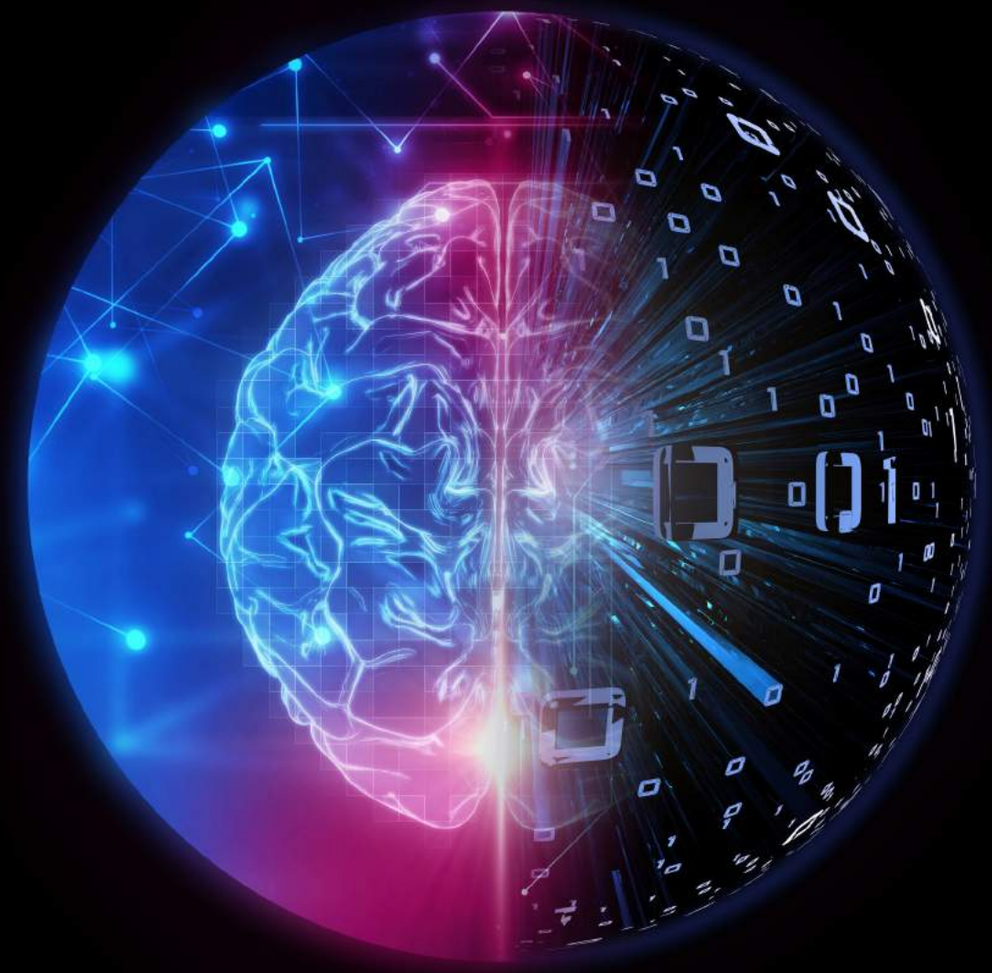
Deloitte.

