Survey Results

The State of Patient Identity Management

Do You Have the Right Authentication Measures in Place to Prevent Patient Identity Theft?

LexisNexis® RISK SOLUTIONS

Health Care

iSMG INFORMATION SECURITY MEDIA GROUP

The State of Patient Identity Management

Tom Field
Senior Vice President, Editorial

As part of healthcare's digital transformation, payers and providers alike have rolled out patient portals and telemedicine platforms to increase access to care, improve patient participation and decrease healthcare administrative costs.

How secure are these portals? What types of authentication protocols are used to verify patient identities during login and for transactions? Are data analytics employed to predict patterns of behavior and identify potential medical identity fraud?

These are among the questions tackled in this State of Patient Identity Management survey. Among the results: Eighty-eight percent of healthcare entities have rolled out or have in the works an online patient portal, and 58 percent believe the cybersecurity of their portal is above average or superior when compared to other patient portals they have seen.

Yet, when asked about their level of confidence in their current authentication methods to prevent unauthorized access to patient information via these portals:

- Only 50 percent are confident they have the necessary controls in place.
- Just under two-thirds have rolled out multifactor authentication to prevent unauthorized access.

Aimed at identifying whether healthcare organizations have the right authentication measures in place to prevent patient identity theft, the study draws upon responses from about 100 participants to determine:

- Current best practices in patient identity management;
- How organizations compare to these standards;
- Which tools, skills and partnerships healthcare entities are investing in to improve patient identity management in 2019 and beyond.

Read on for full survey results, as well as expert analysis of how to put this information to use to improve how your organization approaches authentication.

Best,

Tom Field
Senior Vice President, Editorial
Information Security Media Group
tfield@ismg.io

This survey, conducted online in the spring of 2019, generated about 100 responses from U.S. healthcare entities, including hospitals, physician group practices as well as health insurance plans/payers.

By the Numbers

Some statistics that jump out from this study:

88%

of healthcare entities have rolled out or have in the works an online patient portal.

58%

believe the cybersecurity of their portal is above average or superior when compared to other patient portals they have seen.

50%

are confident they have the necessary controls in place to prevent unauthorized access to patient information.

The Baseline

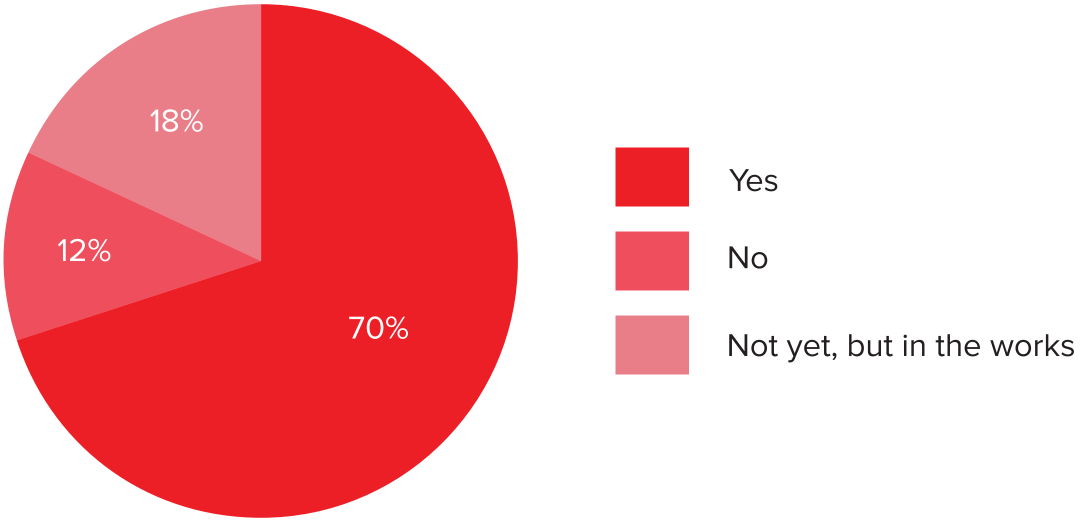
In this opening section of the report, the goal is to establish where healthcare organizations are today in terms of 1) rolling out online patient portals, and 2) the relative security of those portals.

Key statistics gathered from the respondents:

- Only 12 percent do not have portals, nor do they have plans to roll them out.
- 56 percent say the biggest inhibiting factor for portal adoption is that patients are not comfortable with the technology.

