WHITE PAPER

6 Themes Driving Provider IT Investment

New care models, delivery methods, and innovations promise to enhance clinical and financial outcomes — but necessitate complementary focus on security and protection

Executive summary

- The six themes driving provider IT investment are digital transformation and cloud adoption, expanding the Internet of Medical Things, virtual care, care coordination, data sharing and interoperability, and specialty-focused investments

- 95% of healthcare providers plan to make significant investments in technology in 2023 — and beyond — according to a recent joint report from Bain and KLAS Research

- Each of the six themes has associated cybersecurity requirements, including strict regulatory measures and best practices to ensure diligent protection

The COVID-19 pandemic was arguably the most pressing challenge healthcare providers have ever faced, both clinically and financially. The healthcare industry is still struggling with lower patient volumes and lower financial margins, while operational costs continue to rise.

Although COVID-19 was the catalyst for agility and innovation — notably when it comes to virtual care, alternative care models and sites, and automation — there are still myriad hurdles for providers to overcome. Notably, these revolve around organizations' cybersecurity posture, which has not kept up with the pace of change and the increasing sophistication of threat actors. High-profile cyberattacks on providers and hospitals continue to make headlines. The number of breaches reported to the Department of Health and Human Services was at an all-time high in 2021, and tracked at the same rate throughout 2022.

A recent joint report from Bain and KLAS Research, "Healthcare Provider IT Report: Post-Pandemic Investment Priorities," states that among all providers, 95% plan to make significant investments in technology in 2023. It's pivotal for organizations' success that a component of those goals is to integrate — and prioritize — cybersecurity.

The need to think about cybersecurity as a preventive measure, instead of treating it as an afterthought, is crucial. A recent breach at the second-largest nonprofit hospital chain in the United States — one of the many breaches across the world — meant disruption in 21 states, ranging from system shutdowns of the electronic health record and patient appointment scheduling to ambulance diversions. The downstream effect is the loss of millions of dollars due to downtime (or even paying a ransom), the cost to rebuild and reconfigure systems when data is lost, and the loss of patient confidence that will be unquantifiable for years to come.

The takeaways? Although a cybersecurity investment may be difficult to prioritize, it can save organizations millions of dollars in cyber incident cleanup, downtime, and brand repair (Table 1).

Consequences of Cyberattacks	Economic Impact
Data breaches	• Damaged reputation • Loss of trust
Ransomware	• Ransom cost • Operational downtime revenue lost • Subsequent rising costs for cyber insurance (industry-wide) • Patient lives or outcomes at risk due to unavailable data or critical care delivery tools (like robotic surgical devices)
Unauthorized access	• Lost data or works in progress • Rebuilding costs and lost revenue due to operational standstill during rebuild

Table 1: The potential economic impacts of the consequences of cyberattacks

Prioritizing cybersecurity requirements alongside technical investment decisions is the best — and only — way to ensure that you and your patient population are protected from cyberattacks.

There are six themes driving provider IT investment. In the next section, we'll discuss each one and offer best practices you should take to ensure protection against cybersecurity threats.

The six themes in provider IT investments

1. Digital transformation and cloud adoption

The opportunities provided by the migration of core technologies and infrastructure from on-premises to the cloud are vast. Operationally, such innovation decreases the costs to maintain physical infrastructure and the costs associated with the teams performing that maintenance. Providers — who are increasingly regulated to share data across the healthcare continuum — can enhance their data accessibility to enable third-party solutions and potentially improve clinical outcomes by reducing medication interference, for instance. In a landscape that includes merger and acquisition growth, providers can improve scalability of high-bandwidth analytics tools, and ultimately better meet the demands of patients in a consumer-driven ecosystem.

The benefits of digital transformation and cloud adoption for providers include:

- Streamlined collaborative patient care because providers can share data more easily with other providers and with patients themselves — ultimately creating a holistic and longitudinal health record
- Less expensive and more flexible data storage solutions that can be easily scaled
- Lowered costs to manage and maintain infrastructure by outsourcing to cloud service providers
- Enhanced business continuity and/or disaster recovery capabilities

The opportunities provided by the migration of core technologies and infrastructure from on-premises to the cloud are vast.

