# Healthcare Technology Trends for 2026 and Beyond

# An Evolving Healthcare Landscape

Healthcare is an industry that has balanced technological innovation at the bleeding edge with an evidence-based approach to clinical technology implementation. As a result, certain technology advancements may take years to be implemented into practice as they're put through rigorous testing and clinical trials.

Even for non-clinical use cases, healthcare systems have often been slower than other industries to adopt new technologies in order to enhance patient experience and operational efficiencies. But that paradigm is changing. Between a historic labor shortage, declining reimbursement rates, the increasing consumerization of healthcare, and a new raft of emerging cybersecurity threats, the pace of technology adoption in healthcare is rapidly accelerating.

In this report, we'll unpack how technology leaders in the healthcare space are rolling out initiatives across functions:

**Patient experience**
Discover how evolving patient expectations are driving healthcare providers to embrace digital solutions, enhancing care and connectivity for a seamless patient journey.

**Data, interoperability, and analytics**
Learn about the transformative power of data analytics and AI, how new standards are affecting interoperability, and why hybrid cloud and edge matter for real-time workflows.

**AI in healthcare**
Explore how ambient documentation, clinical support, workflow automation, and emerging AI agents are reshaping care delivery and operations.

**The Internet of Things**
Uncover how IoT technologies are enabling smarter operations and workflow optimizations, providing actionable insights and improving patient care both in hospitals and at home.

**Cybersecurity**
Understand the critical importance of robust cybersecurity measures to help protect sensitive patient data amidst an increasingly digital and interconnected healthcare landscape.

Let's dive into the technological innovations reshaping healthcare, highlighting the opportunities and challenges that lie ahead in this rapidly evolving landscape.
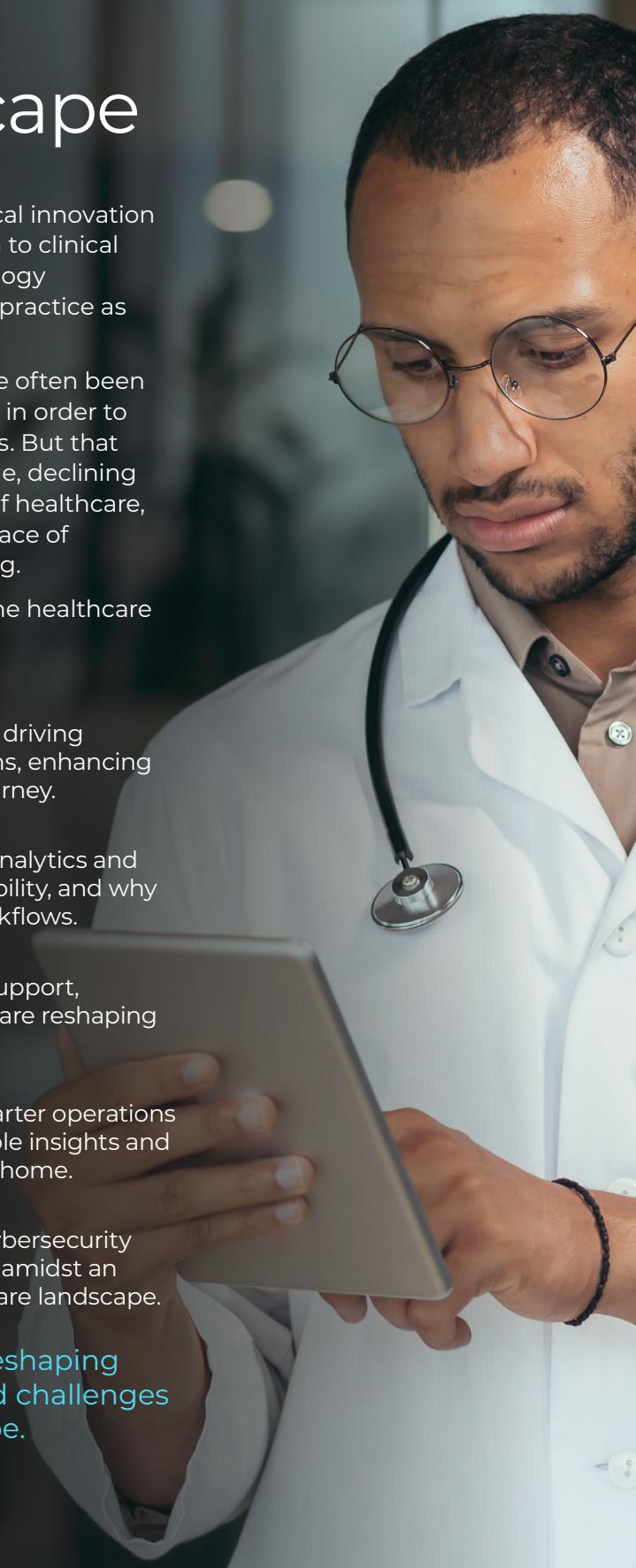
# AI Becomes Healthcare's Co-Pilot