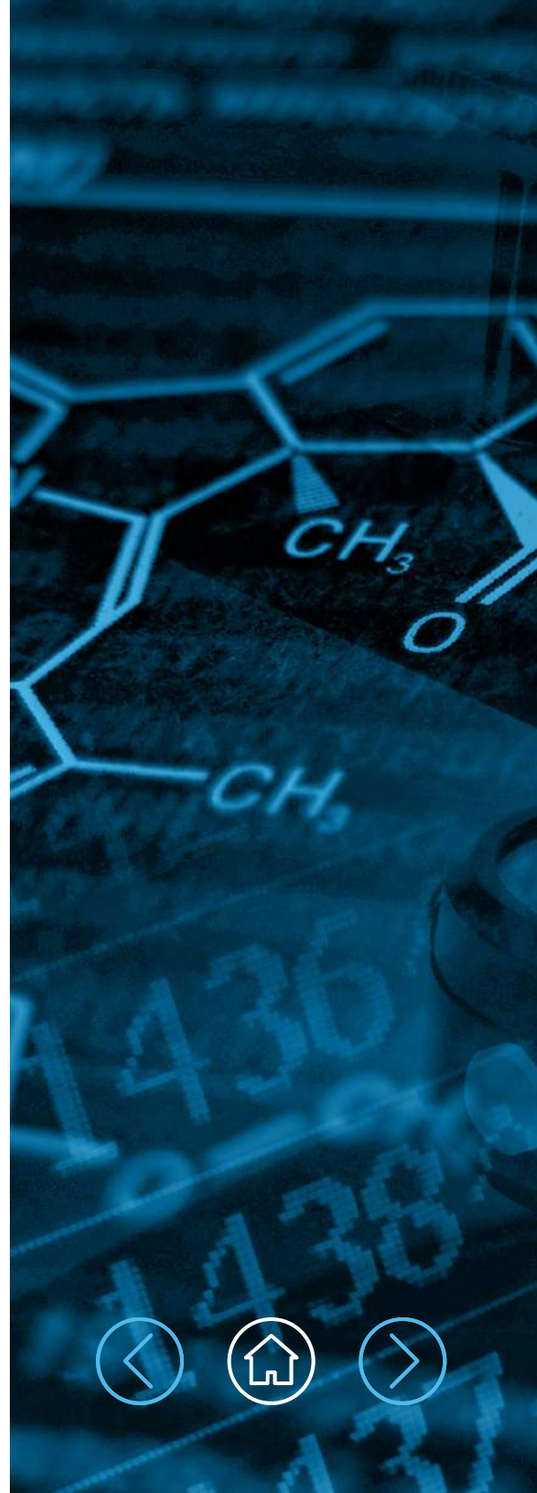


Securing the promise of virtual health care

Addressing cyber risk in a new era of medicine

GET STARTED

Contents



Introduction

It took years for people to become comfortable buying things online. First, the technology had to make it secure. Then, people had to reach a level of comfort and confidence in that new level of security.

A similar process is unfolding today in health care, where an array of virtual technologies offers the potential to bring more care to more people in more places at less cost. If you worry about who might intercept your credit card number, what about your health records, or your genome?

Virtual health—some people use the term "telemedicine"—is the use of digital technologies to provide patient-physician interaction, deliver care, and facilitate other services without traveling in person to a care site. It's a topic we've discussed before, from the patient perspective, the physician's point of view, and where they come together. Yet because the issue hinges on data sharing, it's important to build an approach to address the cyber risk aspects of it as well.

Executive summary

The health care industry continues to seek new advantages in addressing the "triple aim" of access, quality, and cost. Because virtual health may offer advantages in each of these areas, and because people are increasingly oriented toward the daily use of digital tools, it's starting to gain in popularity. A recent Deloitte survey found almost a quarter of responding patient-consumers (23 percent) have tried it already. And among those who hadn't, more than half (57 percent) were willing to try.[1]

But another Deloitte survey, this one of physicians, found less enthusiasm for virtual health. One-third of respondents cited the security and privacy of patient information as one of their chief concerns.[2]

Like many connections, virtual health requires participation at both ends. To address doctors' unease and clear the way for greater adoption, organizations will need to execute a cyber strategy that mitigates these risks. Then—just as with online commerce a generation earlier—organizations will need to follow up on the technical achievement with communication that helps both physicians and patients approach this new form of health care delivery with confidence.

As virtual health increases in capability and popularity, health care organizations will need to continue investing in security services to identify risks and keep them at bay.

THE FIVE KEY AREAS TO ADDRESS INCLUDE:

- Medical devices and wearables security
- Identity management and external device authentication
- Security monitoring and behavioral analysis
- Development, security, and operations (DevSecOps)
- Security training and awareness

[1] Ken Abrams, MD, Steve Burrill, and Natasha Elsner, "What can health systems do to encourage physicians to embrace virtual care? Deloitte 2018 Survey of US Physicians," A report by the Center for Health Solutions, Deloitte Insights, July 18, 2018.

[2] "How do health care consumers and physicians perceive virtual care?" (infographic), Deloitte Insights, June 14, 2018.

The landscape of cyber risk

When you add up the points at which an unauthorized user can take data from or otherwise affect a digital environment, the sum of those exposures is the system's "attack surface." For the system owner and those who rely on it, the smaller the better.

