاقی پذیرش و پیاده‌سازی BYOD را هموارتر کنند. در سطح دانشگاهی نیز با توجه به جدید بودن مفهوم این نوع فن‌آوری در سلامت باید به آموزش و ترویج به‌کارگیری BYOD اقدام نمود و پژوهش‌های بیش‌تری در این حوزه انجام داد.

### تشکر و قدردانی

نویسندگان از معاونت تحقیقات و فن‌آوری دانشگاه علوم پزشکی اصفهان که حمایت مالی این تحقیق را برعهده داشته قدردانی می‌نمایند.

کارمندان از روند اجرای این رویکرد اشاره نموده است که از این جهت با نتایج پژوهش حاضر در ارتباط با منابع انسانی که به طور دقیق به اهمیت آموزش و عوامل فرهنگی کارکنان اشاره کرده است؛ هم‌خوانی دارد.

الانصاری و همکارانش [۲۵] در مطالعه خود به لزوم ایجاد سیاست‌های مرتبط با پرداخت هزینه اشاره نموده‌اند و تاکید نموده‌اند که سازمان باید میزان و شیوه پرداخت هزینه تجهیزات پرسنلی، ارتباطات، تبادل اطلاعات و همچنین مالیات را تعیین کند. این نتایج با یافته‌های مطالعه فعلی که هزینه‌های مستقیم و غیر مستقیم را به عنوان مولفه‌های اصلی آمادگی بیمارستان‌ها شناسایی نموده است هماهنگی دارد.

زیرساخت فنی و توجه به استانداردهای به‌کارگیری دستگاه‌های شخصی همراه به عنوان یکی از جنبه‌های مهم آمادگی بیمارستان در اجرای BYOD حایز توجه است و بالاخص بحث امنیت داده‌ها موضوع بسیار مهمی است که دستیابی به آن توجه به استانداردهای مرتبط با این رویکرد را می‌طلبد [۱۹]. امنیت سایبری به عنوان یکی از بزرگ‌ترین چالش‌های صنعت سلامت است و BYOD خود به تنهایی یکی از تهدیدات اصلی امنیت سایبری است [۲]. وراکولیبیات و همکارانش در چارچوبی که در خصوص BYOD ارائه داده‌اند [۲۶] به منظور حفظ امنیت و محرمانگی تعدادی از جنبه‌های امنیت اطلاعات و تکنیک‌های مربوطه مانند سیاست‌ها، حریم خصوصی محیط کار، کنترل متمرکز، رمزنگاری و امنیت سطح سیستم عامل را در نظر گرفته‌اند که با موارد به دست آمده در امنیت داده‌های این مطالعه تطابق دارد. طبق نظر سوبرز [۱۰] موثرترین راه‌حل برای اجرای BYOD ترکیب امنیت و فن‌آوری با سیاست‌های مرتبط در یک چارچوب جامع و ایجاد تعادل مابین آن‌ها می‌باشد. به این موضوع در پژوهش حاضر در بخش زیرساخت فنی و به ویژه امنیت داده‌ها اشاره شده است که نشان‌دهنده هم‌سویی نتایج می‌باشد.

الانصاری و همکارانش در مطالعه خود که در ارتباط با چارچوب عوامل موثر در پذیرش سازمانی BYOD است [۲۵] عوامل اصلی را به دو بخش قصد رفتاری استفاده از فن‌آوری و معیارهای خاص سیاسی دسته‌بندی نموده‌اند. در خصوص قصد رفتاری استفاده از فن‌آوری اشاره به مواردی هم چون پشتیبانی مدیریت و پشتیبانی فنی با نتایج مطالعه حاضر هم‌خوانی دارد؛ علاوه بر این در معیارهای خاص سیاستی نیز به انواع مختلفی از سیاست‌های مورد نیاز در خصوص بازپرداخت‌ها، توافقات کارمندان، پشتیبانی از

[13] Brodin M, editor Management of Mobile Devices: How to Implement a New Strategy. The 27th International Business Information Management Association Conference, IBIMA 2016, Milan, Italy, May 4-5, 2016; 2016: International Business Information Management Association (IBIMA).

[14] Marshall S. IT consumerization: A case study of BYOD in a healthcare setting. *Technol Innovat Manag Rev* 2014; 4.

