Deloitte.

The future of cyber in the future of health

The evolving role of cybersecurity in health care

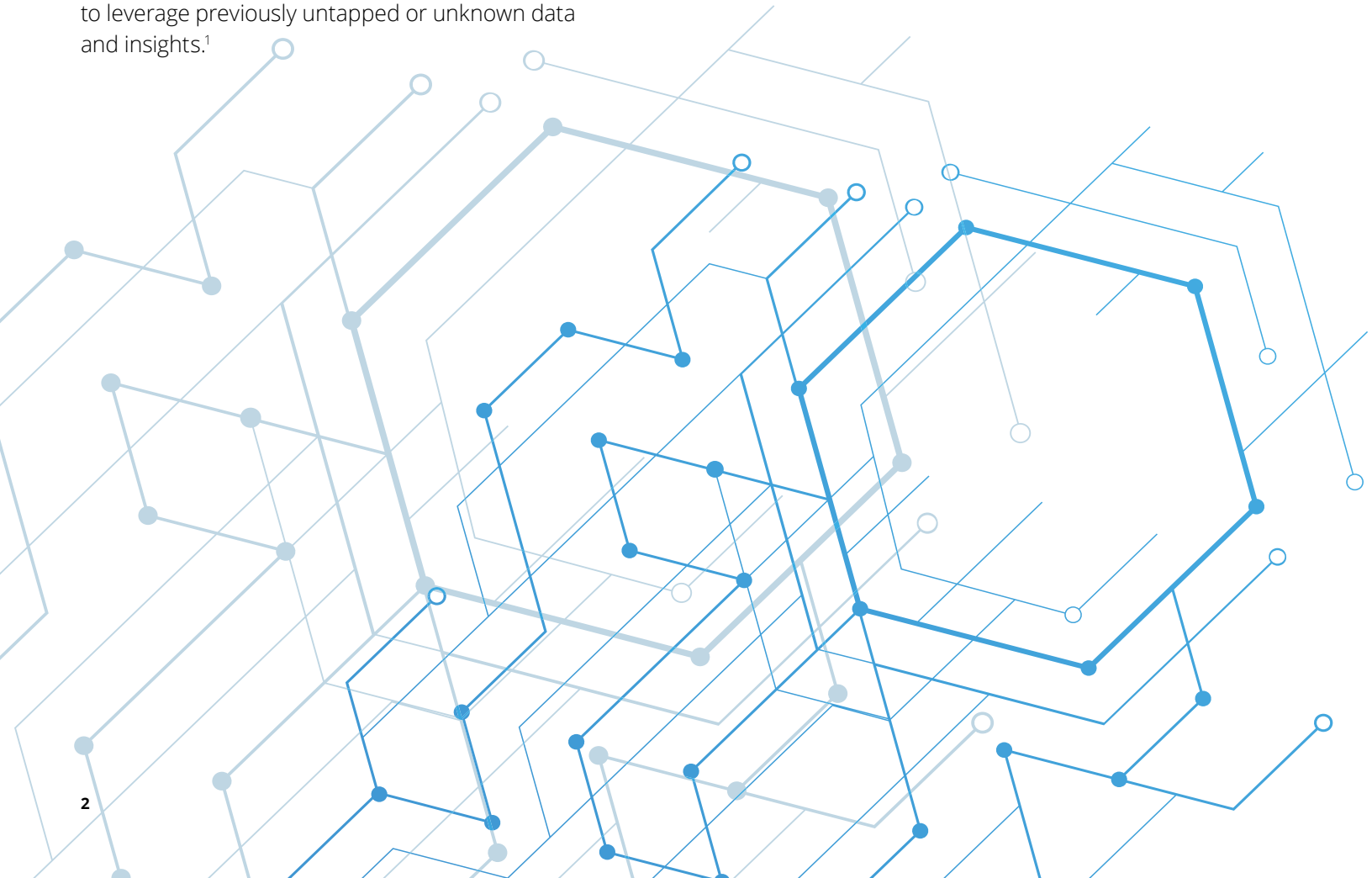
Introduction

Imagine a world where you wake up every morning and your personalized device tells you exactly which supplements to take based on your nutrition, environment, activity, and stress levels over the past week. Powered by artificial intelligence (AI), your device can proactively tell you when you may be coming down with the flu, when you need more sleep, and when your speech patterns or behaviors suggest that you're at risk for a health disorder. Health care is evolving into a new era where nearly everything is connected through digital technologies to meet the common goal of improving the way health care is delivered to patients. In this future, there is no more guessing; consumers will know how to take their health into their own hands.