2. Expanding the Internet of Medical Things

The Internet of Medical Things (IoMT; sometimes referred to as “IoT in healthcare”) allows wireless and remote devices to securely communicate over the internet, yielding rapid and flexible analysis of data. For instance, this can include bedside monitors for inpatient settings, or implanted medical devices for at-home care monitoring. This increasing interconnectedness across the healthcare continuum also includes devices that are more valuable when they can send or receive data that is accessible (or stored) somewhere else. One notable example of this is data that is accessed from a provider’s electronic health record.

The benefits of expanding of the IoMT include:

- Improved patient outcomes and comfort by providing real-time data, trends, and alerts about changes in condition, regardless of care setting
- More robust patient data and vital signs without an in-person visit, which can help physicians make better decisions with more comprehensive information about patient conditions and trends
- More accurate diagnoses more quickly through the availability of more data, which can save lives and reduce costs associated with emergency services and critical care
- Enhanced clinical decision support via tools that speed up triage, improve diagnostics delivery, and facilitate clinic management, which allows physicians to make more informed decisions about treatment, and opens the door to new provider-centric point of care technology solutions

3. Virtual care

Adoption of virtual care — including on-camera modalities (like telehealth) and remote patient monitoring devices — accelerated rapidly during the pandemic. These tools enable clinical care delivery outside of traditional brick and mortar care settings.

- **Telehealth** includes all technologies used to support long-distance healthcare, including any form of treatment without seeing the patient in person
- **Remote** care includes all methods and channels used by providers to interact remotely with patients, including any form of ongoing communication about treatment plans
- **Home care** is typically more cost-effective than ambulatory and episodic in-person care, increasingly considered by providers to treat patients with multiple chronic conditions or functional impairment
- **Electronic prescriptions** include the fulfillment and home delivery of medications and prescriptions

The benefits of expanding the use of virtual care include:

- Increased access for patients who may have transportation issues, like the elderly, and those who live in rural settings
- Operational efficiencies, like reviewing lab results and medications that otherwise would require additional clinical and administrative staff, and supplies, if performed in-person
- E nhanced real-time communication and data collection from patients, reducing time to action, empowering patients to take control of the healthcare journey, and increasing potential medication efficacy
- Reduced costs because preventive care and the care of chronic conditions are delivered outside of a hospital setting

4. Care Coordination

Care coordination involves organizing patient care activities among multiple providers to ensure continuity of care, effective treatment, and a comprehensive care experience. This approach is supported by tools that enable longitudinal health records; communication platforms, like messaging apps and patient portals; and practice management or chronic care management platforms.

The benefits of care coordination for providers include:

- Accessing a holistic record of all previous care the patient has received to provide better overall care and reduce the likelihood of an avoidable (and costly) adverse medical event
- Providing more comprehensive — and, therefore, likely more effective — care with more comprehensive information, especially regarding preventive care
- Accessing the breadth of data necessary to take an evidence-based approach to healthcare and fully utilize analytical tool
- Making sure patients get the best quality of care possible by directly interacting with specialists and other providers across the medical continuum, to debate the merits of different care options and align on the best path forward for the patient
- Aiding in the transition to value-based care by improving diagnostic tools and ensuring patients aren't receiving unnecessary or redundant lab tests, medications, or treatments that increase cost of care

More accurate diagnoses more quickly through the availability of more data, which can save lives and reduce costs associated with emergency services and critical care

5. Data sharing and interoperability

Healthcare data sharing is the timely and secure exchange of information across the healthcare ecosystem and among its players. These players include providers; payers; life science organizations; digital health and healthcare IT solutions; patients; and other third parties, such as reporting agencies and health information exchanges. Interoperability — the integration of electronic health data so that it can be used to optimize health outcomes for individuals and populations — is one of the most crucial components supporting this exchange of information. Data sharing can include diagnostic or treatment information, administrative data, lab and clinical information, and financial and insurance data.