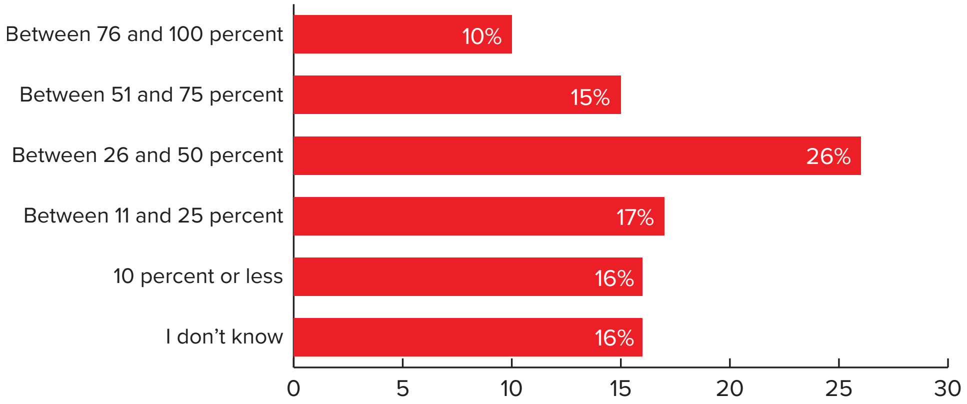
Read on for a clearer picture of how respondent organizations currently approach portals and cybersecurity.

As part of your organization's digital transformation, have you rolled out an online patient portal?



Amidst widespread digital transformation, few healthcare entities have not entered the patient portal realm. In fact, 88 percent of survey respondents say they either have such a portal now or have one in the works.

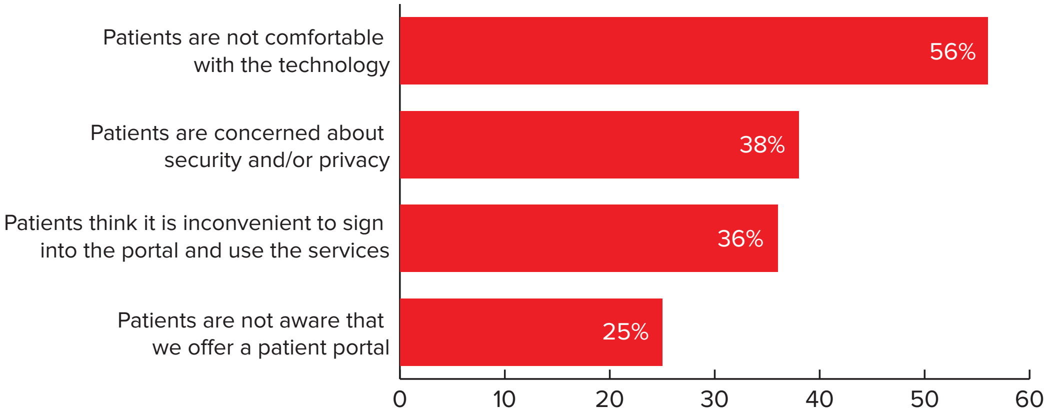
If you answered “yes” to question 1, how would you describe the adoption rate for this patient portal?



As for adoption rates, they are all over the map. Only one-quarter of respondents say that a majority of their user population takes advantage of the portal. Only 16 percent of respondents say that fewer than 10 percent of their patient populations use the portals, while 17 percent say usage is between 11-25 percent, and 26 percent tag it at between 26-50 percent.

Ten percent of respondents say they see 76-100 percent usage.

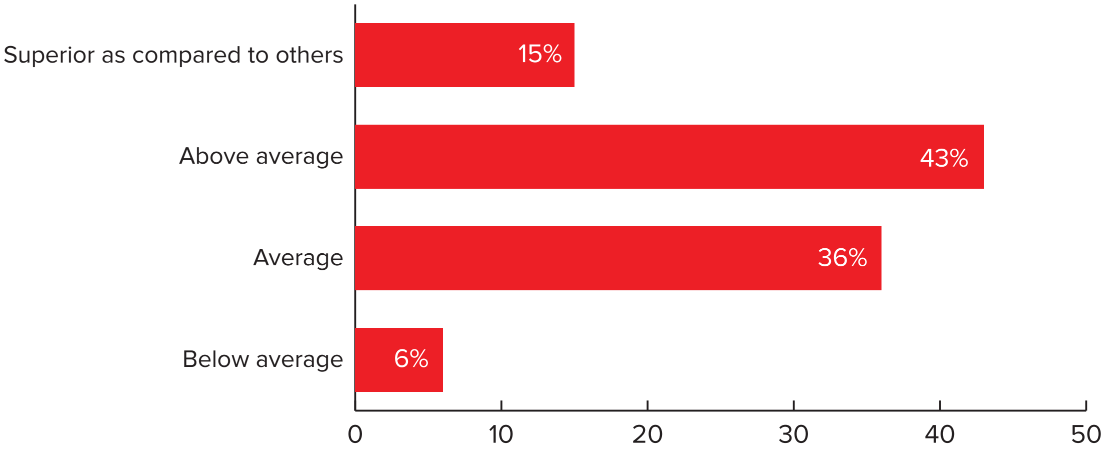
What factors do you believe inhibit greater adoption of your patient portal? (choose all that apply)



Respondents believe the top factor inhibiting portal use is that patients are not comfortable with the technology (56 percent response). Other top factors:

- Patients are concerned about security and/or privacy: 38 percent;
- Patients think it is inconvenient to sign into the portal and use the services: 36 percent;
- Patients are not aware that we offer a patient portal: 25 percent.