One of the most disruptive forces in healthcare today is the rise of artificial intelligence (AI) in both patient care and operations. No longer limited to back-end research projects, AI is now being embedded in daily workflows to assist clinicians and automate routine tasks. In fact, the vast majority of health leaders trust AI technologies (88% in one recent survey from EY),[1] yet they recognize that responsible AI practices and guardrails are critical as these tools move from experimentation into real-world use.

## AI Agents and Ambient Clinical Intelligence

Clinicians and staff are increasingly supported by AI agents and ambient intelligence that help reduce administrative burdens and improve care delivery. For example, ambient clinical documentation tools[2] can listen to doctor-patient conversations and automatically generate medical notes, prescriptions, and referrals, allowing physicians and nurses to focus on the conversation in the room and providing high-value care.

AI is also proving its value in diagnostic workflows. Machine learning models can rapidly analyze medical images (radiology scans, pathology slides) and flag subtle anomalies that a human might miss. These diagnostic assistants don't replace clinicians, but they provide a second set of eyes, improving accuracy and speeding up critical diagnoses.

On the patient-facing side, agentic AI is being leveraged to autonomously assist patients with tasks like triage, appointment scheduling, or medication refills. For example, hospitals are piloting AI-driven symptom checkers that guide patients to the right level of care (televisit vs. ER) based on their inputs. Consumers are becoming more comfortable interacting with AI for basic health needs, with 39% of younger adults reporting being okay with using generative AI tools to evaluate symptoms.[3]

These AI assistants have potential to offload call centers and front desks by handling routine inquiries, only escalating to humans when needed. Health systems deploying such agentic AI are treading carefully, however. They are implementing guardrails, like requiring human review for certain decisions or maintaining human-in-the-loop oversight, to promote transparency, safety, and patient trust as these agents take on greater roles.

## 88%
of health leaders trust AI technologies based on a recent EY study.[1]

## 39%
of young adults approve of generative AI tools to evaluate symptoms.[3]

[1] EY, EY US identifies eight health trends for 2026: transforming operations, talent and finance
[2] Peterson Healthcare Technology Institute, Adoption of Artificial Intelligence in Healthcare Delivery Systems: Early Applications and Impacts
[3] Forrester, Predictions 2026: The Year AI Tests The Heart Of Healthcare

## From General to Domain-Specific Models

In healthcare, generative AI is being applied in targeted ways: generating realistic synthetic data to train algorithms in an effort to protect patient privacy, accelerate drug discovery by suggesting new molecular designs, improve medical imaging quality through AI-driven image enhancement, and even draft patient outreach communications.

