Top of Mind for Top Health Systems 2019

Insights from health systems on IT priorities for the year ahead

Center for Connected Medicine

The Academy
The Health Management Academy

A report from the Center for Connected Medicine
and The Health Management Academy

Table of Contents

Introduction

What is Top of Mind in Health IT?

As health system leaders look ahead to the challenges and opportunities of the coming year, they are increasing their spending to defend against cyberattacks, expressing optimism about higher reimbursement for telehealth services, and feeling anxious about Apple, Amazon, and Google entering the health care space. Those are among the key findings included in this report, which dives into three areas of health IT that those executives believe will have the most impact on health care in 2019.

For the second consecutive year, the Center for Connected Medicine (CCM) partnered with The Health Management Academy (The Academy) on the Top of Mind for Top Health Systems research project to identify the most pressing health IT issues and understand why they are a focus of health system leaders. The Top of Mind 2019 research project is focused on what C-suite leaders are thinking about for the coming year, as they face a growing set of challenges and are looking to technology for solutions as well as opportunities to expand, innovate, and better serve patients and consumers.

The report has been released near the end of 2018 to set an agenda for the next 12 months, inform the innovators and change-makers who make up the CCM community, and provide timely information to industry leaders.

Areas of greatest impact

The top three areas of health IT that executives at some of the largest health systems think will have the most impact in 2019 are:

Cybersecurity

Telehealth

Interoperability

Cybersecurity remained at the top of the list from the previous year's survey, and telehealth and interoperability climbed the ranking. The previous year's Top of Mind report had identified cybersecurity, consumer-facing technology, and predictive analytics as the top three areas of focus for 2018. While consumerism and analytics remain hot topics in health care, it was not surprising to see telehealth and interoperability rise in the minds of health IT executives for 2019. Policymakers, in particular, have emphasized telehealth and interoperability in the past year, and the threats of cyberattacks and data breaches are constant in health care.

The following pages provide insights gleaned from quantitative surveys and qualitative interviews with C-suite leaders on cybersecurity, telehealth, and interoperability.

Methodology

The Top of Mind 2019 research project had three components: An initial survey to establish priority areas, a quantitative survey, and qualitative interviews.

In May 2018, The Academy conducted an online poll of health system C-suite IT executives to determine the most impactful areas of health IT for 2019. With a 60% response rate, 63 Chief Informatics Officers (CIOs), Chief Medical Informatics Officers (CMIOs), and Chief Nursing Informatics Officers (CNIOs) responded. The results of this survey were used to determine the priority areas of the subsequent research.

In July 2018, The Academy conducted an online survey of health system executives regarding their outlook for health IT in 2019. This quantitative survey focused on three high-priority areas identified in the earlier online poll: cybersecurity, telehealth, and interoperability. The 30 respondents included CIOs, CMIOs, and CNIOs.

Following the quantitative survey, The Academy conducted a series of qualitative interviews in September 2018 with 18 C-suite executives, including IT executives (CIO, CMIO) and non-IT executives (CEO, COO), to gather further insights into the quantitative findings and how IT trends impact their organizational strategies and priorities.

This report includes the perspectives from a total of 44 executives, representing 38 health systems, across the quantitative and qualitative assessments.

Top of Mind 2019 Respondent Demographics

Total number of health systems: 38

Average annual revenue of responding health system: $5.3 BILLION

Total number of hospitals owned by responding health systems: 459

Regions of responding health systems:

East 45%

Central 24%

West 32%

Cybersecurity

INTRODUCTION:

A Top Priority as Cyberattacks Mount

Health care is among the most-targeted industries for cyberattacks. And for good reason. Vast amounts of highly valuable data, coupled with less mature cybersecurity programs than other industries, makes health care a prime target for cybersecurity attacks.

Between 2010 and 2017, the health care industry was hit with 2,149 breaches comprising a total of 176.4 million records between 2010 and 2017, according to a study published in JAMA Network in September 2018. And the number of data breaches increased in almost every year, starting with 199 in 2010 and ending with 344 in 2017.

Some of the largest cyberattacks have caused both reputational and financial harm to institutions. Health insurer Anthem agreed to pay $16 million — the largest ever fine related to HIPAA violations — in October 2018 for a series of data breaches in 2014 and 2015 that exposed the records of 78 million individuals. Even the federal government is not immune. The Centers for Medicare and Medicaid Services (CMS) in October 2018 reported that Healthcare.gov was breached by hackers, potentially exposing the records of 75,000 individuals who had enrolled in health insurance plans through the website.

As the number of attacks continues to increase, and these costs are recognized, health systems are elevating cybersecurity to a top priority. The following section delves into executives' confidence in their ability to recover from attacks, how spending is growing, how executives view the risks related to cybersecurity, and where health systems are most vulnerable.

> "Cybersecurity is… right up there on top with regulatory problems and readiness for value-based care. Always there at the top."
>
> – CEO

Cybersecurity

KEY FINDINGS

Health system executives were not uniformly confident in their ability to recover quickly from cyberattacks

- Only 20% of respondents reported being "very confident" in their organization's IT recovery and business continuity plans
- 70% of respondents said they were "somewhat confident" in those plans

Spending on cybersecurity will increase for the second year in a row as health systems play catch-up with sophisticated cybercriminals

- No respondents reported that spending on cybersecurity would decrease in 2019
- 87% of respondents expect cybersecurity spending to increase in 2019, with nearly half expecting an increase of greater than 5%

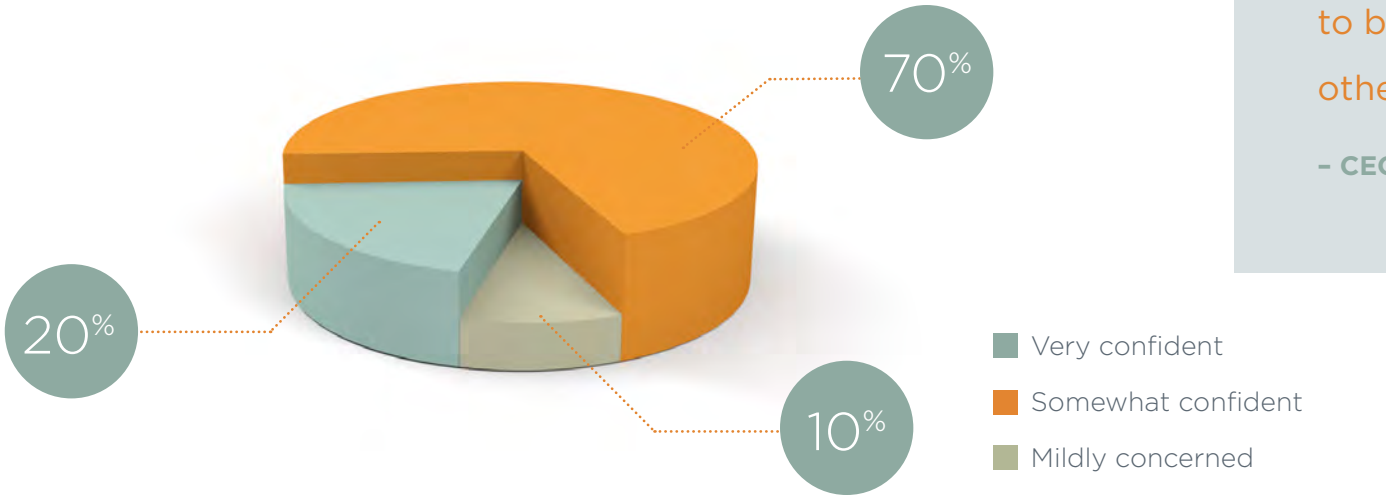
The pervasiveness and sophistication of phishing attacks, along with the need for greater employee vigilance, remains a serious problem for health systems

- The most commonly cited challenge in cybersecurity was employee education
- 62% of respondents named "staff" as greatest point of cybersecurity weakness
- Phishing and spear-phishing cited as most common types of cyberattacks in previous 12 months

‘Somewhat Confident’ Leads Responses

Despite increasing financial investment and prioritization of cybersecurity at health systems, executives did not express robust confidence in their organization’s IT recovery and business continuity plans after an attack or breach. Seven out of 10 respondents reported being “somewhat confident” in their recovery and continuity plans; only 20% said they were “very confident.”

How confident are you in the robustness of your organization’s IT recovery and business continuity plans should you face a data breach, corruption, or loss?