In comparison to other patient portals you have seen, how do you rate the overall cybersecurity of your own portal?



It is noteworthy that survey respondents have a high opinion of the cybersecurity of their portals. Asked how they rate their overall cybersecurity in comparison to other portals they have seen, 58 percent say their own are above average or superior.

Meanwhile, 36 percent consider their cybersecurity average by comparison, while 6 percent mark their efforts as below average.

The next section of the report reviews patient identity management, which further explores whether respondents' cybersecurity optimism is justified.

It is noteworthy that survey respondents have a high opinion of the cybersecurity of their portals.

Patient Identity Management

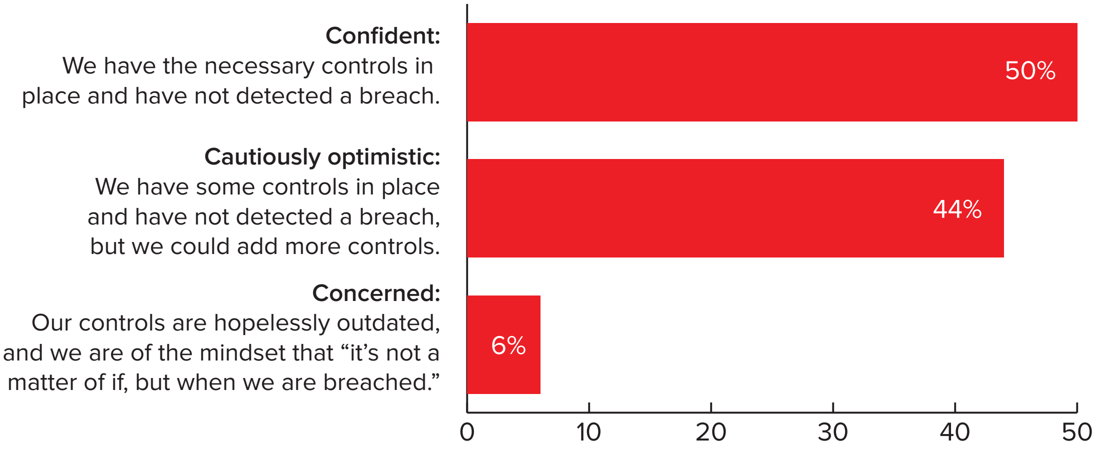
How well are healthcare organizations protecting patient information within their care? The answer is good news/bad news:

Good News: Only 1 percent of respondents say their patient information has been breached in the past year.

Bad News: Not even two-thirds of organizations deploy multifactor authentication to control access to this data.

Full results are below.

What is your level of confidence in your current authentication measures to prevent unauthorized access to patient information via your telemedicine platforms or patient portal?

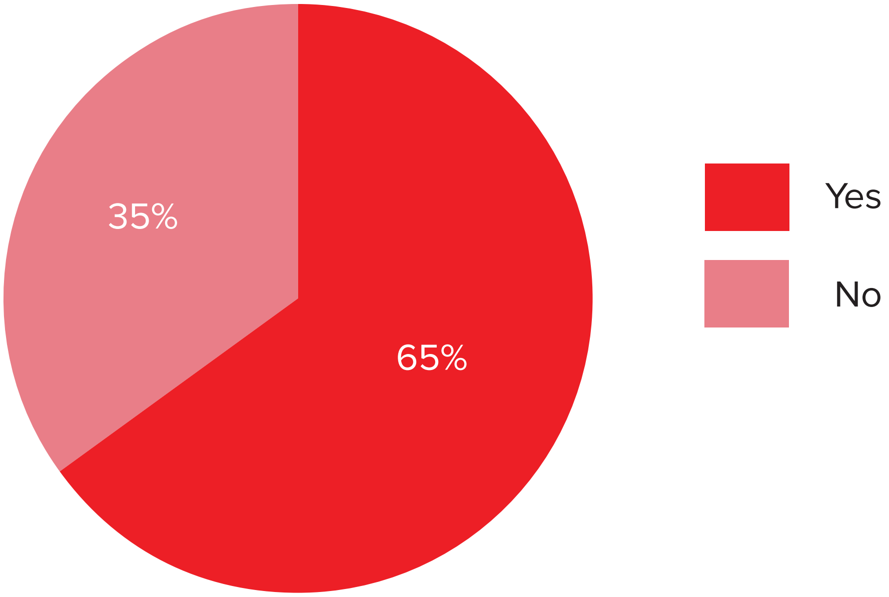


With breach numbers so low, security leaders have relatively high confidence in their authentication measures. Asked to describe that level of confidence, 50 percent say they are confident they have the necessary controls in place and have not detected a breach.

