Akamai

WHITE PAPER

5 Themes Driving Healthcare Payer IT Investment

New innovations promise to increase efficiencies and reduce costs — but they also require a complementary focus on cybersecurity and protection

Executive summary

- There are five themes driving healthcare payer IT investment: value-based care; merging of payers and providers; data sharing, data integration, and interoperability; enhancing the customer and member experience; and digitization and digital transformation.
- Healthcare payer organizations are prime targets for threat actors because they manage both patient health data and financial data.
- Although executives are aware of the proliferation of threats, cybersecurity is often overlooked, deprioritized, or identified too late, adding significant and unnecessary risk.
- Beyond meeting regulatory requirements, best practices will ensure adequate protection against cybersecurity threats.

The pandemic was a catalyst for payer organizations to make sizable investments in their IT infrastructure. In broad terms, these investments are intended to provide additional value and services to increase member acquisition and retention, reduce costs across the medical continuum, and make healthcare operationally efficient.

However, the cybersecurity needs of new innovations are often overlooked, deprioritized, or identified too late. The organizations wind up with inadequate coverage and protection,

which elevates their risks and vulnerabilities. — A single data breach can cost millions of dollars in federal fines alone, increasing the likelihood of important initiatives coming in significantly over budget. Cybersecurity must be a priority — not an afterthought — and requires shifting budget spend from prevention to real-time detection and resiliency.

Although most payers lack adequate cyber protection, that reality is not lost on many IT leaders. As one security executive who took part in a 2023 study conducted by Porter Research noted, "The amount of money we were spending in 2020 early on around cybersecurity was maybe 5% of our total IT budget. Now it is probably 25% of our budget." Other executives surveyed in the Porter Research study noted a similar upward-trending investment of resources in IT infrastructure enhancements.

Making a proactive investment now is the best way — the only way — to protect your organization and support increased revenue and cost savings in the future. Each consequence of a cyberattack has a potential economic impact (Table 1).

Consequences of Cyberattacks	Economic Impact
Data breaches	• Damaged reputation • Loss of trust
Ransomware	• Ransom cost • Lost revenue from operational downtime • 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 • Costs and lost revenue from operational standstill during rebuild
Rebuilding systems after an attack	• Costs of rebuilding and lost revenue from the subsequent operational standstill
Federal and state regulations	• Increased payer liability for compromised member records

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

The five themes in payer investments

There are five themes driving payer technology investments. In the next section, we'll discuss each one and offer best practices to ensure adequate protection against cybersecurity threats.

1. Value-based care

Value-based care is a healthcare strategy focused on improving outcomes. It shifts away from traditional frameworks of the episodic treatment of illnesses, and instead offers reimbursement incentives that encourage preventive care.

More specifically, payers offer a fixed rate of reimbursement per patient. The expectation is that the rate aligns incentives for providers to increase proactive care and reduce overall costs.

To help determine the best reimbursement rates for provider network agreements, payers use technology solutions that help quantify risk among various patient populations and maximize the opportunities for preventive measures at the point of care.

The benefits of value-based care for payers include:

- Predictable reimbursement and revenue levels, regardless of the total cost of care
- Lower administrative costs per patient due to bundled payments that reimburse providers for total care — rather than individually per treatment
- Healthier and happier members, leading to increased retention and renewals — along with decreased churn among both individuals and employers

2. Merging of payers and providers

The volume of mergers between payers and providers (often called "payviders") continues to increase at a rapid pace. Recent examples include Aetna–CVS and Humana–Kindred at Home.

When consolidating, organizations need to address a number of technical considerations, including capability gaps, overlap, and duplication. They also need to think about personnel training and any necessary adjustments to policies and procedures — all of which can directly impact cybersecurity risks.

It's notable that payers are also hiring and building provider capabilities organically as well, such as UnitedHealth's Optum acquisition of physician groups Atrius Health and Beaver Medical Group to increase its lead as the largest employer of physicians in the U.S. Similarly, some providers, like Kaiser Permanente and Geisinger, also offer insurance plans.

The benefits of merging payers and providers include:

- Accelerated transition to value-based care by aligning incentives across the healthcare continuum
- Easy data sharing allows for more collaborative, holistic care and lower payer costs per patient
- The opportunity for payers to be more consumer-centric instead of provider-centric
- Reduced medical expenses and operating expenses for payers (minus offsets from adding provider expenses into the equation)
- Access to more complete, real-time patient data for analytics and diagnostic tools

> "The amount of money we were spending in 2020 early on around cybersecurity was maybe 5% of our total IT budget. Now it is probably 25% of our budget."
>
> — Healthcare security executive surveyed by Porter Research, 2023

3. Data sharing, data integration, and interoperability

Healthcare data sharing is the bidirectional exchange of information through point-to-point integrations. Data is shared – often facilitated by APIs – between providers, payers, employers, patients, and other third parties, like electronic health records, vendors, and health information exchanges.

Provider information can be aggregated to facilitate payer operations and include category options like network agreements and contracts, credentialing data, patient population statistics, and referral and order volumes.