> “The people that are up to no good have far better tools than we do on our platforms. If they really target you, they will likely find a way in.... We are not trying to make it impenetrable, but we are trying to make it more difficult to break into our system than others in our market.”
>
> – CEO

Cybersecurity

SYSTEM RESILIENCE

'When' Not 'If'

While it is encouraging to see that no executives said they were "very worried" — and no one responded that they had no such plans — it is important for the industry to acknowledge that a damaging cyberattack is likely a "when" and not an "if" proposition. Cybercriminals have sophisticated tools and are targeting large, complex systems that are trying to balance security with expanding data volumes and a greater demand for access to data from a variety of sources.

As a CEO commented, "The people that are up to no good have far better tools than we do on our platforms. If they really target you, they will likely find a way in.... We are not trying to make it impenetrable, but we are trying to make it more difficult to break into our system than others in our market."

Stepping Up Security

Many health systems have implemented network segmentation to prevent full access to the organization's network if a breach were to occur. With a greater emphasis on connectivity and data access, as well as the increased adoption of connected devices through the Internet of Things (IoT), health systems are designing their network architecture to allow for the greatest amount of connectivity while ensuring security.

Additionally, health systems have implemented rigorous review processes for any device or product that connects to the network, ensuring they meet the organization's security standards. One CIO commented on this process: "We are reviewing everything that's purchased. If it plugs into the wall and has a battery, it requires IT review. The biggest challenge is getting through the reviews quickly. We are also segmenting devices and having regular reviews to ensure they are current."

> "Many (IoT) vendors use fairly proprietary software solutions that have not been created with cybersecurity in mind. How do we create network partitioned in a manner to isolate devices from the rest of the network? The network and subnetwork architecture supports clinical need and segregates those things that we can't make as secure as we want."
>
> **– CMIO**

Cybersecurity

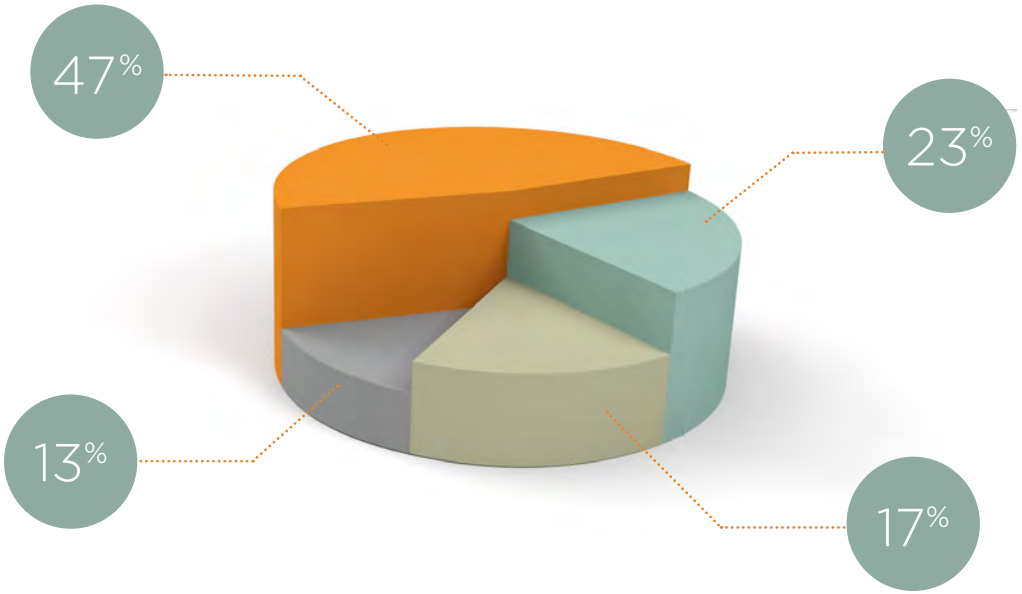
SPENDING

Budgets Grow for a Second Year

Reinforcing the idea that health systems are playing catch-up with the advancing threat of cyberattacks, no health system executive reported that their organization would be decreasing spending on cybersecurity in 2019. And only 13% of respondents said spending would stay the same.

Nearly nine out of 10 respondents said they expect their spending to increase, with about half of those expecting an increase of more than 5%. This finding follows a similar result in last year's Top of Mind survey in which 92% of health systems reported expecting cybersecurity budgets to be higher in 2018.

How do you expect your organization's cybersecurity spending to change in 2019?



Cybersecurity

SPENDING

Where the Money is Going

Many health systems report significant efforts over the last few years to restructure or grow the cybersecurity function at their organization. In last year's Top of Mind survey, 67% of health systems said they were planning to grow their cybersecurity staff. For 2019, health systems said they would invest cybersecurity resources to bolster current areas of investment, with many focusing on both staff and technology, such as firewalls, intruder detection software, and dual authentication that guard against breach of protected health information (PHI).

According to one CIO, "We are looking at our existing systems and enhancing our capabilities, such as firewalls, enabling threat detection, and crawlers in the network that identify PHI and ensure the correct protections are in place. We are also investing heavily on information governance."

Largely satisfied with their current organizational structure and strategy around cybersecurity, health systems are focusing their investments in areas to fill gaps and support their current teams and technologies.

> "Staff is definitely something in which we're investing in the cybersecurity space. We have a pretty good grasp on monitoring, filtering, and screening technologies and the frequent patches and updates that comes with those as the threats shift. The access needs by clinicians and employees to get to information that [the health system] has is a challenge. We have to make sure the right people get through, and in order to do that well you need skilled staff. We are augmenting those roles."
>
> **– CMIO**

TYPE OF ATTACKS

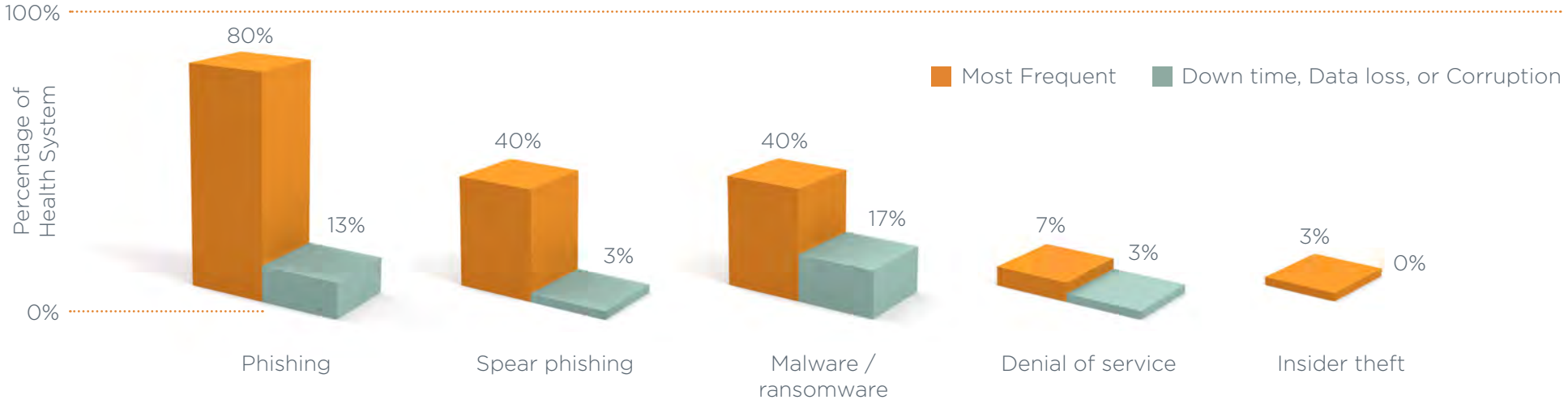
An Easy 'Catch'

The most common types of cyberattacks reported by health system respondents in the past 12 months were phishing, the more-targeted spear phishing, and malware and ransomware. It was not surprising to see phishing as the most common type of cyberattack by a large margin. The wide-net approach of phishing attacks makes them relatively inexpensive to launch. Unfortunately for health systems, these attacks also produce results. Spear phishing, which frequently targets physicians, can be an effective way to steal credentials and gain access to patient health information. Employees at all levels of health systems continue to be fooled by phishing and spear phishing, as we found when we asked about challenges and points of weakness (pages 12-13).

Malware Most Damaging

While executives reported that phishing and spear phishing attacks rarely lead directly to down time, data loss or data corruption, these types of attacks are the vectors for more damaging malware and ransomware. Health system executives reported malware and ransomware as most frequently leading to down time, data loss, or data corruption.