Meanwhile, 44 percent describe themselves as cautiously optimistic – they have some controls in place and have not detected a breach, but could add more controls.

Only 6 percent describe themselves as concerned, meaning their controls are hopelessly outdated, and they are of the mindset that "it's not a matter of if, but when we are breached."

Does your organization deploy multifactor authentication to prevent unauthorized access to patient information via your telemedicine platforms or patient portal?

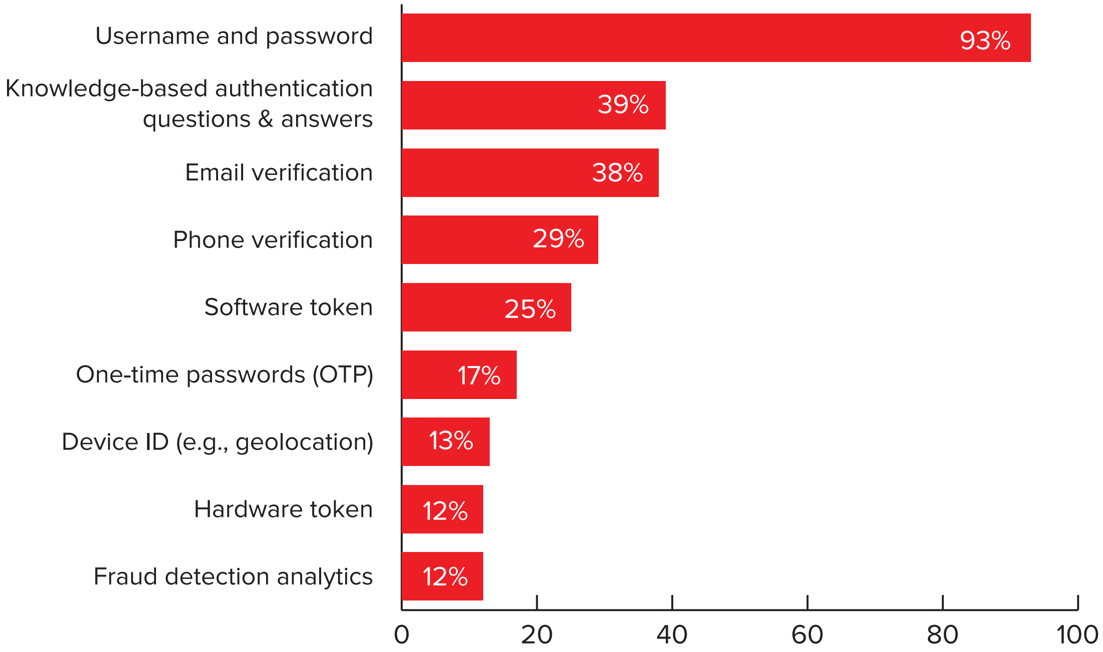


Despite this confidence in authentication, though, only 65 percent of respondents deploy multifactor authentication – considered a mere baseline control by many organizations today - to prevent unauthorized access to patient information via their telemedicine platforms or patient portal.

Given that MFA is a recommendation by virtually every cybersecurity guidance, it is surprising to see 35 percent of respondents have not deployed the control.

> ***Given that MFA is a recommendation by virtually every cybersecurity guidance, it is surprising to see 35 percent of respondents have not deployed the control.***

What methods of authentication do you currently use to control access to this patient information? (Choose all that apply)



What forms of authentication are organizations predominantly deploying? The traditional ones, namely:

- Username and password: 93 percent;
- Knowledge-based authentication questions and answers, 39 percent;
- Email verification, 38 percent.

Later, in the analysis section of this report, Erin Benson of survey sponsor LexisNexis Risk Solutions Health Care weighs in on the forms of authentication that healthcare entities are – and are not – currently using.

Next, the report examines the patient identity management priorities that survey respondents will focus on in the year ahead.