But given those highly specific and specialized use cases, generative AI in healthcare is shifting from one-size-fits-all models to domain-specific language models (DSLMs) tailored for medicine.[4] Unlike general AI models trained on internet data, DSLMs are trained on healthcare-specific datasets and terminology, giving them a deeper understanding of clinical context and yielding more relevant, accurate results. These models, paired with rigorous validation, are boosting confidence in the reliability of AI among a physician population that is already rapidly warming to the idea.[5] Hospital leaders, meanwhile, are looking at their investments accordingly. Gartner predicts that by 2028, over half of the generative models used by enterprise organizations will be domain-specific.[6]

Generative AI in healthcare is shifting from one-size-fits-all models to domain-specific language models (DSLMs) tailored for medicine.[4]

# 2 of 3

physicians are already using some form of health AI.[5]

[4] TechTarget, Generative AI models like DSLMs outperform LLMs in value
[5] American Medical Association, 2 in 3 physicians are using health AI—up 78% from 2023
[6] Gartner, Gartner Identifies the Top Strategic Technology Trends for 2026

# Interoperability and Edge Computing Turn Data into Intelligence

Healthcare providers sit on vast stores of data: clinical data, patient profiles, operational information, Internet of Things (IoT) data, and much more. Given the walled garden nature of electronic health record (EHR) systems, a myriad of legacy systems and databases still in use, as well as the stringent data protections in place regulating the healthcare industry, hospitals and healthcare systems have been traditionally unable to put that data to its highest use.

But when consolidated and leveraged, that data holds tremendous power. It can be used to enhance diagnoses, predict health risks, recommend optimal treatment paths, and drive operational efficiencies. By leveraging advanced data analytics and artificial intelligence, healthcare providers can unlock valuable insights from the immense volumes of patient information they collect. Capitalizing on these opportunities, however, requires networking and data processing strategies and solutions that can handle the intense data demands.

## From Siloed Systems to Real-Time Data Liquidity

Regulatory initiatives like the FHIR® (Fast Healthcare Interoperability Resources) standard and the U.S. TEFCA framework[7] are paving the way for seamless and secure health information exchange across disparate systems. In 2026, compliance with these standards is becoming table stakes: electronic records and devices need to plug into a larger ecosystem where data flows to wherever it's needed. The payoff is better care coordination and analytics. Achieving this means replacing yesterday's fragmented IT systems with connected platforms that speak a common data language.

## Unleashing the Power of Data Analytics

Data analytics offers a lens into the complexities of healthcare, from patient diagnostics to operational efficiencies. The adoption of AI and machine learning technologies is propelling this forward, enabling providers to parse through vast datasets to uncover insights that drive better care decisions and predict health trends. However, the foundation of these technologies' effectiveness lies in their ability to access and analyze comprehensive, relevant and accurate data in real-time, which is only possible through the secure and rapid flow of information among applications and departments. Advanced networking has emerged as a key tool to enable rich analytics, allowing, for example, application-aware network traffic to ensure that analytics applications and AI inference workloads can be accessed optimally, without interrupting other critical healthcare services.

## Harnessing Hybrid Cloud and Edge Computing in Healthcare

To make use of the deluge of data and support AI and analytics everywhere, leading healthcare organizations are adopting hybrid cloud architectures that leverage edge computing, deploying compute resources on-site or closer to the source of data. This allows critical applications to run with ultra-low latency even if the connection to the cloud slows. For instance, an AI-powered cardiac monitor might be able to analyze rhythms and alert doctors to arrhythmias in milliseconds locally, rather than waiting seconds for round-trip cloud analysis. In an emergency, those milliseconds matter.

Edge computing goes hand-in-hand with the cloud. Hybrid models let healthcare IT decide what runs locally versus in a central cloud. Large-scale analytics, population health insights, or machine learning training can happen in cloud data centers where massive compute power is available. Meanwhile, time-sensitive functions reside at the edge, on-site. This best of both worlds allows a hospital network to keep its enterprise data lake and AI model training in a public cloud, but run each facility's medical device controllers, nurse communication apps, and emergency alert systems on local edge servers for speed and resiliency.