In the past 12 months, which types of cyberattacks have been most frequent? Which have led to down time, data loss or corruption?



Cybersecurity

CHALLENGES

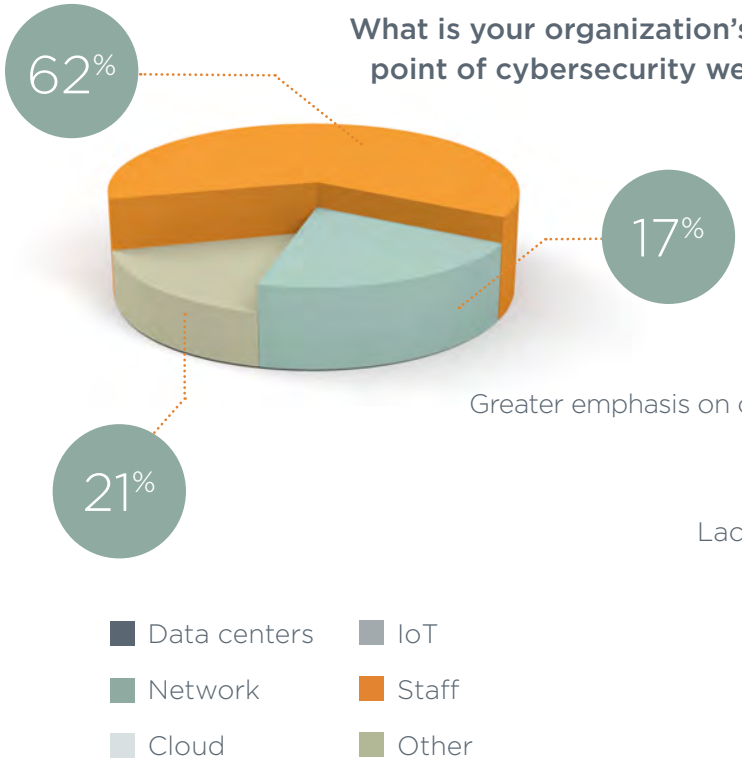
Biggest Challenge: Employee Awareness of Threats

Health systems executives cited employee education as their greatest challenge to maintaining a secure environment for health data. In sync with this finding, executives reported staff as the greatest point of weakness. Despite extensive news coverage of cyberattacks and emphasis by health systems on employee education around the threat posed by phishing, this remains a major vulnerability.

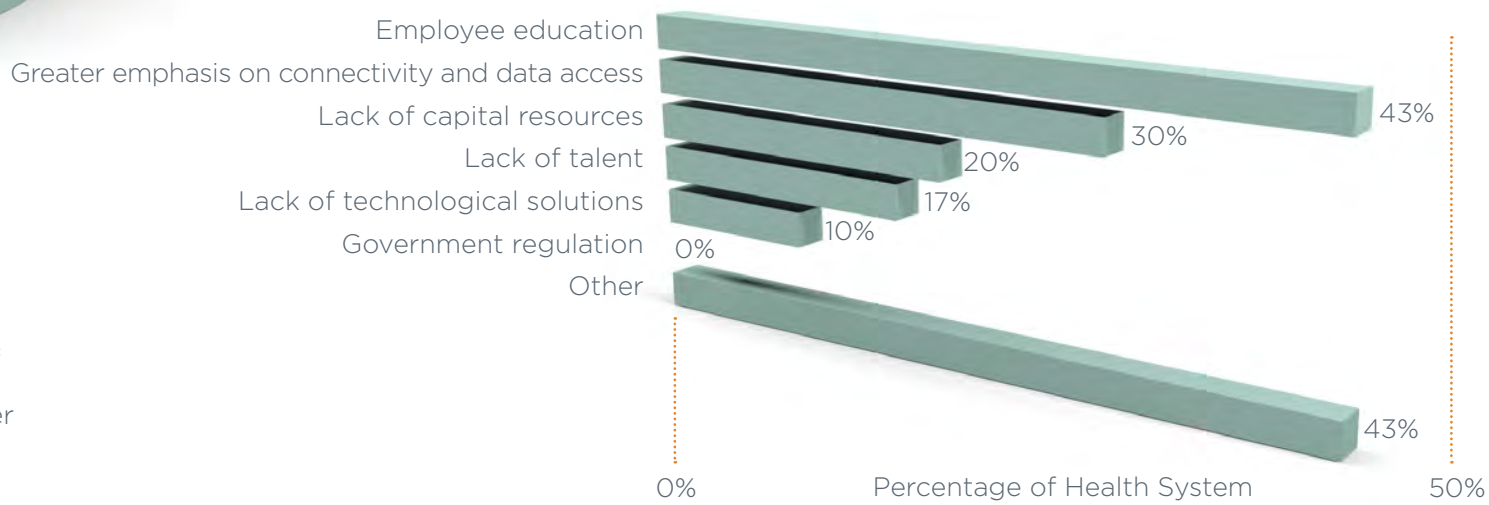
Wide Variety of Challenges

Challenges listed by respondents in the "other" category included organizational and cultural issues such as competing priorities, staff behavior, and leadership alignment, as well as more technical concerns including medical devices, vulnerability management, security in the cloud, decentralized IT, and integration of technology solutions. Executives also cited the rapidly evolving cybersecurity landscape and challenges around keeping up with cybercriminals and fulltime hackers.

What is your organization's greatest point of cybersecurity weakness?



What are your organization's top cybersecurity challenges? [Select up to two]



Cybersecurity

EDUCATION AND AWARENESS

Education is Favored Approach

As health systems continue to build out the staff and infrastructure needed to strengthen their cybersecurity functions, one of the most commonly cited challenges is employee education and awareness of vulnerabilities. Facing frequent phishing attacks, all health systems have implemented educational programs on the threat, commonly involving anti-phishing educational material posted virtually and throughout the buildings, compliance trainings, and leadership communication.

Additionally, most organizations have implemented their own phishing campaigns in which health systems can identify employees in need of additional education. A CMIO commented: "We use these to implement very directed education coupled with realistic threats about minimizing access to data. Not in a disciplinary way but getting [clinicians and staff] to understand that their lack of attention puts patient data at risk. An aspect of being a good clinician is stewardship of electronic patient data."

While health systems have seen click-rates on phishing emails decrease due to internal educational programs, many executives recognize that continued efforts are necessary. Executives cite that it only takes one click by one employee for a phishing hack to break into the health system's network and, therefore, health systems prioritize keeping cybersecurity top of mind for all employees.

Employee Discipline Coming?

Although most health systems do not take a punitive approach to these campaigns, a few organizations reported escalating to disciplinary action after repeat offenses. With the implementation of repercussions, one organization was able to reduce their employee click-rate on phishing emails from 20% to 2% across the organization. "We started phishing campaigns many years ago. Over the last year and a half ago we put some teeth to the program," a CIO said. "We found that we had some people being caught more than a dozen times, even after focused attention and individualized training. Now if we catch an employee clicking on the link three times in 12 months they are reported and either suspended or terminated."

> "We started phishing campaigns many years ago. Over the last year and a half ago we put some teeth to the program. We found that we had some people being caught more than a dozen times, even after focused attention and individualized training. Now if we catch an employee clicking on the link three times in 12 months they are reported and either suspended or terminated."
>
> – CIO

Telehealth

INTRODUCTION:

Anticipation High for Wider Use, Favorable Reimbursement

As health systems rethink care delivery and look for ways to expand access to high-quality care while reducing the total cost, many organizations are implementing telehealth services that allow consumers to receive care in a more convenient and lower-cost setting.

Telehealth is becoming more widely available because of improved technologies, indications that reimbursement policies will be more favorable to health systems, and the normalization of virtual interactions in both personal and professional environments. While telehealth remains a low percentage of overall methods of care delivery at many health systems, the findings in this report show that expectations for an expansion of telehealth are at an all-time high.

Government policy is driving some of this optimism. For example, CMS published a proposal in July 2018 that provided three new remote patient monitoring reimbursement medical codes. While some critics have said the proposal's $14 reimbursement for virtual check-ins is too low, the move by CMS appears to cement telehealth reimbursement as a priority for the agency.

With this optimistic outlook, health systems are making the leap to offer telehealth services, despite the nebulous economics of offering such services. Most health system executives interviewed for this study said their health system had not yet calculated a specific return on investment (ROI) for telehealth. But systems are investing anyway as a hedge that future reimbursement will outweigh the potential losses of today. For the moment, reimbursement is widely thought of in terms of physician time, but as technologies evolve, the question will be whether reimbursement will expand to hardware. Investment can also be seen as a bellwether for provider sentiment toward transformation to value-based care.