The Year Ahead: Patient Identity Management Priorities

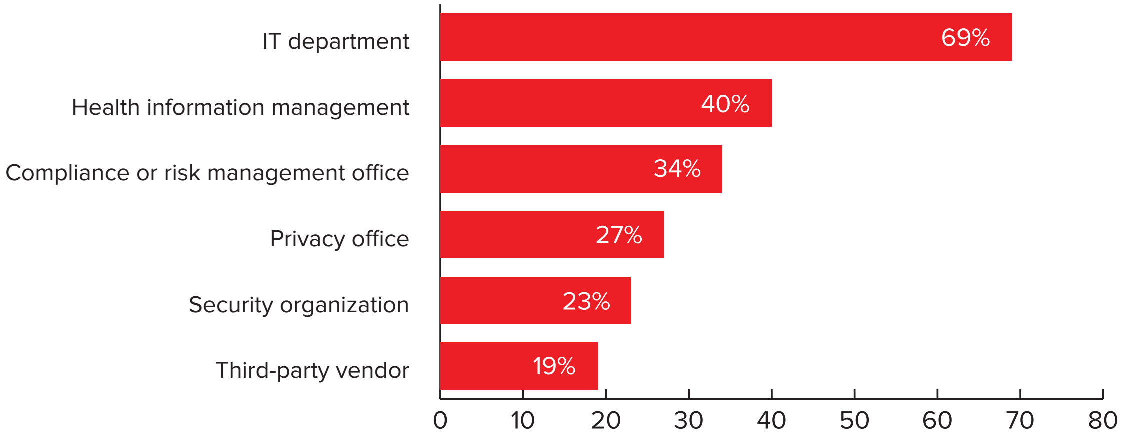
As healthcare organizations look ahead, they start with encouraging news: 95 percent of them will have the same or increased funding for improving patient identity management.

The main focus of those funds:

- Rollout or complete patient portal;
- Improve multifactor authentication for login.

Read on for details about planned investments.

Who has responsibility for Patient Identity Management within your organization? (Choose all that apply)

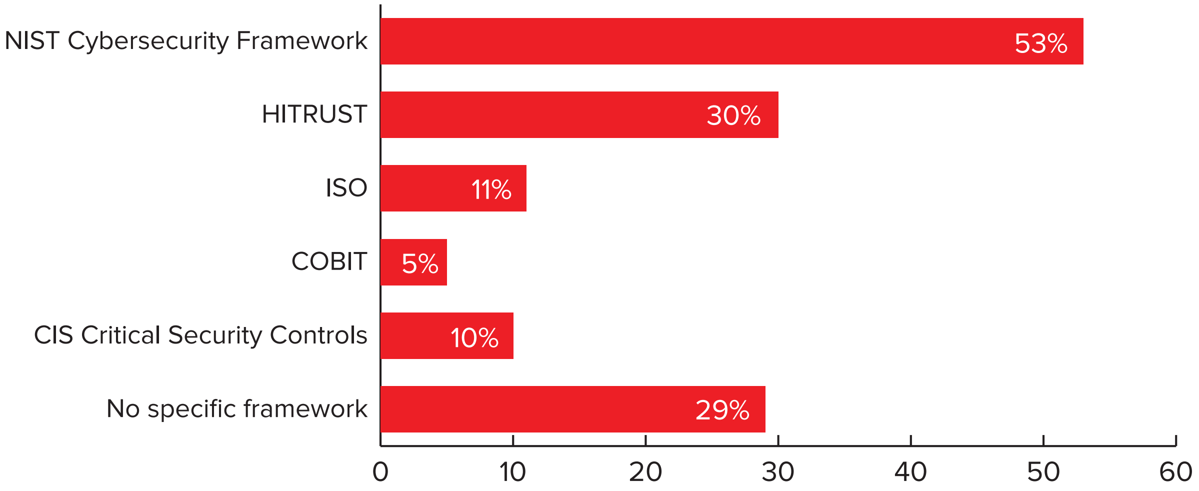


When it comes to making decisions about patient identity management systems, the IT department has the reins in 69 percent of organizations, followed by health information management offices at 40 percent and compliance/risk management office at 34 percent.

Privacy offices come in fourth at 27 percent, followed by security at 23 percent.

When it comes to making decisions about patient identity management systems, the IT department has the reins in 69 percent of organizations.

As you move forward in 2019, which (if any) cybersecurity framework will guide the decisions you make about patient identity management? (Choose all that apply)



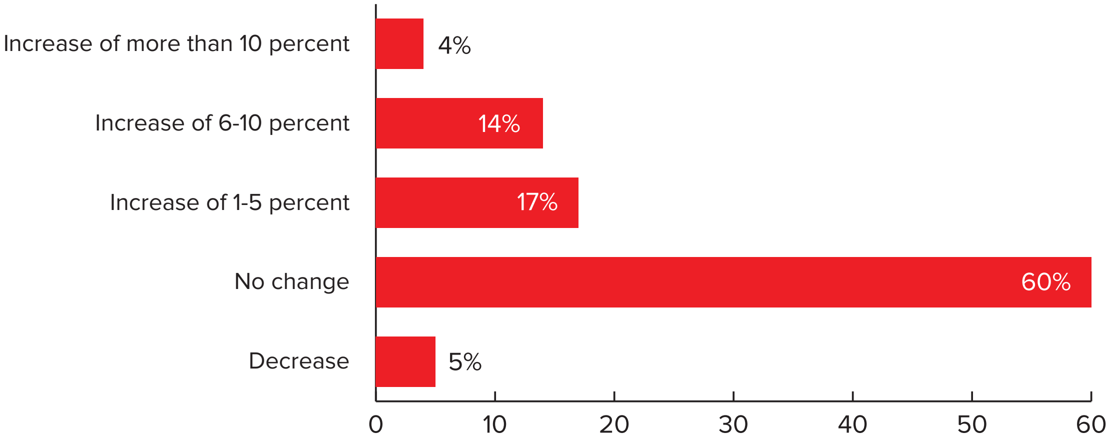
To adopt best practices and industry standards, healthcare organizations can use many frameworks. HITRUST, ISO, COBIT and NIST are the frontrunners.