Industry watchers agree the future of health will likely be driven by radically interoperable data. Open platforms will connect individual, population, environmental, and institutional data sets in real time and allow life science and health care companies to leverage previously untapped or unknown data and insights.[1]

And while the COVID-19 pandemic has created many new challenges for the health care sector, it has also greatly accelerated change in some areas: Remote work is now the norm versus the exception, consumer adoption of virtual health is widespread, clinical trials are being digitized, and outbreak detection is powered by AI. In fact, by 2023, 20% of all patient interactions will involve some form of AI enablement within clinical or nonclinical processes, up from less than 4% today.[2]

Underlying all of these exciting developments is cyber. It's truly everywhere. And the risks surrounding it will only increase as the future of health takes shape. This report takes a critical look at the future of health through the lens of cyber risk. We explore six key factors driving cyber in the future of health, along with the cybersecurity considerations that accompany them and the steps leaders can take to help manage these evolving risks.



The future of health at a glance:

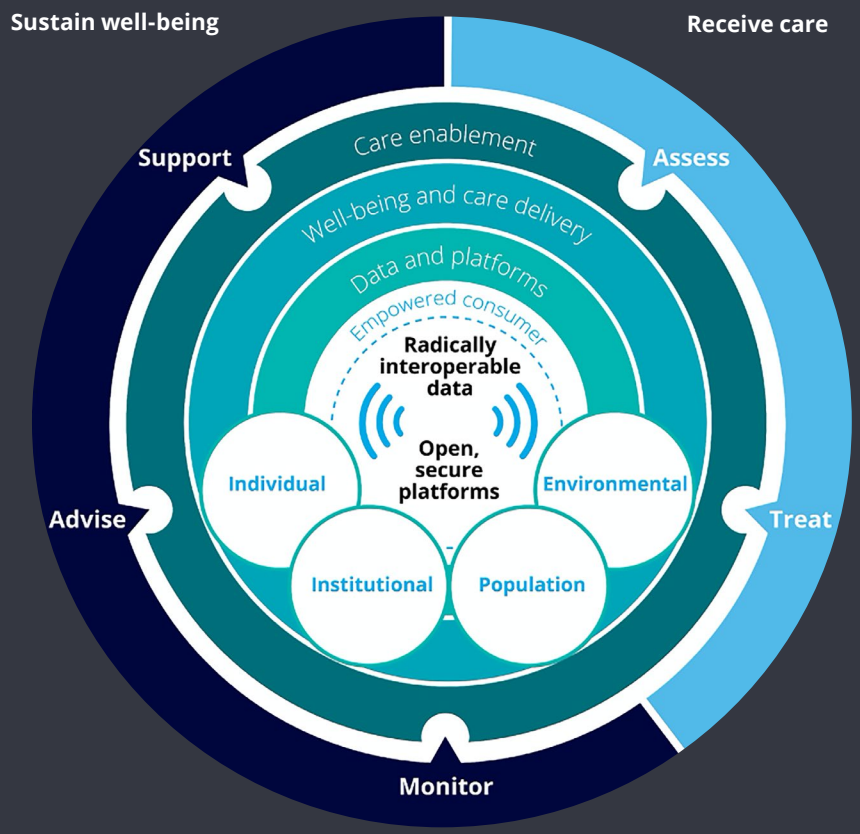
Before exploring the future of cyber in health care, let's review some of what we can expect to see in the future of health overall:

Radically interoperable data that empowers hyper-engaged customers to sustain well-being and receive care only in the instances where well-being fails.

Always-on sensors for capturing data 24x7 and platforms that aggregate, store, and drive insights from individual, institutional, population, and environmental data will catalyze the transformation.

Prospective and predictive care that adapts to the needs of the empowered consumer can enable a dramatic shift from the retrospective and reactive care of today's current environment.

The future of health will be driven by digital transformation enabled by radically interoperable data and open, secure platforms



Cyber in the future of health

In the future of health, data will be more widely shared, collected, and analyzed. Health care organizations will be positioned to create new value from this previously unavailable information, using it to drive operational efficiencies and help enhance consumer engagement. As this transformation advances, organizations will need to pay closer attention to data privacy and take steps to modernize data protection standards. They will also face added pressure to establish better cyber threat awareness, detection, and response capabilities. According to a 2020 Gartner report, "Privacy and security are considered top barriers to the adoption of AI and other advanced technologies."[3] Integrating security, privacy, and ethical considerations into future health capabilities will be essential to earning and retaining consumer trust across health ecosystems and providing the benefits that consumers expect.