## Enabling Interoperability at Scale

FHIR® and TEFCA[7] are setting the foundation for secure, seamless health data exchange across fragmented systems.
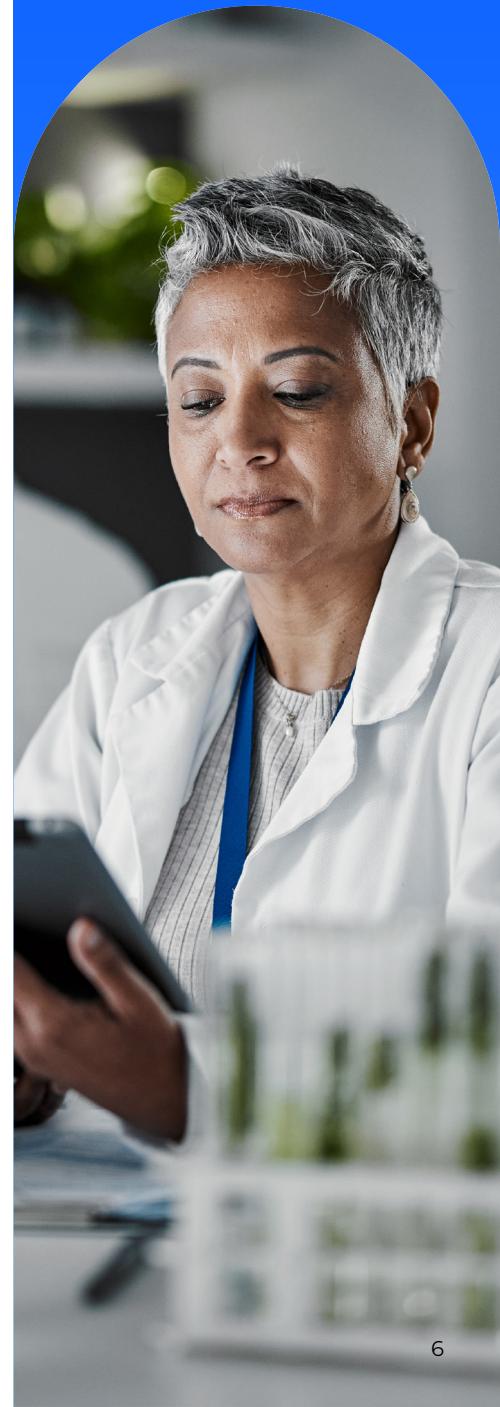
# IoT for Smarter Operations

Healthcare leaders are increasingly turning to The Internet of Things (IoT) as both a source of data and actionable insights—as well as a means to put those insights to bear in real-time. From tracking equipment and managing inventory to monitoring environments and streamlining workflow, IoT technologies are helping providers achieve new levels of operational efficiency.

## Device Insights Inside (and Outside) the Hospital

IoT devices are quickly becoming ubiquitous in every healthcare environment. Within hospital facilities, IoT sensors can monitor temperature, humidity, air quality and other environmental factors to ensure optimal conditions for patient care and staff safety and comfort. Connected biomedical devices—leveraged in the hospital or in Hospital-at-home settings—can automatically upload data to patient records. RFID asset tracking tags allow real-time location monitoring of critical medical equipment to avoid misplacement.

Meanwhile, IoT can enable smarter inventory management by providing real-time supply chain visibility. RFID and IoT sensors can automatically detect low stock levels for medications, supplies, and equipment, triggering restocking alerts to avoid outages. This level of operational intelligence helps reduce waste, cut costs, and ensure critical resources are always available.

For healthcare's mobile workforce, IoT wearables help track staff locations and activity levels to optimize scheduling and ensure enough resources are deployed to meet patient needs across a facility. IoT environmental sensors in ambulances can monitor factors like temperature control of medication storage.