But when asked which framework (if any) will guide their decisions about patient identity management, nearly one-third of respondents said “no specific framework.”

Among other responses:

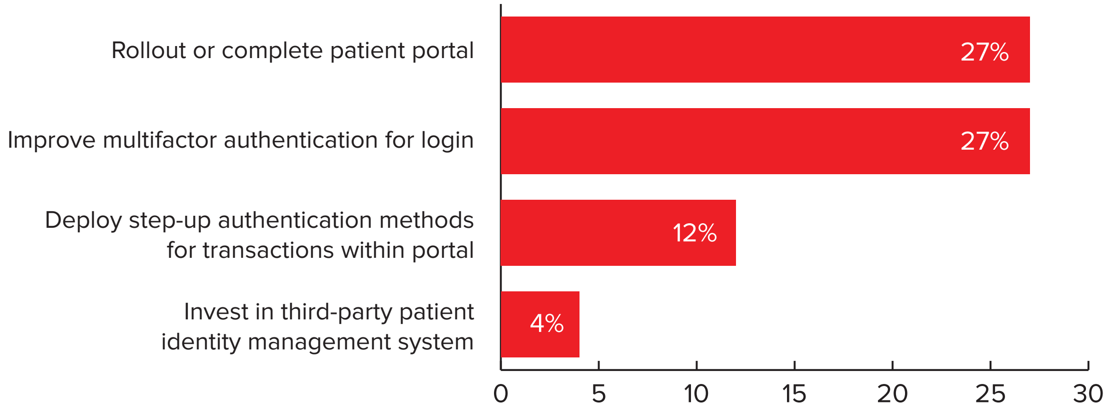
- NIST Cybersecurity Framework – 53 percent;
- HITRUST – 30 percent.

How do you expect your budget for improving patient identity management to change in 2019?



In terms of budgeting for patient identity management, 95 percent of organizations expect to see the same or more funding in the year ahead, with 31 percent expecting increases between 1 and 10 percent.

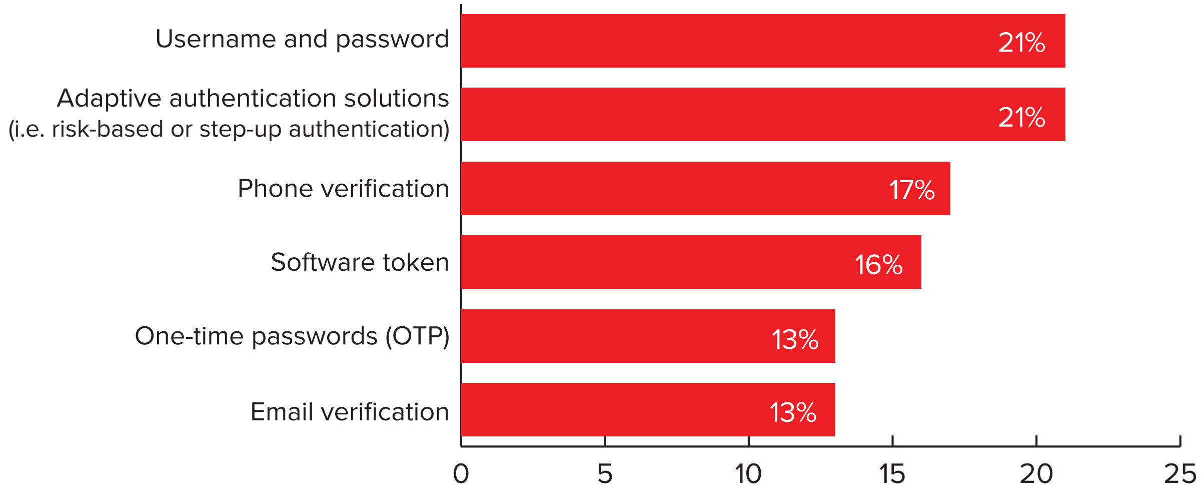
What will be your primary patient identity management investment priority in 2019?
(Top responses shown here)



Asked how they will prioritize those investments, respondents had many varied answers. But the top two responses (cited equally by 27 percent):

- Rollout or complete patient portal;
- Improve multifactor authentication for login.