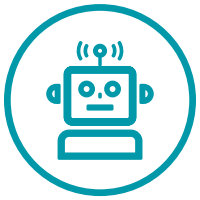
With the future of health taking shape sooner than predicted in large part due to COVID-19, health care leaders need to prepare for the rapidly changing risk landscape that comes with progress and innovation. They can start by understanding the six drivers that are likely to play a key role in defining the future of cyber in health care.

Agility

Ecosystem coordination

Devices

Data



Artificial intelligence

User-friendly

Agility

Health care organizations are investing in and piloting various types of solutions related to delivering health care services, driving consumer behaviors, monitoring critical life-supporting services, and more. These experiments are typically incubated and deployed at an accelerated pace by nontraditional departments or divisions within organizations. And while typical cybersecurity and data privacy practices are not known for being agile or adapting to change quickly, cybersecurity and privacy groups should be integrated to these pilot groups for insights and learnings that could make their people, process, technology, and data capabilities more agile and forward-looking. Doing so will not only help cyber adapt to fast-moving change, but also enable a more efficient digital health–related innovation within their organizations. For the critical digital services associated with patient life, it will be extremely important to integrate and apply agile security processes to help manage the risk and expand the availability of services (including the up-front integration of cyber during the ideation and pilot phases of solution development, processes to provide enhanced speed of recovery in digital devices in case of a security incident, continuous enhancement of monitoring and notification capabilities, and more).

Let us consider the potential impact of agile approaches in the following processes:

DevSecOps: Through the use of automation (e.g., preconfigured components and integrated security requirements or triggers), DevSecOps can help improve the security and compliance levels of a company's software development life cycle while boosting quality, efficiency, and productivity across four key capabilities:

- **People:** In the traditional waterfall model, the development, security, and operations teams are siloed. Agile approaches call on organizations to break down silos quickly, integrate teams, and create shared goals.
- **Process:** : Organizations need to simplify manual processes as much as possible without sacrificing cybersecurity needs. By creating normalized development processes like incremental static code scanning and incorporating it into the design phase rather than in the development or test phase, organizations can gradually progress toward becoming more agile.
- **Technology:** Effective solution ideation and pilot processes require the securing of specific technology, rapid solution deployment, and the up-front integration of cyber.
- **Culture:** In order to enable and embed the agile capabilities related to security, DevSecOps also needs to embrace organizational and cultural change management that revolves around risk awareness, assessment, and resolution. Threat- and solution-based change review tiering and triggers can help organizations adapt to change and operate with greater agility while keeping current risk in your direct line of sight and emerging risk on your radar screen during change management.

Risk management: As interest in and focus on information security and privacy threats have grown, organizations have acquired more resources to identify these risks. However, their ability to address the "visibility bubble" of risks remains limited. Organizations need to reexamine their risk management processes, including the concept of risk tolerance. Understanding risk tolerance and associated guardrails will be important as organizations experiment with new ways to engage consumers and deliver health and wellness services.

Digital identity management: As the number of connected devices grows, health care system access and identity management becomes more complex—and the user experience more important. It will be critical for an organization to provide a seamless access experience across multiple tools or platforms by leveraging flexible, next-generation forms of authentication that leverage behavior analysis and machine learning to grant access versus relying on static and defined roles. Therefore, more cost-, time-, and risk-effective approaches to the digital identity management of people, emerging new solutions like bots, the growing number of devices, and certificates will play an essential role in the success of the future of health.

Third-party risk management: Ecosystems and alliances will also play a pivotal role in this new future. In this fast-paced environment of innovative and solution development, collaboration, not a siloed and solo approach, will drive success. But as these partnerships expand to provide new digital services, so can the risks and challenges. Associated third parties and contractors need to be effectively managed by life sciences and health care organizations. Traditional ways of collecting and sharing information will no longer be feasible and effective to manage third parties. Organizations will have to adopt technologies and innovative solutions to streamline the process of identifying, analyzing, and monitoring third parties to allow data-driven decision-making and risk analysis. For example, how can organizations use data analytics that incorporate context, correlation, and tolerance to drive insights and enable a collective focus on the issues and initiatives that matter most?