Edge computing, 5G, WiFi, and software-defined networking all play a role in this smart, connected healthcare operations environment. Robust cybersecurity is also paramount to help protect this proliferation of IoT devices and data streams from threats.
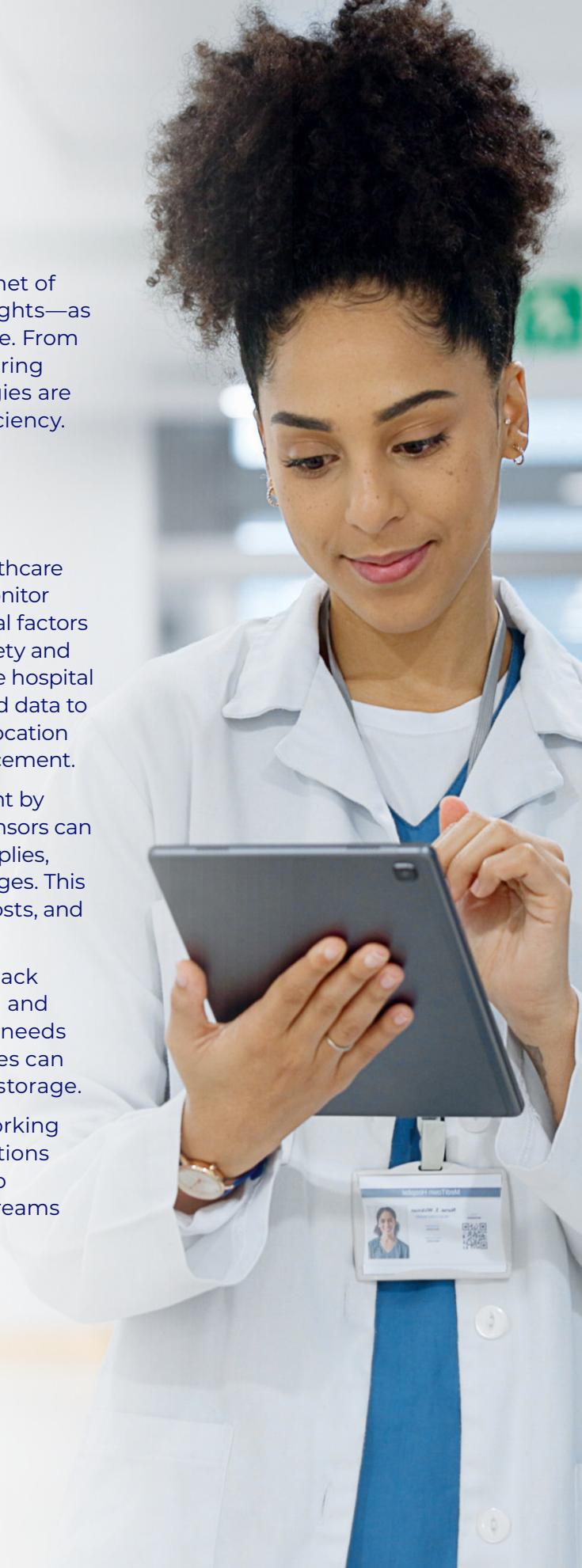
# Cybersecurity in an AI- and Data-Driven World

Unfortunately, healthcare organizations have become an attractive target for bad actors.

Electronic health records, connected IoT medical devices, telehealth solutions, and other new data streams all contain valuable data for would-be attackers, and they are all exponentially expanding healthcare's attack surface area. At the same time, strict data privacy regulations like HIPAA are being enforced with significant noncompliance penalties. Investing in robust cybersecurity has shifted from an IT priority to an overarching clinical and operational imperative. Generative AI and ease of access on the dark web have made more sophisticated attacks readily available for attackers. And finally, the rise in the use of agentic AI means technology leaders need to grapple with an ever-increasing volume on non-human identities accessing systems and networks.

Healthcare breaches cost more than any other industry, averaging around $7.4 million per incident.[8] And 72% of health executives experienced moderate to severe financial impacts from cyber incidents.[9]

## Zero Trust and Identity-Aware Defense

In 2026, healthcare cybersecurity needs to integrate zero-trust architectures and identity-aware defenses. In a zero-trust model, every user, device, application, or data flow is treated as untrusted by default. Instead, continuous verification is required. By verifying identities and contexts for every access request, healthcare organizations can contain breaches before they spread.