The benefits of data sharing and interoperability include:

- Supporting care coordination by making it easier for providers to access patient health information and reduce redundant testing, preventing inadvertent treatment interactions, and reducing miscommunications
- Improving patient outcomes and cutting costs by helping providers analyze patient records, expedite clinical decision-making, and improve coverage decisions and costs of care
- Making the analysis of data trends easier thanks to aggregated data sets; providers can more easily review past performance outcomes and make data-driven decisions to enhance clinical and financial operations (such as across patient care, office operations, billing, and beyond)
- Improving patient and employee experiences by reducing redundant administrative work

6. Specialty-focused investments

Providers have increasingly invested in technology and digital tools to aid specialty care. These innovations include, but aren't limited to, solutions that target mental and behavioral health, women's health, and emergency medical services.

The benefits of of specialty-focused investments include:

- A reduction in the administrative burden on healthcare systems, and an associated reduction in operating costs
- An improvement in the quality of care for patients
- Triage tools driven by artificial intelligence or machine learning technology that can manage a virtual waiting room, assisting one of the highest-volume departments in a provider organization
- Apps that let providers monitor conditions and associated symptoms (like those of mental health conditions) and reduce the number of hospitalizations
- Digital smoking cessation tools and other innovative behavioral health solutions that can remotely guide patients through a course of treatment, and video/text communication tools that can help providers virtually connect with patients for therapy appointments in a low-cost and non-intrusive way
- Support that encourages the use of digital health tools — including wearables and condition-monitoring tools, AI/machine learning condition management solutions, and digital pregnancy tools — so providers can compete in growing markets and increase patient volume
- A competitive edge in competition to enhance patient volume and loyalty

The need-to-know on cybersecurity for providers

Each cybersecurity-related regulation affects provider investment in different areas of concentration (Table 2).

Relevant Regulations	Area(s) of Concentration
Health Insurance Portability and Accountability Act (HIPAA) — Protects personally identifiable information and protected health information	• Digital transformation and cloud adoption • Expansion of IoMT devices • Virtual care • Care coordination • Data sharing and interoperability • Specialty-focused investments
21st Century Cures Act — Enables patients to have access to their own data	• Digital transformation and cloud adoption • Expansion of IoMT devices • Virtual care • Care coordination • Data sharing and interoperability • Specialty-focused investments
Quality system regulations for medical devices and wearables	• Virtual care

Table 2: The cybersecurity-related regulations that affect provider investment

You can protect your organization with the cybersecurity capabilities that are most important to the six provider investment themes (Table 3).

Relevant Regulations	Area(s) of Concentration
Secure your infrastructure • Harden the outside of your infrastructure with a DDoS mitigation tool • Harden the inside of your infrastructure with a microsegmentation solution	• Digital transformation and cloud adoption • Care coordination • Data sharing and interoperability • Specialty-focused investments

Secure your access
• Zero Trust Network Access
  • Multi-factor authentication to avoid account takeovers
  • Secure web gateway
	• Digital transformation and cloud adoption
	• Expansion of IoMT devices
	• Virtual care
	• Care coordination
	• Data sharing and interoperability
	• Specialty-focused investments

Secure applications and APIs • Secure web applications and APIs to ensure data and analytics outcome integrity	• Digital transformation and cloud adoption • Expansion of IoMT devices • Virtual care • Care coordination • Data sharing and interoperability
Have the resources and expertise to correctly set up and manage cybersecurity solutions	• Digital transformation and cloud adoption • Expansion of IoMT devices • Virtual care • Care coordination • Data sharing and interoperability • Specialty-focused investments

Table 3: The cybersecurity capabilities that are most important to protect provider investment themes

Keep yourself protected

Although this is one of the most dynamic periods for providers when it comes to innovative models and technologies, myriad challenges still persist. Healthcare is one of the most vulnerable industries when it comes to cyberattacks because of the vast number of patient records and system entry points. Providers handle large quantities of patient data, and recent investment trends and solution implementation have accelerated data storage, organization, and analytical tools. However, these tools provide a much larger surface area for threat actors to target provider networks. Operational downtime or restricted access to patient records after an attack means that providers' role in patient safety is no longer restricted to scheduling visits and making a proper care plan.

The best way to stay on top of risks as you invest in transformation is to work with a trusted leader in the healthcare cybersecurity space — from product, expertise, and resource perspectives — to ensure adequate protection against potential cyberthreats amid technology advancements.

Contact Akamai for a deeper dive into which solutions would benefit your organization the most.