While the use of telehealth services is limited compared to total volume of care delivery — just 23% of patients have had video visits, according to the Deloitte 2018 Survey of US Physicians — it is not a stretch to call telehealth "table stakes" for health systems that want to be prepared for the future. What may ultimately differentiate providers and procure value from the investment is whether telehealth strategy is viewed as engaging a new population; yielding visits to higher acuity patients; and opening new horizons for care. For example, the trove of data collected from remote patient monitoring yields tremendous opportunities for analytics and predictive action — the holy grail of value-based care and health care transformation itself.

Telehealth

KEY FINDINGS

Telehealth services represent a low percentage of total care delivery, yet executives unanimously anticipate telehealth growth

- All responding health systems report telehealth accounts for 10% or less of their organization's total care delivery
- Over the next three years, 45% of respondents expect use of telehealth to increase by 10% or more

Lack of reimbursement is the most significant barrier to adopting greater telehealth services among health systems, as less than a third of costs for delivering care via telehealth is reimbursed for a majority of respondents

- 70% percent of respondents cite lack of reimbursement as a barrier to greater adoption

Executives expect the majority of funding for telehealth to come from commercial and government payers within the next three years

- In 2019, health systems expect internal funding and patient co-pays / out of pocket payments to provide most funding for telehealth services

When considering a telehealth technology system, top features/priorities are "integration with the clinical workflow" and "ease of patient triage and virtual follow-up"

- Chatbots, video chat, and secure messaging ranked low by comparison

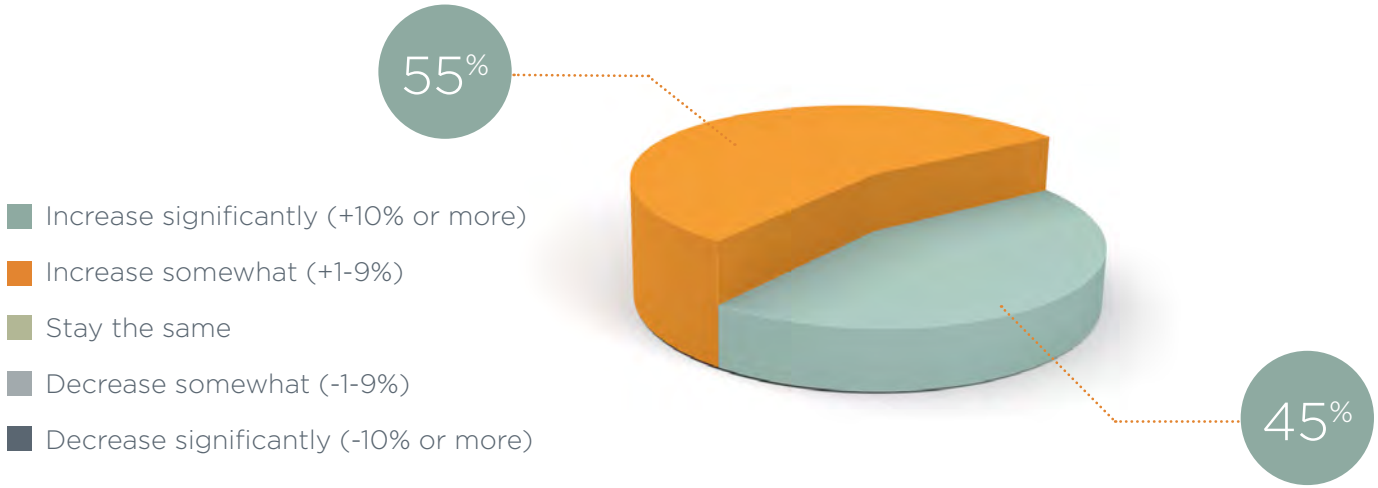
Telehealth

GROWTH OF SERVICES

Health Systems Anticipate Growth

Telehealth represents a low percentage of total care delivery at all responding health systems, yet executives unanimously anticipate growth in the next three years as reimbursement increases and consumer demand picks up. All responding health systems report 10% or less of their organization's total care delivery is currently provided through telehealth. However, all health systems expect an increase over the next three years, with 45% expecting a significant increase of 10% or more.

How would you expect your organization's percent of total care delivery provided through telehealth to change in the next three years?



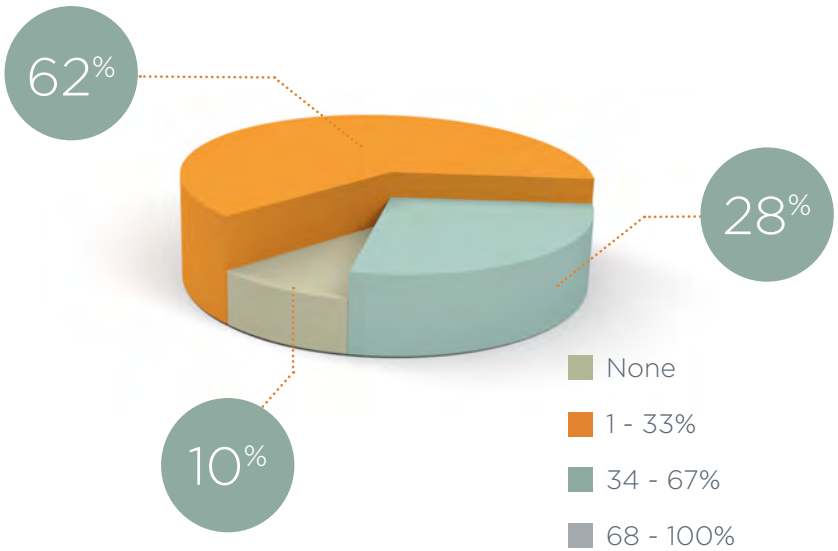
Telehealth

REIMBURSEMENT

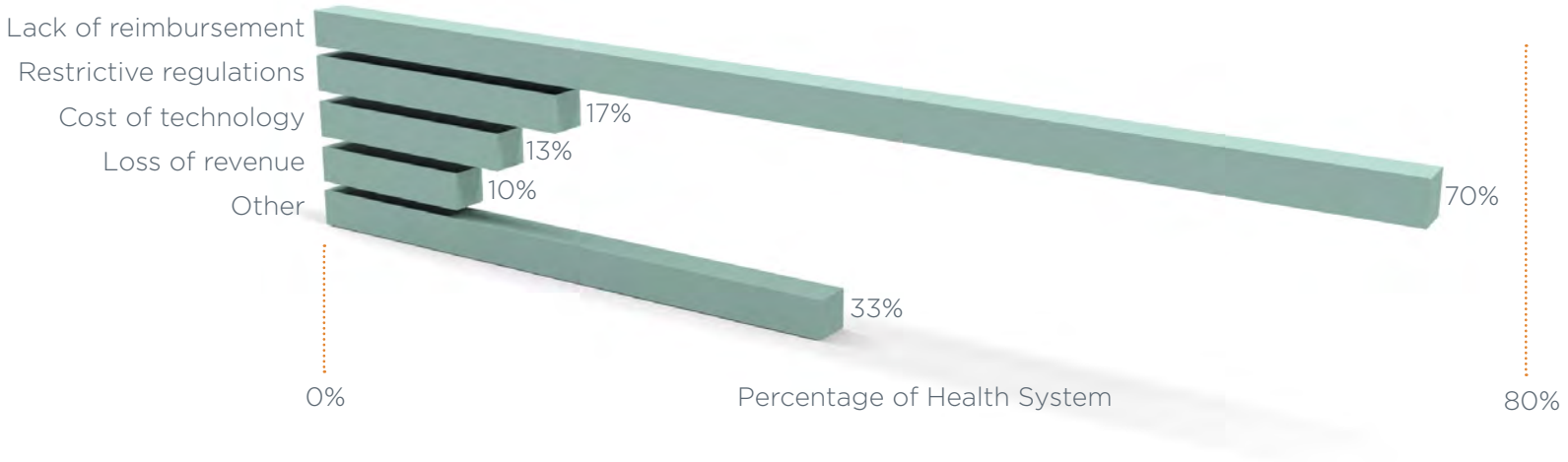
Reimbursement is a Barrier

Currently, a majority of health systems report that less than one-third of their cost for delivery telehealth services are covered by either reimbursement or other external funding sources. Despite this deficit, health system executives are optimistic about government and commercial telehealth reimbursement increasing in the next three years. But for 2019, reimbursement from government and commercial payers remains the greatest barrier to telehealth adoption. This lack of funding is challenging for health systems in adopting and expanding telehealth services, with 70% of executives ranking lack of reimbursement as a top barrier to greater telehealth adoption at their health system. Other challenges include provider availability, readiness, and interest; workflow adoption; capital funding; and competing priorities.