Yet because virtual health introduces new tools that share information across more locations, it risks adding to the overall "attack surface" of health care in general. Virtual health adds to this risk exposure in key areas of cyber risk, such as:

- Technology failures
- Lack of informed consent
- Complex identity and access management
- Increased compliance requirements
- Physical security risks
- Legacy IT infrastructure
- Unpatched software in consumer environments
- Increased third-party risks

By addressing the five key areas identified in the right-hand column, provider organizations can bring more consumers and providers into a comfort zone with virtual health. When the actual security is strong, and the perception of it matches that reality, patients and providers alike will be more likely to take part in virtual health and fuel its growth.

HIGH STAKES, HARD QUESTIONS

- How can organizations maintain the integrity of data as wearables add to the flow of information?
- How should organizations balance the need for monitoring with security and privacy?
- What's the most appropriate way to balance thoroughness and privacy with each type of patient-specific information, ranging from clinical events and consent to scheduling and location?
- How can organizations maintain privacy while meeting patient demands for convenience and strong user experiences?
- What kinds of awareness programs are most effective at helping individuals stay connected and vigilant about protecting their data?

The landscape of cyber risk (cont.)

Medical devices and wearables security

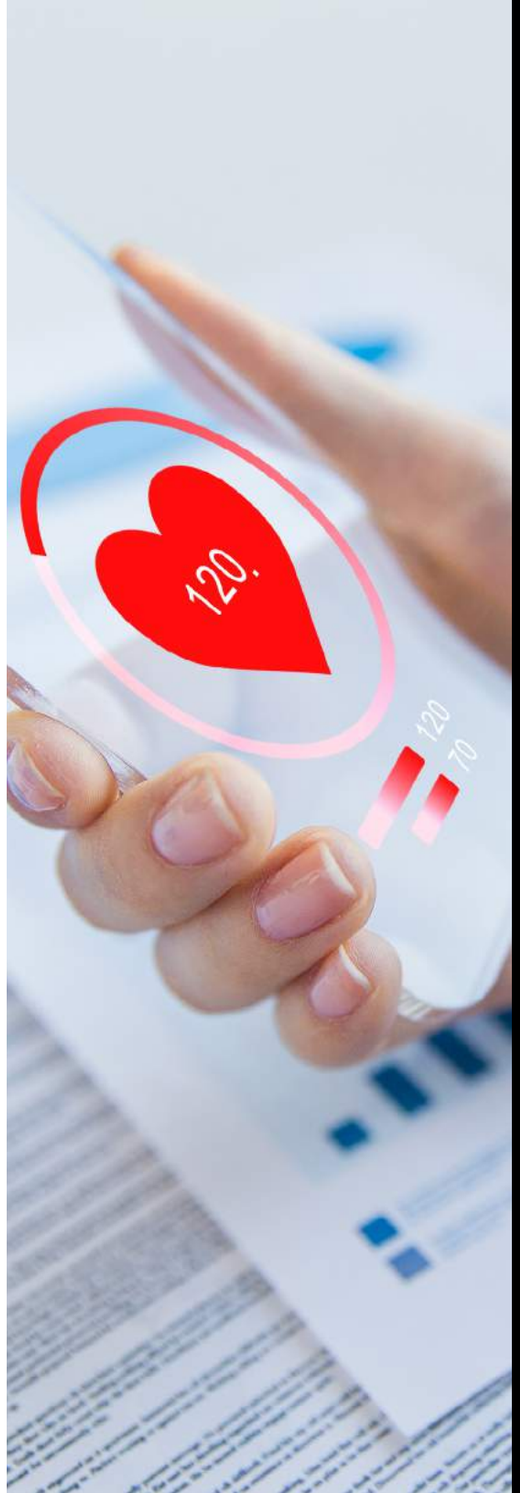
According to the MedTech Impact on Wellness symposium, the wearable tech market is expected to more than double, from $6 billion in 2017 to $14 billion in 2022.[3] And the Deloitte Center for Health Solutions survey conducted from February to March 2018 found that half of consumers are already using technology to track their health information and share that information with their doctors.[4]

Connected devices present security concerns by their very nature. Much of the data they generate is classifiable as protected health information (PHI), and the use of that data involves entrusting it to the cloud. As consumers increase their use of connected health devices, and as provider organizations use them more, the risk to patient health data grows accordingly.

For example, devices that send diagnostics back to providers need safeguards that protect the confidentiality and integrity of that data as it arrives and becomes part of a patient's confidential record. Users should be able to rescind participation and potentially delete their data—in some cases as a courtesy, in some as required by law. If a patient sends pictures or other data to a physician as part of a virtual session or monitoring program, it's important to develop strategies for complying with and addressing the requirements of the Health Insurance Portability and Accountability Act (HIPAA).