Which new methods of authentication do you plan to invest in over 2019? (Choose all that apply)
(Top responses shown here)



And as for new authentication controls for deployment, respondents prioritize these for investment:

- User name and password: 21 percent;
- Adaptive authentication solutions (i.e. risk-based or step-up authentication): 21 percent;
- Phone verification: 17 percent.

In the next and final sections of this report, the findings will be summarized in a set of conclusions, then analyzed by Erin Benson of LexisNexis with an eye toward what the results mean to healthcare entities and how they can best be put to use.

Conclusions

Reflecting on the survey results, three clear conclusions emerge:

Traditional Authentication Methods Are Insufficient

A majority of respondents may feel the cybersecurity of their patient portals is above average or superior when compared to others in the industry. But when not even two-thirds of these organizations have deployed multifactor authentication to prevent unauthorized access … they are just a data breach waiting to happen. Users are easily phished, and there are too many legitimate credentials in the marketplace today as a result of so many high-profile breaches. Traditional usernames and passwords are no longer a barrier; they are an entry point. They cannot be relied upon for any confident level of cybersecurity.

MFA Is Only Table Stakes

And because traditional authentication controls have failed so badly, multifactor authentication today is the bare minimum of what organizations must employ to prevent unauthorized access to critical data. The most secure organizations rely on a variety of controls – ranging from knowledge-based questions and one-time passwords to device analytics and biometrics – to authenticate users based on the criticality of transactions. The more sensitive that request, the more stringent the authentication technique.

Cybersecurity Must Co-Exist With Ease of Use

It isn't a question of a frictionless customer experience or secure access to critical systems. It is a matter of "How can you maintain both?" Healthcare organizations are under pressure to give patients and partners access to digital health records, and at the same time secure them. To do so requires a balance of layered security controls. Entities must make it easy for patients and partners to access records, but then require step-up authentication for transactions such as payments and data transfers. It requires knowing users, benchmarking typical behavior and flagging the anomalies.

In the survey analysis that follows, Erin Benson of LexisNexis Risk Solutions Health Care discusses some of the ways healthcare entities seek to create this balance between cybersecurity and frictionless user experience.

The State of Patient Identity Management

Insights from Erin Benson of LexisNexis Risk Solutions Health Care

Erin Benson

Ms. Benson serves LexisNexis Health Care as Director, Market Planning. Her focus is on the development and execution of strategic planning for Member Identity and Socioeconomic Determinants of Health solutions. Prior to joining LexisNexis, Ms. Benson was a Senior Consultant at Deloitte Consulting. She holds a Bachelor's and Master's degree in Human and Organizational Development from Vanderbilt University and an MBA in Strategy and Management from Duke University, The Fuqua School of Business.

NOTE: In preparation of this report, ISMG's Tom Field interviewed Erin Benson of survey sponsor LexisNexis Risk Solutions Health Care about the survey results and what they mean for healthcare organizations. This is an excerpt of that conversation.

Survey Says

TOM FIELD: Erin, you've had the opportunity to look at the survey results that we've just put together. What's your initial reaction?

ERIN BENSON: The thing that really stood out was that there's an overconfidence in the preparedness around cybersecurity compared to the number of breaches that we're seeing in the marketplace actually happening.

So, for example, in the survey, 58 percent believe the cybersecurity of their portal is above average or superior when compared to other patient portals. But there were 503 U. S. healthcare breaches in 2018. And 88 percent of all ransomware attacks were against healthcare organizations. So there's a lot of evidence to the contrary to say that even if a healthcare organization is above average compared to its peers, we have not come far enough in terms of protecting patient data.

'False Confidence'

FIELD: In your experience with these healthcare organizations, what bolsters this false confidence in the security of their portals?

BENSON: I honestly am not sure what is bolstering that because all the evidence in the industry would point to the opposite. We're seeing healthcare organizations being targeted more and more all the time because healthcare data has not been commoditized in the black market, and it has become a primary target for hackers. With the shift to digital records, there's been so much focus on getting infrastructure in place … but that cybersecurity still needs to get stronger.

Traditional Controls

FIELD: Why are organizations still so bound by tradition and so resistant to implementing something like multifactor authentication?

BENSON: I think that's changing. I actually do think that multifactor authentication is becoming more accepted and that we are going to see it start to increase in terms of importance.

When we spoke with CIOs through the CHIME organization earlier this year, they acknowledged that multifactor is becoming the norm and it's what everyone should be doing because every layer of defense covers more holes in security. We also saw that there was an increase in interest not only to validate patient identities as they log into portals, but they're also interested in being able to validate employees and vendors as they're logging in. CIOs are taking a holistic view of a system and making sure that protections are in place anywhere where anyone can log in.