Approximately how much of your organization's costs for telehealth services are covered by reimbursement or other external funding sources?



What are the biggest barriers to greater adoption of telehealth services at your organization? (Select up to two)

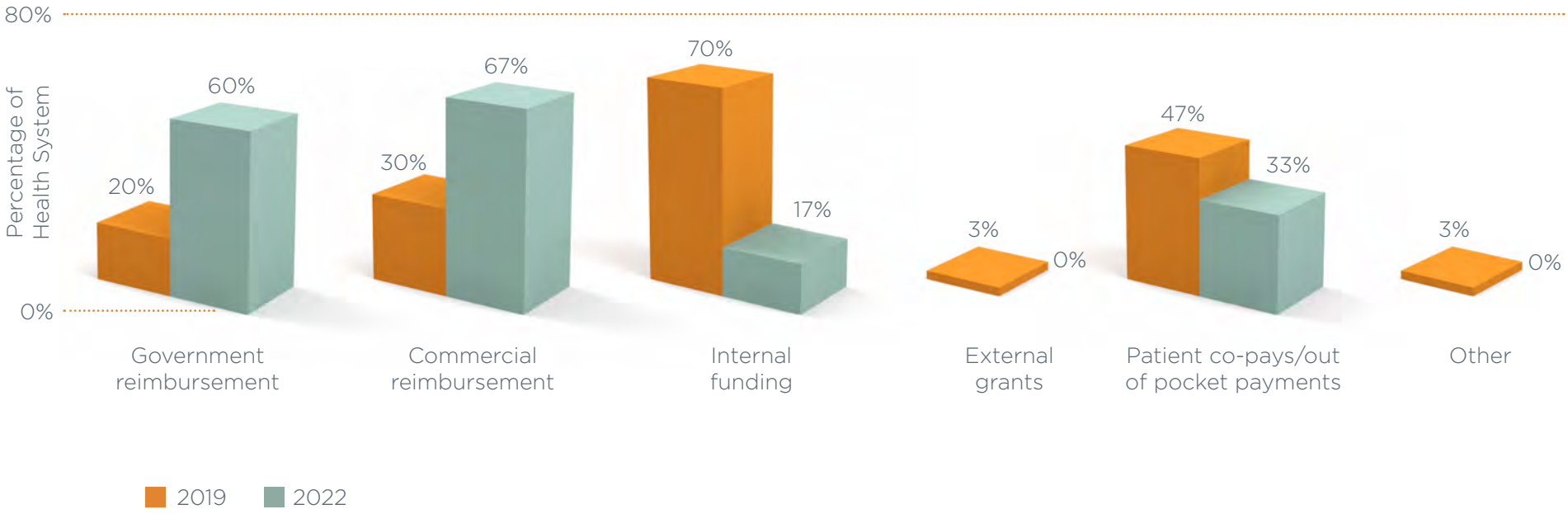


Internal Funding Dominates in 2019

In 2019, health systems expect internal funding (70%) and patient co-pays / out of pocket payments (47%) to provide the majority of funding for telehealth services. Executives expect the majority of funding for telehealth to come from commercial and government payers within the next three years, with just 17% saying they anticipate internal funding will provide a majority of funding in 2022.

Patient co-pays and out of pocket payments drop, but not as significantly: from 47% to 33%. This tracks with the direction of recent federal policies, which foreshadow expanded reimbursement for telehealth services, but have left some thinking that more reimbursement is necessary to shift payment away from patients and health systems.

Which two sources do you expect will provide the majority of funding for your telehealth care delivery services in 2019? And three years from now?



Telehealth

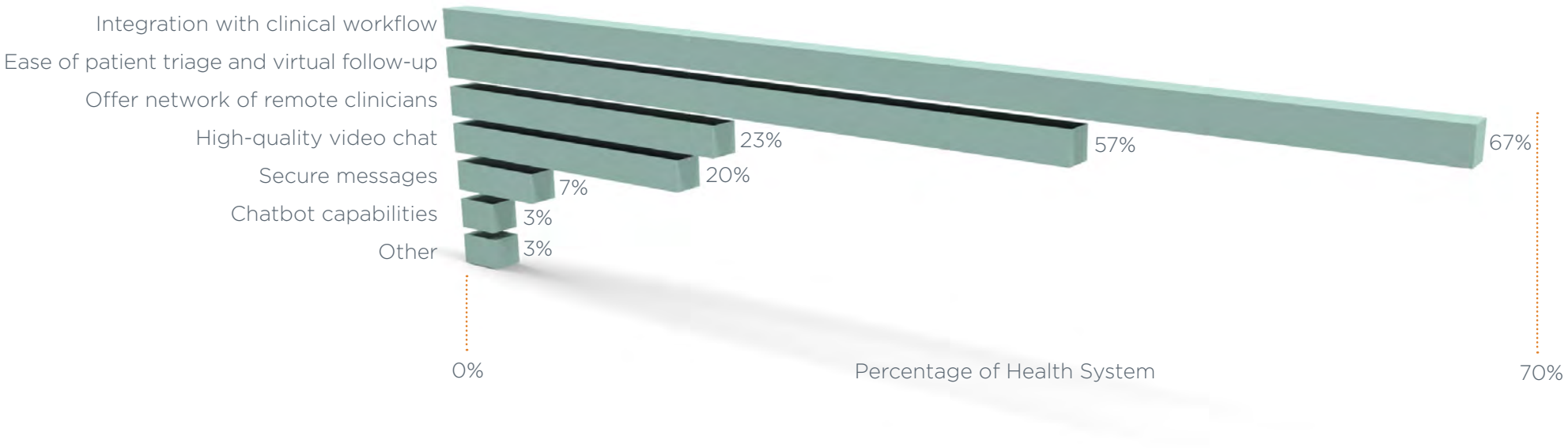
TECHNOLOGY PRIORITIES

Workflow Integration is Top Feature

Health systems commonly leverage external vendors for the technology solutions necessary to provide telehealth services, while utilizing their own physicians or clinicians to deliver services. When considering a telehealth technology system, health systems' top priorities include integration with the clinical workflow (67% of respondents) and ease of patient triage and virtual follow-up (57%). Lower priorities for technology features are high-quality video chat, secure messaging and chatbot capabilities.

As many health systems use their own physicians to deliver telehealth services, solutions that make care delivery seamless for providers and encourage physician adoption are highly valued. Due to this focus, in 2017 the majority (71%) of health systems reported clinicians were supportive of telehealth services.

What are your top priorities in a telehealth technology system? (Select up to two)



Preparing for the Future

Despite minimal reimbursement for telehealth services at many health systems, most organizations are committed to implementing telehealth. Health systems report that a lack of reimbursement is a challenge and has moderately slowed their pace of adoption, though other driving factors have prompted health systems to continue developing and implementing additional telehealth services.

These factors include increasing access, leveraging specialty services across the broader network, and meeting consumer demand. "Consumers want it. When we talk to our customers, they say they want access to clinical information 24/7 at their fingertips. They want it to be easy and streamlined," according to a CEO.

> "The greatest value is improved access to care. Remote areas get access to specialty services they wouldn't otherwise have access to."
>
> – CIO

While most health systems have not calculated an ROI for their telehealth services, many consider developing the patient connections and the associated potential downstream revenue as a proxy ROI. Additionally, telehealth can be viewed as a cost saving initiative as these services can help prevent unnecessary visits or admissions, freeing up physician time to manage patients with more serious conditions.

> "The ROI that we see from telehealth is that it provides access to organizations to funnel patients to us. May lead to admissions and downstream revenue. In terms of savings, it allows us to better manage patients that otherwise would have come to the hospital but don't need to. There's an avoidance of unnecessary admissions."
>
> – CMIO

Telehealth

ARTIFICIAL INTELLIGENCE

A.I. could make telehealth more valuable

The commonly hailed benefits of telehealth are convenience for consumers and greater access to care. But artificial intelligence and machine learning tools could bring an additional level of value to telehealth. Analysis of data obtained through telehealth, and specifically remote patient monitoring platforms, may help health systems implement more robust predictive risk modeling and preventative care. In qualitative interviews with executives, we found that some health systems already are harnessing telehealth data to target interventions and prevent readmissions, though most are not yet leveraging advanced tools such as A.I. and machine learning.