[3] Wearable Tech Market Set for Significant Growth, MedTech Impact on Wellness, February 12, 2018.

[4] Ken Abrams, MD, and Casey Korba, "Consumers are on board with virtual health options: Can the health care system deliver?" Deloitte Insights, August 29, 2018, based on the Deloitte 2018 Survey of US Health Care Consumers and Physicians.



The landscape of cyber risk (cont.)

Identity management and external device authentication

When delivering virtual health, how can a health care professional be certain the people on the other end of the line are really who they say they are? Multifactor authentication (MFA) is the leading way for providers to confirm patient identity over digital channels. Some providers supplement MFA with biometrics (touch or facial recognition in a mobile application), short message service (SMS) texts, or device fingerprinting. For patients, an additional benefit of MFA is that it can remove the need for a password as part of using virtual health.

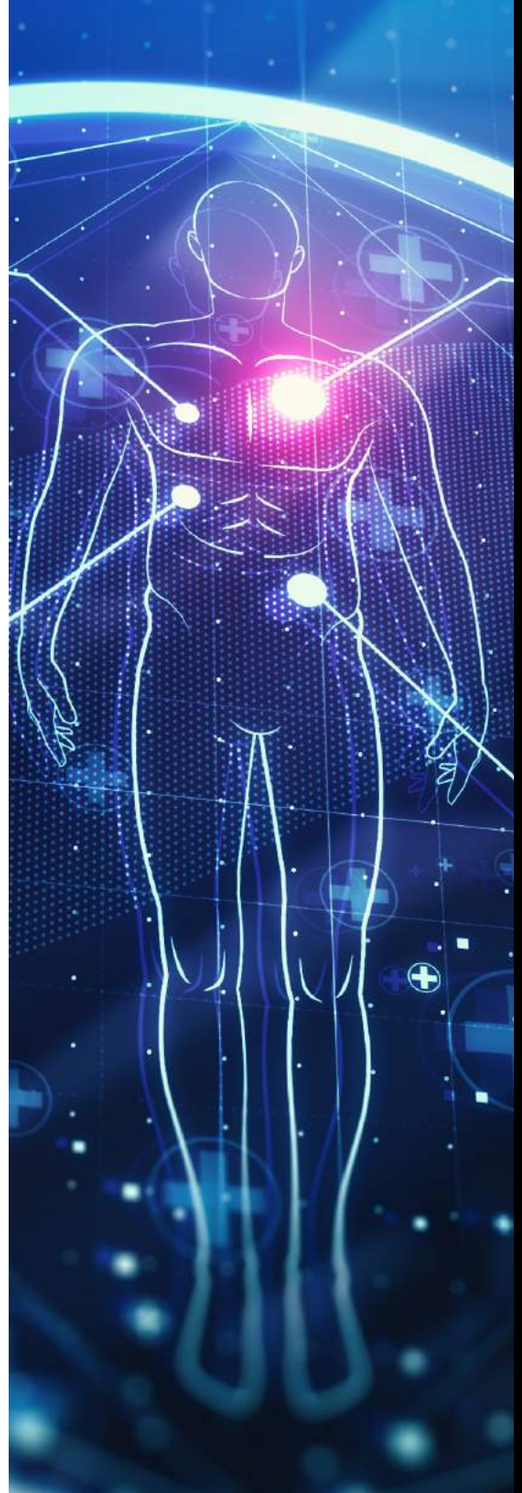
Many providers are also attaching contextual information about each patient to their electronic medical records or customer relationship management records as a way to improve patient profiling. Contextual information might include metrics from wearables, parental consent for minor patients, or just information about a patient's habits in using the system. Understanding when and why a patient enters the ecosystem in search of services can help inform enriched analytics on that patient, and the resulting insights can suggest services that can improve the patient experience. Making this work relies on an identity management system that's flexible enough to send identity data about a patient to multiple systems, and that means the security concerns are multiplied as well.

The landscape of cyber risk (cont.)

Security monitoring and behavioral analysis

For many applications of virtual health, the most common location for receiving services is at home. But in some cases, patients will request these services from other locations. Organizations that provide services in “virtual space” still need to monitor where in the real world their patients are receiving those services. They may take a lesson from credit card companies, which often allow users to set rules for the acceptance of out-of-region purchases.