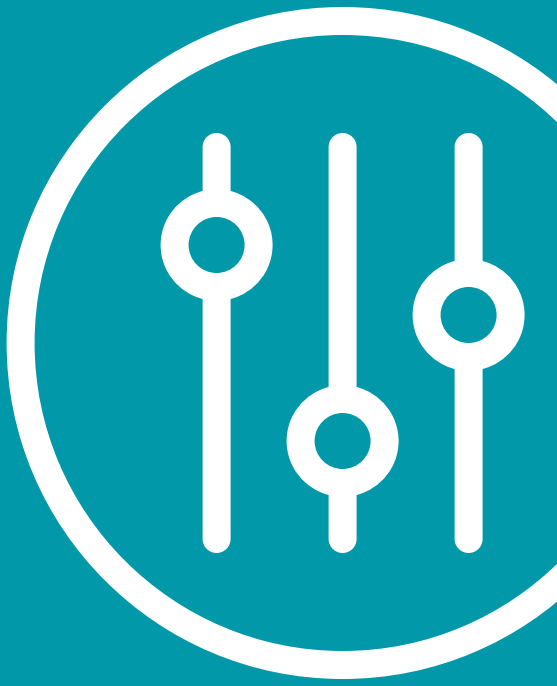
Back to Cyber in the future of health

Ecosystem coordination

Across many industries, by 2023, organizations that are part of a connected digital business ecosystem will have 40% of their customer service cases initiated by business partners in that ecosystem.[4] Many health care entities are collaborating with vendors and business partners in the ecosystem to develop new solutions (e.g., cloud-based analytical platforms, medical applications on smart devices, and data aggregation).

Securing these ecosystems will be key to their achievements and those of the digitally powered and virtual health care services they provide.

As part of their governance, risk, and compliance function, many organizations have processes to assess risks posed by extended relationships. Typically, those entail reliance on contracts such as business associate agreements and extensive, static questionnaires with business partners and vendors—which can take weeks, even months to assess. These current approaches are not likely to be sustainable when accounting for costs, results, and business needs in the fast-moving, digitally powered future of health. For health and wellness services to be developed and delivered via ecosystems, organizations may need to assess end-to-end security and privacy considerations at an architecture level, considering interoperability of security, the impact on user experience, and more. Some organizations are starting to more efficiently evaluate third parties by reassessing risk tolerance, using data analytics on third-party network data and account behavior, and relying on certifications and/or shared assessments.



Devices

The number of devices will significantly increase in the future of health, as will their value in the health care ecosystem. Gartner forecasts that "by 2023, device makers will focus on offering smaller, clinical-grade sensors for health wearables that increase monitoring accuracy by 20 percent."[5] The challenge for health care organizations will be trusting the devices and data they generate, which may often be outside their control.

From wearables and home-based telemetry devices, managing the security and privacy risks for these types of devices and the data they produce will be a front-and-center priority.

Organizations should start thinking about their identity and access management processes for how these devices will be registered and linked to consumers. They should also explore the use of analytics to detect unusual behavior, which could indicate devices have been compromised. Some organizations may need to create or partner with a security operations center (SOC)–type capability to prevent, detect, analyze, and respond to incidents related to consumer identity and device cybersecurity.

Back to Cyber in the future of health

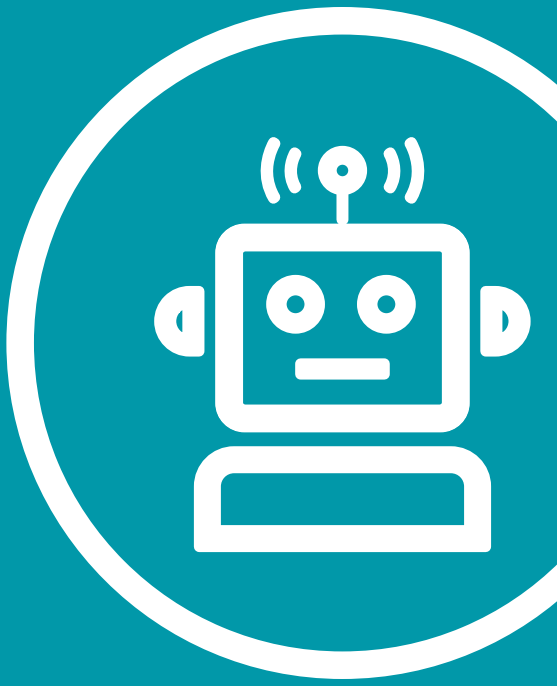
Data

"By 2024, 20 percent of all health information exchanged among patients and providers in the US will be consumer-mediated."[6] And that is only four years from now. The future of health will be characterized by lots of devices, lots of data, and lots of sharing—which will make radically interoperable data and open platforms key enablers of the innovative services and delivery models on the health care horizon. These same forces will also make digital privacy a high priority. Health care organizations will need to account for privacy, ethics, and other considerations when designing and creating data flows.