> "We are using algorithms to determine highest risk patients and intervene with telemedicine visits at home or in a long-term care facility to decrease the risk of being readmitted. [We are] also using models to understand those patient populations and understand where applying telemedicine might provide the best clinical benefit."
>
> – CMIO

Interoperability

INTRODUCTION:

Need for Innovation Drives Focus on Interoperability

Interoperability has emerged as a key challenge in health care as hospitals and health systems pursue value-based care, consumerism, and other initiatives that require broad sets of data from disparate IT systems. Health system leaders are increasingly realizing that standing up their electronic health record (EHR) systems was only a first step on the path to data-driven health care. The government's Meaningful Use requirements forced health systems to go digital — but it was only a start. To drive meaningful change and promote value, health data should be freed from proprietary IT systems, easily downloaded by patients, and put to work in any number of applications.

Consider that CMS this year renamed the Meaningful Use program as Promoting Interoperability. CMS Administrator Seema Verma said the name change reflected changes to the program to reduce the burden on providers and "to ensure the health care system puts patients first."

Bringing interoperability to health data also is a key to innovation in the health care space, which has been stagnant compared to many other industries when it comes to providing consumer-friendly tools and information. It is likely not a coincidence that interoperability was "Top of Mind" for executives in this year's survey, given that large technology companies from outside the health care industry are showing interest in the space. These companies, such as Apple, Amazon, and Google, have dominated other industries by employing data and a consumer-focused approach. Apple, for instance, launched its Health Record app which gives patients the ability to view all their medical records in one place from multiple participating health systems.

As the health care industry continues to evolve, provider health systems are having to think more creatively about their strategies in order to remain successful. In this section of the report, we explore how a lack of interoperability may be slowing or stifling innovation at health systems, the sentiment of health leaders toward outside disrupters, and the role of the cloud in the future of health IT.

> "They are new competitors that look very different from traditional health care competitors. They are better in their space and can catch up quickly. Current stakeholders are resistant to change. If we're slow and dodgy we're going to get lapped."
>
> **– CEO**

Interoperability

KEY FINDINGS

A lack of interoperability has made it more difficult for health systems to address certain key priorities, most commonly improved efficiency / cost reduction, and advanced analytics

- Additionally, executives report challenges addressing care gap closure, longitudinal patient data, and integration with non-owned partners

61% of respondents said the use of a major EHR system was not stifling digital innovation at their health system

- However, in qualitative interviews, several executives said an EHR was limiting their ability to innovate by locking them into a single vendor's products

70% of informatics executives are "somewhat concerned" about Big Tech companies, such as Apple, Amazon, and Google, entering the health care space

- 10% are very concerned and 17% are not worried at all

A majority of health care data is expected to be stored in on-premises data centers (20%) or hybrid / private cloud (60%) in the next three years

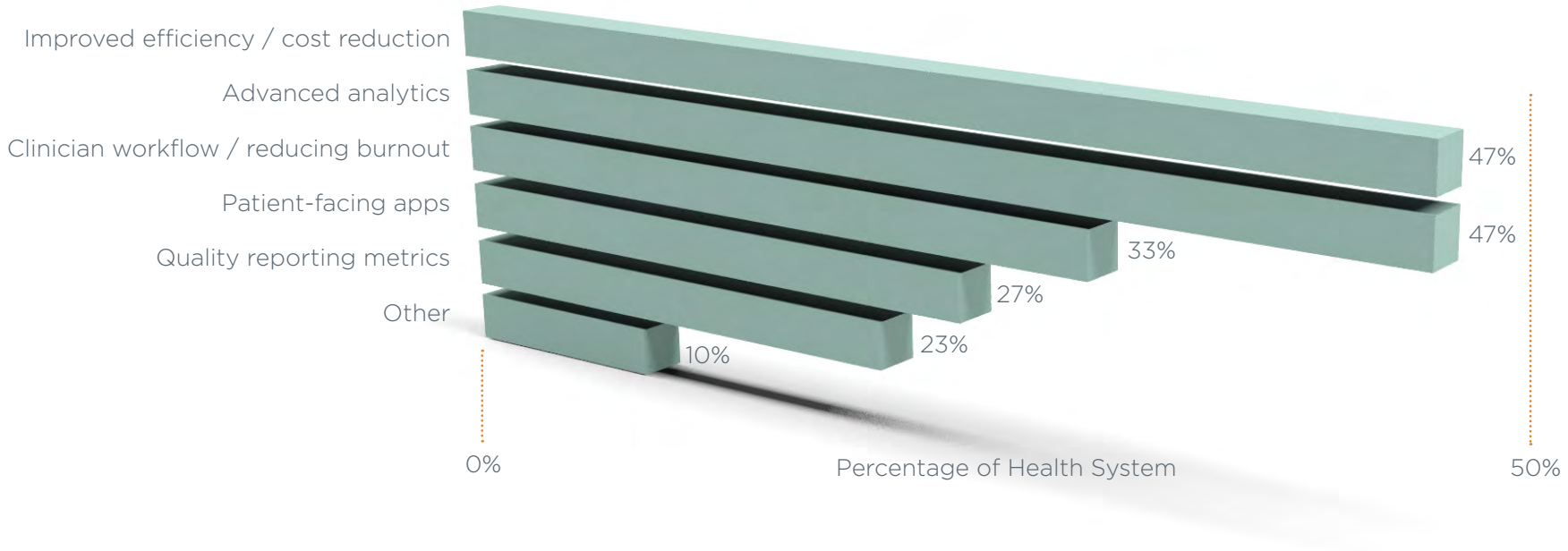
- 10% said they anticipate storing health data in a public cloud

IT Priorities Hampered

The inability of health systems to easily exchange data among various health IT systems has made it more difficult to address certain IT priorities that are key to the future of health care. When asked to identify which IT priorities were hampered by a lack of interoperability, the top choices of respondents were improved efficiency / cost reduction and implementation of advanced analytics. In the "other" category, respondents included closing the care gap, collecting longitudinal patient data, and integration with non-owned partners.

When health systems are unable to bring all their data together in a standardized form, it is challenging to employ advanced analytics that could promote network integration, improve efficiency, find cost reductions, and deliver better patient care. According to one CIO, "[Without interoperability] the complexity of developing and scaling a clinically integrated network is increased and the speed of scaling is impaired."

What key priorities is your organization unable to address because of a lack of interoperability? (Select all that apply)



INTEROPERABILITY CHALLENGES

One EHR Not Practical

Most health systems have not quantified the impact of poor interoperability on their organization, although respondents recognized the significance of the issue. Health systems that are on one instance of a single electronic health record (EHR) across their organization report fewer issues with interoperability.

While health systems could try to move to a single EHR, that is likely not practical for many organizations. "We have a split patient record. One instance for ambulatory and another for acute care. In many years of those two instances coexisting side by side, we're not any closer to getting them synchronized and harmonized. We have a specific team of people working through that," according to a CMIO.

> "You don't want your direction and strategy determined by your EHR vendor. Innovation within EHR space has dropped since the passing of HITECH Act. There's been a stifling of innovation since then."
>
> **– CMIO**

Feeling 'Locked In'

In qualitative interviews, executives were more critical of major EHR systems and their impact on innovation. Executives said they agreed that the implementation of a major EHR vendor can stifle innovation due to health systems feeling "locked in" to solutions developed by the system's vendor, which can make it difficult to adopt "best of breed" solutions. "I think the use of a major EHR does stifle innovation to a great deal," a CMIO commented. "Epic and Cerner are incredibly slow to add functionality to systems and poor at listening to user feedback. Both often start a new idea from an engineer's point of view instead of a clinician point of view, which carries through to the final product. That workflow is maintained through the development of product."