The balancing point is to watch out for location-based cues that may signal a cyber threat while at the same time offering patients an experience that remains consistent wherever they are. Some vacationers don’t like to juggle extra security steps when they use credit cards far from home. In the same spirit, patients shouldn’t have to jump through additional authentication hoops simply because they’re away from home. The solution is to define “ordinary” and to trigger extra authentication only when a contact (virtual visit) exceeds those settings.



The landscape of cyber risk (cont.)

Development, security, and operations (DevSecOps)

Virtual health integrates patient services and security with a provider organization's business processes and applications. With so many bespoke factors, software in this ecosystem may in many cases require custom development. The development practice of building security controls and processes from the beginning, instead of treating security as a separate layer at the end of development, is known as DevSecOps. It's an approach that's increasingly central to protecting the confidentiality of data.

Many providers use Agile development to speed the deployment of user experiences that can handle fast-paced patient feedback on mobile applications. Using DevSecOps to build security into the development life cycle should be part of this process, whether a health care organization manages development internally or outsources it to a third party.

DevSecOps can elevate development costs. The business case for making that investment is that it may cost the organization less than cleaning up after a problem has been discovered—not to mention the reputational cost of losing patients' trust.

The landscape of cyber risk (cont.)

Security training and awareness

When an organization introduces new services, it's important to educate the consumer about the risks that come with it. Patients need to understand that their data belongs to them, and that no provider safeguards can replace their own responsibility to make smart decisions about how and where they use virtual health services. Communicating that principle is one responsibility of a provider organization that offers virtual services. So is the parallel responsibility to make sure physicians who use the system approach it with the same understanding.

Demand among millennials paves the way

Digital habits vary with age group, and millennials—now the largest segment of the US workforce at 83 million strong—are also the most comfortable with virtual health. According to a First Stop Health survey, 60 percent of millennial respondents support use of virtual care to replace in-office visits.[5] The Deloitte 2018 Survey of US Health Care Consumers and Physicians corroborates these findings: Among all age groups surveyed, millennials were the most interested in telemedicine services across different types of care, such as filling prescriptions, measuring fitness, monitoring health issues, or transmitting information about medications.[6]

This demographic group is both a worthy target for virtual health offerings and an indicator of things to come, given that succeeding generations are likely to bring even more sophistication to their digital habits. By catering to them now, provider organizations can contribute to both present and future adoption. This is relevant to the question of cyber risk because "digital native" generations of both patients and physicians perceive it differently and bring different thresholds to their use of it.

[5] Dave Guttman, "29 Statistics You Need To Know About Healthcare & Telemedicine," First Stop Health, August 1, 2017.

[6] Ken Abrams, MD, and Casey Korba, "Consumers are on board with virtual health options."

Security as a key to broader adoption

There are many parts of the health care environment that rely on data security and cyber risk protocols. Some of them, such as electronic medical records and patient finances, have already reached a maturity level based on years of experience.

Virtual health is a different kind of cyber challenge in part because it's a frontier—an emerging practice without those years of experience in place. It also relies more directly on cybersecurity: People are concerned about securing their medical records and payment information, but they won't avoid using the health care system because of those concerns. As Deloitte's surveys indicated, security is a reason some users—particularly physicians—may be reluctant to use virtual health at all.

Taking the steps described here to strengthen cybersecurity in virtual health, and to make people feel confident in those safeguards, is a complex challenge that encompasses clinical technology, digital technology, legal compliance, and consumer relationships. Answering that challenge will require provider organizations to offer innovative new services, protect data, and develop new applications, business processes, and cloud strategies all at once. And of course, this entire undertaking is only one of the competing investment needs a provider must balance.

The argument for putting this investment at the head of the line? It's a key that can unlock the potential of many others. When virtual health works, provider organizations and their patients can make new strides toward that "triple aim" of access, quality, and cost. But virtual health won't work that way until a critical mass of people is comfortable using it, and people won't feel comfortable until they're confident it's secure.

Let’s talk

Raj Mehta
Partner
Deloitte & Touche LLP
rmehta@deloitte.com
+1 713 982 2955

Daniel Poliquin
Principal
Deloitte & Touche LLP
dpoliquin@deloitte.com
+1 312 486 5627

Sean Wright
Principal
Deloitte & Touche LLP
seawright@deloitte.com
+1 404 631 2845

Deloitte.