That is not likely to be easy given the volume, variety, and velocity of data (e.g., social media, medical devices, and smart home data) that will be generated, analyzed, and shared among health ecosystem players. Setting up strong aggregation, interoperability, and analytics will be integral to unlocking the potential of this data and confirming its security. As organizations work toward this future state, many questions are likely to arise: What does digital privacy look like in the future? How will organizations provide consumers with transparency when it comes to their data and how it is being used? Who will own the data? If there is a breach, who is responsible? How might regulations evolve and apply? There is no one playbook or framework to address these new questions. Relying on a regulatory perspective alone will be insufficient in addressing complicated data management and security issues. Organizations have to adapt a forward-looking strategy for managing these emerging risks and securing patients' data.

Back to Cyber in the future of health

Artificial intelligence



During the COVID-19 pandemic, AI projects have accelerated in health care, bioscience, and health-related sectors such as manufacturing, financial services, and supply chain. "Gartner polls conducted during May 2020 and June 2020 found that 47 percent of respondents' AI investments were unchanged since the start of the pandemic and 30 percent of respondents planned to increase their investments."[7] Why the continued commitment? The insights that AI can help generate add a new layer of value to the data that is being collected and shared across the health care ecosystem. As AI is starting to be applied in clinical settings, organizations need to heed the early lessons learned. The implications of incorrect results based on faulty algorithms, as well as the potential impact on recipients of health care services, could be magnified by associated cyber risk and ethical issues. Model theft (counterfeit functionality of AI model), model inference (further manipulation of model with malicious intent), and outcome manipulation (malicious training to change outputs) are just a few examples of new threat types posed by AI solutions.

Proactive threat analysis on AI applications and protection of AI source data and algorithms are just a few of the strategies organizations should be prepared to use to enable the ethical design and governance of this powerful technology. Addressing these issues early on will help safeguard against potentially disastrous consequences for health ecosystems and the consumers they serve and allow organizations to continue exploring the revolutionary potential uses of AI in this new future.

Adapting a holistic framework for trustworthy AI and AI ethics can help organizations mold their cybersecurity capabilities to address emerging threats and ethical risks from the application of AI- and machine-based decisions. Built on our deep risk, audit, and assurance heritage, Deloitte's Trustworthy AI™ Framework can be an effective first step in assisting in diagnosing and addressing the ethical health of your AI deployments while helping in maintaining customer privacy and abiding by relevant regulations.

Back to Cyber in the future of health

The ethical design and governance of AI will be essential in the future of health

Deloitte's Trustworthy AI™ Framework

Fair and impartial
AI applications include internal and external checks to help ensure equitable application across all participants

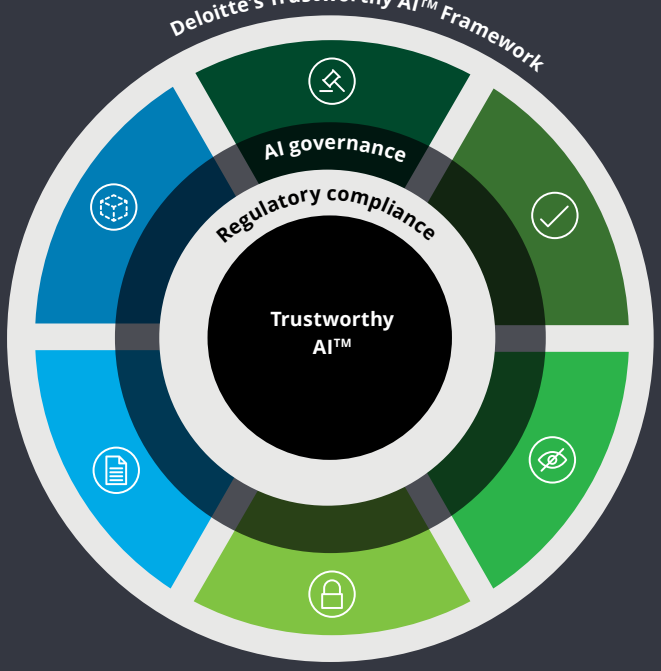
Transparent and explainable
All participants are able to understand how their data is being used and how AI systems make decisions; algorithms, attributes, and correlations are open to inspection