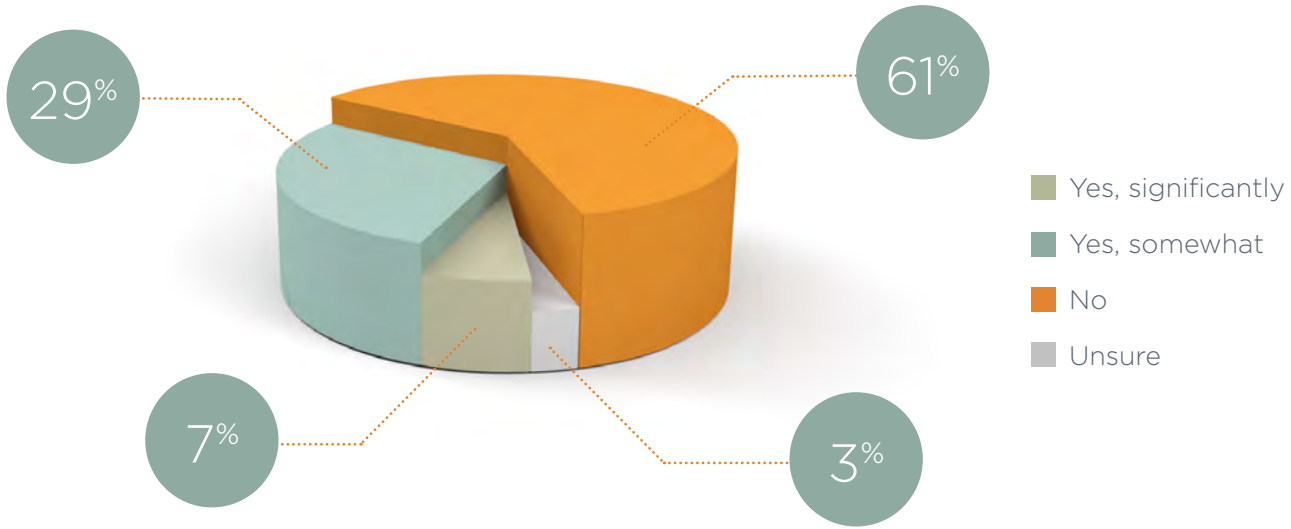
Executives commonly cite the investment that their organization has made in their current EHR and the need for effective integration with their current system as reasoning for this issue. According to another CMIO: "[The EHR] does restrict you in certain ways from doing things in certain ways that may be more innovative. We're not going to invest in anything that's not our EHR vendor anymore. We have to justify the investment. We've already spent $250 million on it. We wanted to do something, but it wasn't on our EHR, so we didn't do it."

A Surprise Finding

A lack of interoperability may be a barrier to achieving certain IT priorities, but when asked in the quantitative survey if their organization's use of major vendor EHRs was stifling innovation, 61% of respondents said "no." This was a surprising finding that appeared to conflict with the comments provided by executives in the qualitative interviews (page 28). There also may be some hesitance on the part of informatics executives to admit problems with infrastructure their health systems have spent millions of dollars to stand up.

Meanwhile, more than one-third (36%) of health system executives who responded to the quantitative survey said they believed their organization's use of a major EHR system either significantly (7%) or somewhat (29%) stifled innovation. As interoperability and integration are high priorities for health systems, the use of a major EHR may prevent an organization from implementing "best of breed" technology solutions.

Do you believe your organization's use of a major Electronic Health Record system stifles innovation at your organization?



Concern Over Outside Disruption

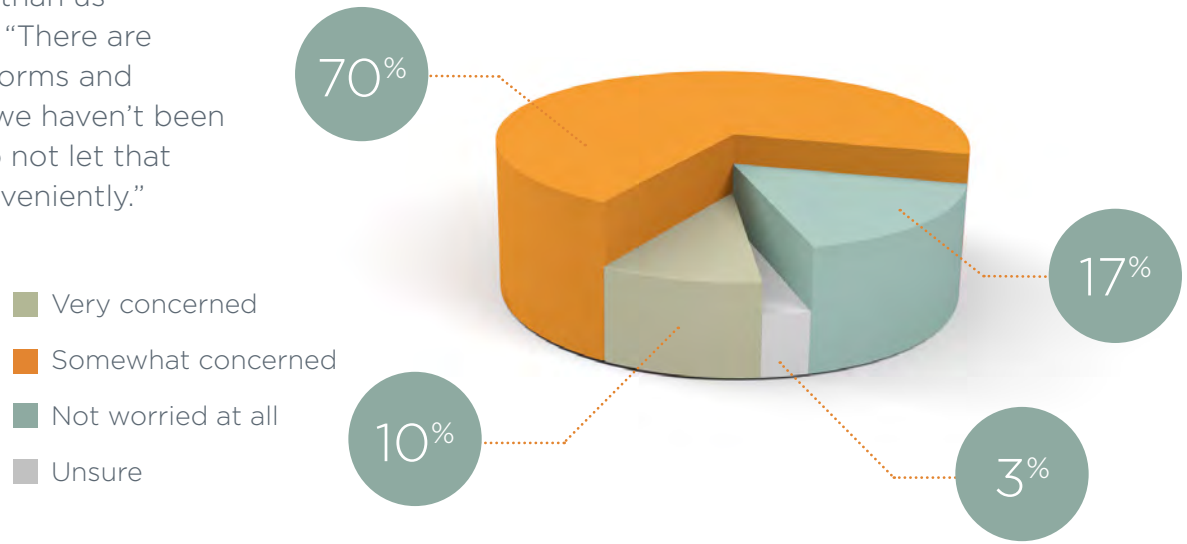
News reports abound on the latest moves by Apple, Amazon, Google, and other "Big Tech" companies entering the health care space. With a focus on consumers, a mastery of data and analytics, and a history of disrupting other industries, the conventional wisdom indicates that incumbent health systems should be worried. The quantitative survey bore that out. A majority of executives (70%) were "somewhat concerned" and 10% were very concerned.

Among health system executives, an overarching concern about technology companies entering the health care space focused on their ability to offer a better consumer experience — an area where many health systems have been subpar. "The biggest threat is if these companies get between us and the end consumer. If there is a platform regulated and controlled by someone other than us — that makes us nervous," a CEO commented. "There are many places where some of these new platforms and conveniences can and will likely succeed — we haven't been good in this space. Going to try very hard to not let that happen and deliver our own capabilities conveniently."

Price Transparency is a Risk

There also is concern that this disruptive competition would force health systems to more rapidly adapt their business models than they are prepared to do. Executives cited concerns over "Big Tech" forcing price transparency before health systems are ready to justify their pricing models. Revealing the current variability in pricing within organizations could lead to consumer confusion and distrust. "One of the bigger challenges is all this activity will drive cost transparency and move us from the traditional business model," a CIO said. "We will be driven to truly understand costs and get a handle on pricing services."

How concerned is your organization about "Big Tech" companies (Apple/Amazon/Google/etc.) entering the health care space?



Not All Reactions Negative

Health systems also see significant opportunity with the entry of new consumer-focused players into health care. Areas such as supply chain, pharmacy, data analytics, and consumerism could benefit significantly from solutions offered by outsiders. Health system executives said they recognized they would be forced to think more creatively to solve problems and redesign care delivery as "Big Tech" companies disrupt the current model. "These are expert technology companies and expert consumer companies. We are reaching out to them and having conversations with multiple companies. Is it helpful for them to partner with large health systems in key markets? If so, what does that look like? They almost universally have interest," a CEO said.

Potential for Partnerships

Additionally, many health system executives see opportunity to partner with these companies and work together to transform the health care industry. Reflective of the potential changes and opportunities health systems see with the entrance of "Big Tech," many executives see the future of health IT in areas that will help streamline provider workflows, leveraging the vast amounts of data generated through analytics, and implementing consumer-focused services such as precision medicine. "I think it's all great news. Especially with companies like Amazon. They can help us solve bigger issues such as supply chain costs," a CIO commented.