<https://doi.org/10.22215/timreview771>

[15] Weeger A, Wang X, Gewald H, Raisinghani M, Sanchez O, Grant G, et al. Determinants of intention to participate in corporate BYOD-Programs: The case of digital natives. *Inform Syst Front* 2015; 1-17.

<https://doi.org/10.5465/ambpp.2015.11188abstract>

[16] Sharif MH, Datta R, Sankarasetty SN, Garikapati H, Valavala M, Maraboyina S. Bring your own device (BYOD) program. *Int J Engin Appl Sci Technol* 2019; 4: 2143-2455.

[17] Blagden RJ. An implementation strategy for bring your own device in the NHS: an innovation study: imperial college London; 2020.

[18] Shabazi M, Rarani MA, Tahmasebian S, Jahanbakhsh M. BYOD and its application in the healthcare environment applied health information technology. 2020; 1: 60-64.

<https://doi.org/10.18502/ahit.v1i1.5260>

[19] Kaitlin B, Nakia G, Gema H, Naomi L, Jason A, Milissa M, et al. Mobile device security: bring your own device (BYOD). *Nist Spec Public* 2023; 1800: 22.

[20] Jahanbakhsh M, Amini-Rarani M, Tahmasebian S, Shahbazi M. Identifying and ranking the attributes of hospitals readiness to apply bring your own device: An explanatory sequential mixed study. *Proce Singapore Health Care* 2022; 31.

<https://doi.org/10.1177/20101058221144113>

[21] Lincon YS, Guba EG. *Naturalistic inquiry*. Beverly Hills Sage 1985.

[https://doi.org/10.1016/0147-1767\(85\)90062-8](https://doi.org/10.1016/0147-1767(85)90062-8)

[22] Brodin M, Rose J, Ahlfeldt RM, editors. Management issues for bring your own device. European, Mediterranean & Middle Eastern Conference on Information Systems 2015 (EMCIS2015), 1-2 June, Athens, Greece; 2015: European, Mediterranean & Middle Eastern Conference on Information Systems (EMCIS).

[23] Krey M. A framework for the adoption of bring your own device (BYOD) in the hospital environment. *GSTF J Comput (JoC)* 2018; 6.

[24] Zahadat N, Blessner P, Blackburn T, Olson BA. BYOD security engineering: A framework and its analysis. *Comput Secur* 2015; 55: 81-99.

<https://doi.org/10.1016/j.cose.2015.06.011>

[25] Alansari Z, Soomro S, Belgaum MR, Shahabuddin SJAJSR. A new conceptual model for BYOD organizational adoption. 2016; 10: 400-405.

<https://doi.org/10.3923/ajsr.2017.400.405>

[26] Vorakulpipat C, Sirapaisan S, Rattanalerdnusorn E, Savangasuk V. A policy-based framework for preserving confidentiality in BYOD environments: A review of information security perspectives. *Secur Commun Networks* 2017; 2017.

<https://doi.org/10.1155/2017/2057260>

[27] Aguboshim FC, Udobi JI. Security Issues with Mobile IT: A narrative review of bring your own device (BYOD). *Inform Technol* 2019; 8.

[11] Elwess T. Bring your own device (BYOD): Utica College; 2013.

## مشارکت و نقش نویسندگان

به طور کلی همه نویسندگان در ایجاد این مقاله همکاری کردند. جهانبخش و امینی رارانی در ایده‌پردازی، طراحی مقاله، شهبازی در جمع‌آوری داده‌ها و نوشتن نسخه اولیه مقاله، جهانبخش، شهبازی و امینی در تحلیل و تفسیر داده‌های کیفی شرکت داشته‌اند. طهماسبیان در پشتیبانی فنی همکاری داشته است. همه نویسندگان نتایج را بررسی نموده و نسخه نهایی مقاله را تایید نمودند.

## منابع

[1] Moore PY. Factors Influencing the Adoption of Bring Your Own Device Policies in the United States Healthcare Industry: Capella University; 2018.

[2] Wani TA, Mendoza A, Gray K. Hospital bring-your-own-device security challenges and solutions: systematic review of gray literature. *JMIR Mhealth Uhealth* 2020; 8: e18175.