Identity and access management (IAM) is a huge focus area here, implementing strict controls so that staff only access the minimum necessary information, and continuously monitoring for anomalous behavior. This identity-centric approach also extends to the emerging world of AI agents: as hospitals deploy more bots and automated scripts, they too must be assigned identities and permissions and watched to ensure they operate within bounds.

Defense-in-depth remains key. Multi-layered cybersecurity frameworks combine network-level protections (firewalls, intrusion detection systems) with endpoint security on devices, encryption of data at rest and in transit, and advanced threat intelligence. Many healthcare organizations extend their in-house teams through managed security services and round-the-clock monitoring (e.g. 24/7 Security Operations Centers or managed detection and response services) to augment their stretched IT teams. They are also leveraging SASE (Secure Access Service Edge) architectures that merge networking and security functions. For healthcare systems that might have hundreds of sites and thousands of remote endpoints, this multi-layered approach can simplify and standardize protections.

## $7.4 M

The average cost of a healthcare data breach.[8]

## 72%

of health executives report moderate to severe impacts from cybersecurity incidents.[9]

COMCAST
BUSINESS

[8] IBM, Cost of a Data Breach Report 2025
[9] EY, EY US identifies eight health trends for 2026: transforming operations, talent and finance

8
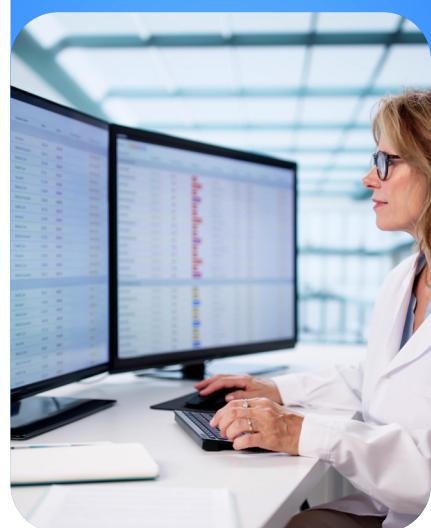
# Experience Remains Paramount

Amid all these technology trends—AI, data interoperability, IoT, and security—one theme remains paramount: patient and caregiver experience is the ultimate benchmark of success. The visible output of intelligent systems and connected infrastructure is a smoother, more personalized healthcare journey that better engages patients—improving outcomes in the process[10]—and better empowers clinicians.

Throughout this report, we've touched on experience improvements: AI freeing doctors to spend more time listening to patients, IoT making hospital stays more comfortable, data flowing seamlessly so patients don't have to lug records from doctor to doctor, and strong security to help enable patients' trust. It all culminates in a healthcare model that is patient-centric and experience-driven by design.

Beyond the hospital walls, the focus on experience means meeting patients where they are. Advances in telehealth, remote monitoring, and AI-driven digital front doors aim to remove friction from healthcare interactions. Patients can get care on their terms, whether that's a video visit from their living room, a quick text follow-up from their doctor, or an AI health coach nudging them with personalized wellness tips. When tech is orchestrated correctly, the experience feels connected and continuous: a patient could schedule an appointment online, have a virtual pre-visit with an AI intake assistant, get lab work done at a local pharmacy, and only come to the clinic if absolutely necessary.

# Envisioning Healthcare's Tech-enabled Future

As healthcare organizations navigate an evolving landscape, the integration of advanced technologies and robust cybersecurity measures will be paramount in delivering care that is not only effective and personalized but also secure and resilient. Looking ahead, healthcare leaders have myriad opportunities to redefine patient care and operational excellence. The key to unlocking this potential lies in harnessing the power of digital innovation, ensuring that technology serves as a bridge to the future of healthcare, where care is personalized, every endpoint is secured, and every process is optimized.

Learn more about how Comcast Business is powering elevated, reliable, and connected healthcare experiences.

**Learn more**

## COMCAST BUSINESS