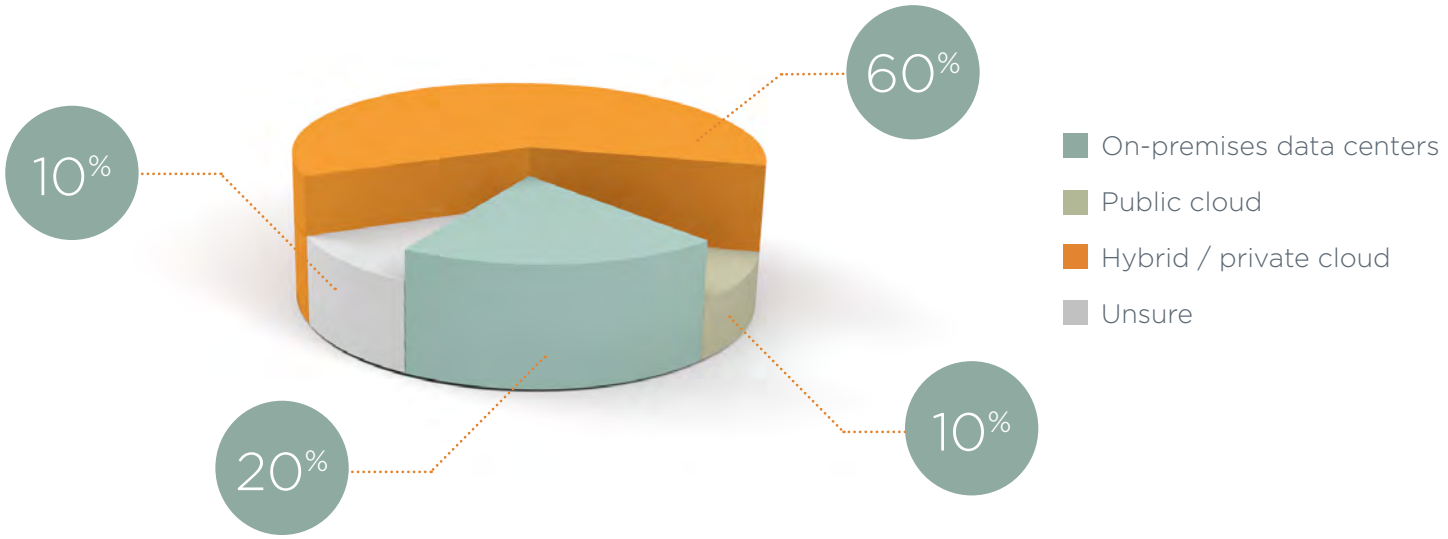
> "I am regularly disappointed in the industry conversations on this topic. The way my colleagues talk it almost feels like [providers are] just doomed. Instead we are approaching this aggressively with a great deal of energy and excitement."
>
> **– CEO**

Few Moving to Cloud

With health systems' concerned about protecting health data and recognizing substantial investment in on-premises data centers, many organizations appear hesitant about moving to the cloud for storage of health care data. Accordingly, a majority of responding health systems expect to store a majority of health care data in on-premises data centers or a hybrid / private cloud in the next three years. Few health systems (10% of respondents) anticipated storing health data in a public cloud in the next three years.

While security is a concern for many health systems, most health system executives realize movement to the cloud is inevitable due to the impracticality of storing the vast amounts of data collected in on-premises data centers. "There are real concerns and a need for understanding all around security, but it's where we're headed in the next five years. We can't keep up with all that storage especially as IT resources get more streamlined," a CMIO said.

Where do you expect the majority of your organization's health care data to be stored in the next three years?



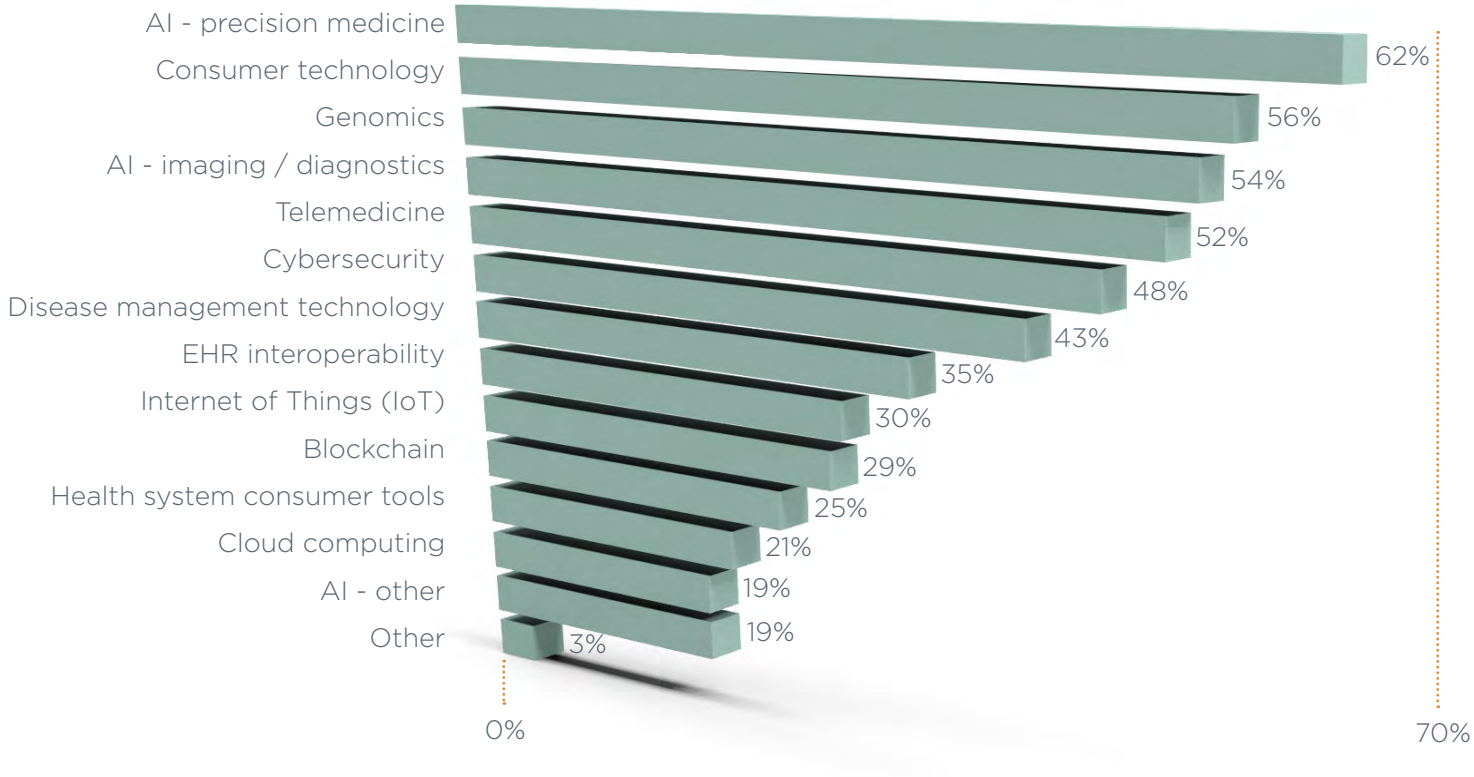
Looking Ahead

TOP OF MIND FIVE YEARS FROM NOW

Artificial intelligence, consumer technology, and genomics jump to the top of the list when health system IT executives think about the technologies that will have the most impact on health care in five years. While these technologies command a large share of health IT media attention, it is clear from the Top of Mind findings that many health IT executives believe the impact of these advanced solutions will be further down the road when compared to the more pressing concerns of cybersecurity, telehealth and interoperability.

Yet technology is evolving quickly. Solutions that seem far away one year can offer a very real use case the next. As one CNIO said: "The technology is moving so fast that it is hard to predict five years out. I would not have picked some of these for 2019 one year ago."

Which five categories of health IT do you anticipate will have the most impact on health systems five years from now?



About the Authors

Center for Connected Medicine

The Center for Connected Medicine (CCM) is a gathering place where those seeking to drive improvements in health care through technology come to connect and inspire each other, both in the real and digital worlds. The CCM, jointly operated by GE Healthcare, Nokia, and UPMC, connects and inspires leaders and innovators to join the CCM community by cultivating thought-leadership activities, creating a relevant content hub, and fostering trusted relationships through exclusive events. Learn more at www.connectedmed.com.

Center for Connected Medicine

NOKIA UPMC

The Health Management Academy

The Health Management Academy (The Academy) is a membership organization exclusively for executives from the country's Top-100 Health Systems and most innovative healthcare companies. The Academy's learning model identifies top priorities of health system leaders; develops rich content based on those priorities; and addresses them by convening members to exchange ideas, best practices, and information. The Academy is the definitive trusted source for peer-to-peer learning in healthcare delivery with a material record of research and policy analysis. Offerings include C-suite executive peer forums, issues-based collaboratives, leadership development programs, research, advisory, and media services. The Academy is an accredited CE provider. More information is available at www.academynet.com.

The Academy
The Health Management Academy

View more health IT content from the CCM at www.connectedmed.com

@connectedmed

#TopOfMind2019

Center for **Connected** Medicine

U.S. Steel Tower, 60th floor
600 Grant Street
Pittsburgh, PA 15219