Responsible and accountable
Policies are in place to determine who is held responsible for the output of AI system decisions

Robust and reliable
AI systems have the ability to learn from humans and other systems and produce consistent and reliable outputs

Privacy
Consumer privacy is respected, and customer data is not used beyond its intended and stated use; consumers are able to opt in and out of sharing their data

Safe and secure
AI systems can be protected from risks (including cyber) that may cause physical and/or digital harm



User-friendly

Gartner predicts that "by 2022, 50 percent of large organizations will have failed to unify engagement channels, resulting in the continuation of a disjointed and siloed customer experience that lacks context."[8] Having a 15-character password that must be changed every 30 to 60 days may not be an effective way to engage consumers seeking access to health services from their personal devices. And if individuals don't have visibility into their personal data and how it is being used, they may be reluctant to share it with organizations.

As the future of health takes shape and consumers assert more control over their health decisions, cybersecurity and data privacy solutions should be easy to consume if they are to be viable.

Creating balance between reasonable security and ease of use will be crucial. For example, how can advancing technology help organizations move away from cumbersome password systems to more intuitive authentication programs that rely on a combination of behavior, location, and other factors? Designing user interfaces that are persona-based is another potential way to engage users in an easy-to-use and safe way. As with many of the solutions in the future of health, designing and developing these capabilities will likely require new collaborations with ecosystem partners, human capital resources within their own organizations, and end consumers.

Back to Cyber in the future of health

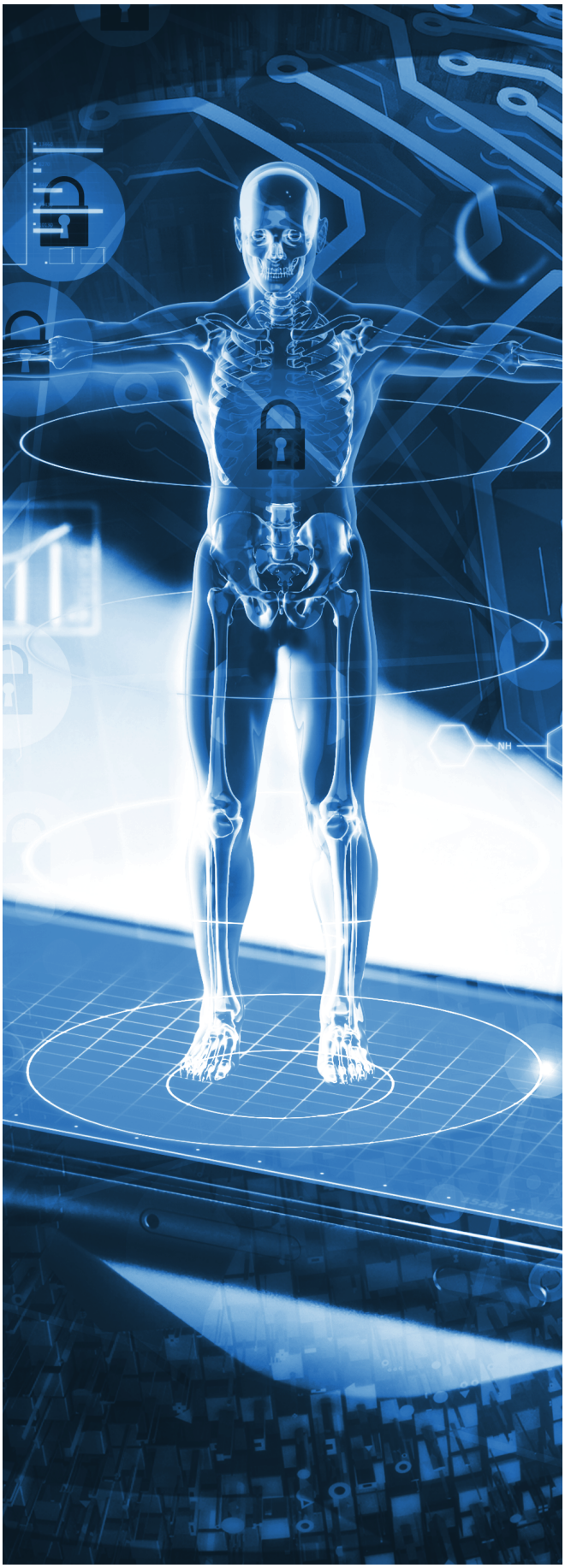
Preparing for a promising and secure future