Multiple Security Frameworks

FIELD: Nearly one-third of our respondents said that they didn't adhere to a specific cybersecurity framework. Did that surprise you?

BENSON: It really didn't surprise me that much. The NIST Cybersecurity Framework tends to be the one that's most often used, and we did see 53 percent of respondents saying that they use it in some form. It's a set of guidelines, so typically what we see in organizations is that they use parts of different security frameworks in order to piece together what they feel will work best for their organization. As the healthcare industry is being encouraged to focus on making patient records available via API, I expect more standardization of the security frameworks and protocols to develop.

> *"I actually do think that multifactor authentication is becoming more accepted and that we are going to see it start to increase in terms of importance."*

Risks to Patient Identity

FIELD: What do you see as the biggest risk factors to patient identity management?

BENSON: The foundation of managing security risk is having clean records, so that as you're managing the patient's data and identity, it's all tying back to one golden record. Right now, with the transformation to digital records plus all the interoperability initiatives happening, where healthcare organizations are being encouraged to share records across different organizations and more mergers and acquisitions are bringing data together, we're seeing a lot of duplicate records being created within systems. And it's hard to protect that data when you're not even sure what data you have. It also causes patients to lose trust in their healthcare organizations when they log in and only get access to part of their records, and it can even be dangerous to not have all of a patient's information in one record if providers are making decisions about their health based on an incomplete file.

By cleaning the data and organizing it so each patient has a single, comprehensive record, healthcare organizations are better able to match that record to the right patient. This alleviates the biggest risk to patient identity management.

After that, we see an increase in bot attacks and ransomware, so all organizations are going to want to add some kind of digital identity assessment to what they're currently doing today.

Security Controls

FIELD: Are there other specific technologies that you recommend organizations investigate as they make their investment plans?

BENSON: There are so many different technologies out there. Every point where you can access the system should have several layers of defense in case one of them doesn't catch every type of fraud. But it's also easy to get overwhelmed with all of the different verification and authentication options.

Different use cases, such as logging in to a system for the first time or making a payment, have different levels of risk. Therefore, it is important to pick the right multi-factor authentication tools to match the risk level – letting the real users quickly complete their tasks while the fraudsters face a lot of friction and are not permitted to proceed. Possible tools can include anything from facial recognition to voice biometrics to device and digital identity assessments to more traditional methods such as knowledge-based authentication. Which tools you should use depends on what you're trying to accomplish. And that's where a data vendor can come in and help to guide you to the right solutions based on the use case.

LexisNexis Risk Solutions Health Care

FIELD: So, Erin, talk to me about LexisNexis Risk Solutions Health Care. What are you doing specifically to help organizations to improve patient identity management?

BENSON: When organizations come to us looking to better protect patient data or other data on their portals, we talk through their use cases and then put together a multi-factor authentication solution framework around what would work best for their different needs, based on the risk of the data that they're protecting and also their need to find a balance between encouraging patient engagement with the portals and protecting the data from fraud.

We don't want to make it hard for the right people to get access to their data or complete other online transactions. We want that to be as seamless as possible. To do this, we often put low-friction verification and authentication tools up front in the multi-factor authentication workflow where they are not really causing any pain to the user. A lot of the checks are happening behind the scenes. But if any of those turn out to be suspicious, then what we can do is layer in higher-friction verification and

> *“We help to find that balance between encouraging patient engagement while also protecting their data.”*

authentication checks in the later steps of the process. After all, we want fraudsters to feel the friction and drop out of the identity verification process.

Our goal is to encourage patient engagement with the portal while also protecting their data, and we do this by matching the right multi-factor authentication solutions to the right places in the portal workflow.

Putting the Survey to Work

FIELD: How do you recommend that the audience put these survey results and insights to work so they can improve patient identity management?

BENSON: I would encourage the audience to look at what the survey results are telling us versus what we're seeing every day in the news and in the industry. Cybersecurity needs to be a top priority, and I hope that what the audience will take away from this is that we still have a long way to go to really protect patient data. Multi-factor authentication is an important step in making these strides, and this survey listed different types of verification and authentication tools to consider. There are a lot of different things that organizations could be exploring when creating their cybersecurity strategy, and hopefully this gives them some ideas of what their peers are doing. ■

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to information security and risk management. Each of our 28 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North AmErina to Southeast Asia; and topics such as data breach prevention, cyber risk assessment and fraud. Our annual global Summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401 • sales@ismg.io

BANK INFO SECURITY® CU INFO SECURITY® Just for Credit Unions GOV INFO SECURITY® HEALTHCARE INFO SECURITY®

infoRisk® TODAY CAREERS INFO SECURITY® ~~Data Breach~~. Prevention. Response. Notification. TODAY CyberEd.io

iSMG
INFORMATION SECURITY
MEDIA GROUP

902 Carnegie Center • Princeton, NJ • 08540 • www.ismg.io