<https://doi.org/10.2196/18175>

PMid:32554388 PMCID:PMC7333072

[3] Singh N. BYOD genie is out of the bottle-"Devil or angel". *J Bus Manag Soc Sci Res* 2012; 1: 1-12.

[4] French AM, Guo C, Shim JP. Current status, Issues, and future of bring your own device (BYOD). *CAIS* 2014; 35: 10.

<https://doi.org/10.17705/1CAIS.03510>

[5] Moyer JE. Managing mobile devices in hospitals: A literature review of BYOD policies and usage. *J Hosp Librarian* 2013; 13: 197-208.

<https://doi.org/10.1080/15323269.2013.798768>

[6] Portela F, da Veiga AM, Santos MF. Benefits of bring your own device in healthcare. *Next-Generation Mobile and Pervasive Healthcare Solutions: IGI global*; 2018; p: 32-45.

<https://doi.org/10.4018/978-1-5225-2851-7.ch003>

[7] Weeger A, Wang X, Gewald H. IT consumerization: BYOD-program acceptance and its impact on employer attractiveness. *J Comput Inform Syst* 2016; 56: 1-10.

<https://doi.org/10.1080/08874417.2015.11645795>

[8] Yang A, Vlas R, Yang A, Vlas C, editors. Risk management in the era of BYOD. 2013 International Conference on Social Computing, Alexandria, VA; 2013: Citeseer.

[9] Eslahi M, Naseri MV, Hashim H, Tahir N, Saad EHM, editors. BYOD: Current state and security challenges. *Computer Applications and Industrial Electronics (ISCAIE)*, 2014 IEEE Symposium on; 2014: IEEE.

<https://doi.org/10.1109/ISCAIE.2014.7010235>

[10] Sisala S, Othman S. Developing a mobile device management (MDM) security metamodel for bring your own devices (BYOD) in hospitals. *Internat J Innovat Comput* 2020; 10.

<https://doi.org/10.11113/ijic.v10n2.273>

[12] Sobers A. BYOD and the Mobile Enterprise-Organisational challenges and solutions to adopt BYOD. arXiv preprint arXiv:151203911. 2015.

## Bring your device in the hospital: a qualitative study

Masoumeh Shahbazi (M.Sc)<sup>1</sup>, Mostafa Amini-Rarani (Ph.D)<sup>2</sup>, Maryam Jahanbakhsh (Ph.D)<sup>\*3</sup>, Shahram Tahmasebian (Ph.D)<sup>4</sup>

1- Management and Health Information Technology Department, Isfahan University of Medical Sciences, Isfahan, Iran

2 - Social Determinants of Health Research Center, Isfahan University of Medical Sciences, Isfahan, Iran

3- Health Information Technology Research Center, Isfahan University of Medical Sciences, Isfahan, Iran

4- School of Advanced Technologies, Shahrekord University of Medical Sciences, Shahrekord, Iran

\* Corresponding author. +989133215351 jahanbakhsh.him@gmail.com

Received:11 Mar 2023; Accepted: 13 Jan 2024

**Introduction:** The Bring Your Device (BYOD) approach has promoted the use of personal mobile devices to achieve organizational and occupational goals, but the use of this approach can bring various challenges and risks for health organizations. This research was conducted to identify the components of hospitals' readiness to use BYOD which can be used to develop appropriate policies and ultimately control related challenges.

**Materials and Methods:** In this qualitative study, participants were selected using purposeful sampling with a snowball approach till reaching saturation point. For data gathering, semi-structured interviews were conducted with 15 experts in the BYOD field. Qualitative data were analyzed with the thematic analysis method and using MAXQDA Plus version 12 (Release 12.3.0, VERBI GmbH Berlin).

**Results:** 6 main themes and 23 sub-themes were identified. The main themes include management principles, human resources, cost, technical infrastructure, legal considerations, and ethical considerations that play critical roles in hospitals' readiness for BYOD.

**Conclusion:** Focusing on the issues identified in the form of formulating and implementing official programs as well as appropriate policies by the managers and stakeholders of the organizations can properly benefit from the advantages of BYOD and reduce the related challenges as much as possible.

**Keywords:** Information Technology, Health Information Management, Bring-Your-Own-Device (BYOD), Healthcare Organizations