Clinical and patient data can also be shared to make workflows more efficient. This includes anything related to a patient's medical records, prescriptions, demographics, social determinants, and other clinical services. Administrative data, like eligibility requests, prior authorizations, claims and payment data, and accumulator values, are also easily shared among entities.

Data sharing, data integration, and interoperability benefits for payers include:

- Increased administrative efficiency for a wide array of payer-driven care interventions, allowing payers to easily inform providers which treatments are covered, or to directly intervene to decrease costs
- Improved patient outcomes and lower costs by expediting and enhancing clinical decision-making, such as when duplicate orders and labs are removed across disparate teams and systems
- Enhanced interoperability and data exchange across back-end systems to help manage an increasingly complex healthcare ecosystem — one in which patients are likely to receive care from a variety of healthcare sources (as mandated by the 21st Century Cures Act)
- Increased in-network referrals for low-cost, high-value ancillary and specialty services

4. Enhancing the customer and member experience

With the growing competitiveness of the payer market, increased member engagement is seen as a powerful way to elevate member retention and growth. That's why many organizations are leveraging technology solutions to enhance member satisfaction and engagement.

Consumers demand digital products that are personalized, easy to use, and offer quick access to the tools and information they need. Payers who overlook this demand are likely to see a drop in member retention and acquisition rates.

It's also worth noting how complicated U.S. health insurance can be for patients. Payers who develop educational tools that help members understand their situation and options are likely to deliver more value.

The benefits of enhancing the customer and member experience include:

- Reduced barriers for payers to interact with employers and patients through online portals, chat support, and other asynchronous communication
- Enhanced digital front doors that boost the member experience, resulting in higher retention rates
- Improved member case management to help payers offer more education and guidance about preventive care
- Increased patient satisfaction and retention by modernizing digital interfaces to take advantage of online transaction habits

5. Digitization and digital transformation

Payers recognize the need to modernize their services and member engagement opportunities. In recent years, they've increased their value to members through a substantial rise in the adoption of technologies that digitize historically nondigital services and operations.

The purpose of these investments goes far beyond boosting the member experience. They lower operational costs by making processes more efficient, while also offering unique opportunities for customization and scalability. A prime example is the transition from on-premises solutions to cloud-based software.

The benefits of digitization and digital transformation include:

- Improved cost, quality, and convenience of member services, making it easier to attract new customers
- Digitized payment solutions attract customers who are accustomed to online transactions, price transparency, education, and payment understanding; without these, customers often struggle to understand their options and go elsewhere
- Customized interactions with members by developing tools internally (as opposed to using third-party solutions)
- Migration of key technologies to the cloud, which decreases the costs associated with maintenance and support while increasing scalability

The need-to-know on cybersecurity for payers

Each cybersecurity-related regulation affects payer investments 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	• Value-based care • Merging of payers and providers • Data sharing, data integration, and interoperability • Enhancing the customer and member experience • Digitization and digital transformation
21st Century Cures Act — Enables patients to have access to their own data	• Value-based care • Merging of payers and providers • Data sharing, data integration, and interoperability • Enhancing the customer and member experience • Digitization and digital transformation
State legislation rewarding healthcare providers with incentive payments for the quality of care they give to Medicare populations	• Value-based care

Table 2: The cybersecurity-related regulations that affect payer investments

You can protect your organization with the cybersecurity capabilities that are most important to the five payer 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	• Value-based care • Merging of payers and providers • Enhancing the customer and member experience • Digitization and digital transformation

Secure your access
• Zero Trust Network Access
  • Multi-factor authentication to avoid account takeovers
  • Secure web gateway
	• Value-based care
	• Merging of payers and providers
	• Data sharing, data integration, and interoperability
	• Enhancing the customer and member experience
	• Digitization and digital transformation

Secure your applications and APIs • Secure web applications and APIs to ensure data and analytics outcome integrity	• Value-based care • Merging of payers and providers • Data sharing, data integration, and interoperability • Enhancing the customer and member experience • Digitization and digital transformation
Have the resources and expertise to correctly set up and manage cybersecurity solutions	• Value-based care • Merging of payers and providers • Data sharing, data integration, and interoperability • Enhancing the customer and member experience • Digitization and digital transformation

Table 3: The most important capabilities for protecting against cyberattacks

Keep yourself — and your members — protected

With all of the dynamic innovation across the payer industry, there are impactful challenges. Because payers handle both financial and healthcare information — two of the most valuable data sources for cybercriminals — they are prime targets for cyberattacks. Protecting member information is crucial.

As the chief medical officer at one national health plan shared with Porter Research, "[Payers] need to hire experts who can help with these attacks. We need to hire the most qualified people who can help prevent the attack. That's really the answer."

Make sure you are working with a trusted leader in the healthcare cybersecurity space. Find a partner, like Akamai, that has the deep expertise and product knowledge to make sure you have superior protection against threat actors who are targeting your technology investments.

> **"[Payers] need to hire experts who can help with these attacks. We need to hire the most qualified people who can help prevent the attack. That's really the answer."**
>
> **— Chief Medical Officer for a U.S. Payer Organization surveyed by Porter Research, 2023**

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