Over the past several months, the COVID-19 pandemic has pressure-tested our vision for the future of health. We've seen firsthand that consumers want to engage with the health system differently than they have in the past. As consumers continue to move toward the center of the health care system—and many of the pillars in the future of health dramatically accelerate—the health care industry is turning to technology to drive these changes as efficiently as possible.

Now more than ever, it is imperative for cybersecurity and privacy to become fully integrated, by design, in the piloting and deployment of new health care services and solutions. To do this effectively, organizations should challenge how they think about security, from risk tolerance to the application of analytics. And security and privacy leaders will need to consider the following:

- Focusing on risk management, not just compliance; the art of communicating risk (e.g., what is the issue, why do I care, and what are my options?) in nontechnical security language is key to influencing and supporting business decisions
- Building a team with skills that go beyond traditional "security thinking," including insight into persona-based user experiences, the application of innovative approaches (e.g., analytical and predictive models to manage security outside the walls of the organization), and the willingness to challenge bureaucratic processes
- Effectively integrating security and privacy capabilities (which will require breaking down the silos between functions) to reduce overlaps and capitalize on complementary capabilities
- Identifying an ecosystem of partners to collaborate with on designing solutions to new or thorny problems (e.g., what does the identity management life cycle look like for devices that we do not own or manage outside our walls, but need to trust?)

Health care is on the brink of many seismic shifts. Innovations and external factors will continue to elevate and introduce new risks. And industry players are beholden to responsibly embrace the drivers of change and the challenges to come, not only to deliver on the promise of the future of health, but also to enable a safe and secure tomorrow.



Contact us

John Lu
Principal, Life Sciences & Health Care
Deloitte & Touche LLP
jolu@deloitte.com

Raj Mehta
Partner, Health Care
Deloitte & Touche LLP
rmehta@deloitte.com

Neal Batra
Principal, Life Sciences & Health Care
Deloitte Consulting LLP
nebatra@deloitte.com

Authors

Raj Mehta
Partner, Health Care
Deloitte & Touche LLP
rmehta@deloitte.com

Ali Muzaffar
Senior consultant, Life Sciences & Health Care
Deloitte & Touche LLP
amuzaffar@deloitte.com

Endnotes

1. Deloitte, "Harnessing opportunities and managing risk in the future of healthcare," July 2019, https://www2.deloitte.com/us/en/pages/risk/articles/opportunities-and-risks-in-future-of-health-and-life-sciences.html.
2. Gartner, "Gartner Says 50% of U.S. Healthcare Providers Will Invest in RPA in the Next Three Years," May 21, 2020, https://www.gartner.com/en/newsroom/press-releases/2020-05-21-gartner-says-50-percent-of-us-healthcare-providers-will-invest-in-rpa-in-the-next-three-years.
3. Gartner, "Business Drivers of Technology Decision for Healthcare Providers, 2020," January 22, 2020, https://www.gartner.com/document/3979844?ref=solrAll&refval=254603464.
4. Gartner, "6 Critical Technologies to Advance Healthcare Ecosystem Orchestration Ability," September 13, 2019, https://www.gartner.com/document/3957374?ref=solrAll&refval=258829768.
5. Gartner, "Forecast Analysis: Wearable Electronic Devices, Worldwide," October 24, 2019, https://www.gartner.com/document/3970729?ref=solrAll&refval=260386436.
6. Gartner, "Healthcare Provider CIOs: Prepare for the Consumer-Mediated Health Information Exchange," December 20, 2019, https://www.gartner.com/document/3978614?ref=solrAll&refval=258830042.
7. Gartner, "Hype Cycle for Artificial Intelligence," July 27, 2020, https://www.gartner.com/document/3988006?ref=solrAll&refval=258830293.
8. Gartner, "The Evolution of Healthcare Consumer Engagement Hub Architecture," February 25, 2020, https://www.gartner.com/document/3981326?ref=solrAll&refval=258829965.

Deloitte.