From infrastructure to insights

Top priorities for healthcare leaders in 2019

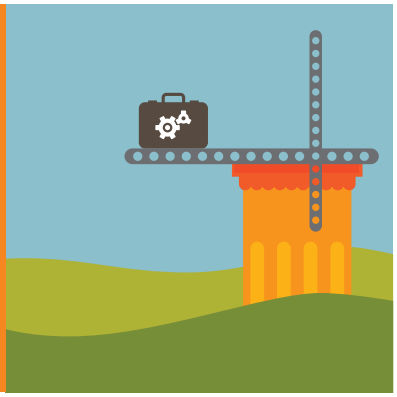
Cybersecurity, interoperability and healthcare consumerism top the list

In its second annual focus group of more than 30 healthcare executives, all members of the College of Healthcare Information Management Executives (CHIME), on top priorities for hospital CIOs and other healthcare technology leaders, LexisNexis® Risk Solutions healthcare business assembled the group to find out what topics they anticipate will demand the majority of their attention in 2019.

If there's one point that participants drove home, it's this: Today's healthcare leaders have a lot on their plates. Managing and leveraging dynamic data for success under value-based payment models, protecting health information in an increasingly mobile environment, and providing patients with an excellent healthcare experience are just the tip of the iceberg.

Overall, executives are less concerned with checking boxes for specific compliance regulations and more concerned with earning—and retaining—patient trust, whether it be by keeping information safe, maintaining accurate and complete records, or providing a personalized and meaningful healthcare experience.

Interestingly, priorities for 2019 differ largely depending on the current phase of EHR deployment. Organizations in the early phase of adoption and upgrades are focused primarily on infrastructure (i.e., interoperability and data security). Once this foundation for secure data input and exchange is laid, priorities shift to data governance and data cleansing—that is, stabilizing the data so it can eventually be used for business intelligence. Organizations in the last phase of deployment have already begun using analytics to gain actionable insights. They're also starting to employ technology to engage patients in an age of healthcare consumerism.



Key priorities

Phase 1
Establishing EHR infrastructure

1. Cybersecurity. Cybersecurity is a major priority, particularly as organizations expand system access to third-party vendors, patients, auditors and others. There's a consensus that up-front investments to protect patient information is paramount.

Participants said they are increasingly using multiple layers of security, including one-time passwords, biometric screenings and knowledge-based authentication. They likened their strategy to that of plugging holes, with each additional security layer plugging more vulnerabilities in their system infrastructure. One challenge? Multiple access points require daily cyberscurity monitoring—and the threats are not just coming from outside the system anymore. Cybersecurity used to mean protecting the perimeter of a system with firewalls, but the increasing sophistication of cybercrime has led the industry to focus more on threat detection from the inside too. Every point where a user can enter a system needs to be appropriately secured.

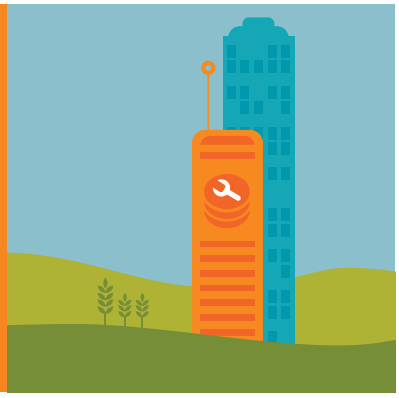
In addition to the financial cost of remediating a significant security breach or event, participants cited several other types of costs they are working to avoid including revenue loss and even reputational harm.

"You lose the patient's confidence in your ability to deliver healthcare," said one participant. "Patients will go somewhere else because they don't trust that you can take care of their data." Patient safety is also jeopardized as providers are unable to access critical information.

Everyone agreed that providers are ultimately the custodians of patient information, and securing that information is the right thing to do regardless of whether they're obligated to do so by virtue of HIPAA.

2. Interoperability. Interoperability remains an ongoing challenge as organizations look for ways to exchange data within healthcare systems and externally with other data partners. However, interoperability isn't only about data exchange. It's also about data consumption and being able to use the data in a meaningful way.

"You can have all the connectivity you want, but if you're not able to deliver that information into the clinical workflow of those who would use it, then you shouldn't even bother," said one participant.



Phase 2
Stabilizing the data

1. Data governance. Participants cited several challenges (e.g., mismatched patients and duplicate records) in terms of ensuring records are current, complete and accurate. Interestingly, most of these executives primarily handle data warehousing and aren't yet responsible for data quality.

However, they acknowledged that a siloed approach to data governance doesn't work. Instead, they're focusing on an enterprise-wide effort that includes significant input from health information management and quality assurance.

2. Patient and provider directories. For these healthcare executives, managing patient directories is highly complex, especially during mergers and acquisitions. They said a national patient identifier would be ideal, but they weren't hopeful that it would actually happen. Still, they agreed that some type of universal patient identifier would support true interoperability across the entire healthcare ecosystem. Maintaining an accurate provider directory also supports more efficient referrals and coordination of care.

Phase 3
Gaining actionable insights

1. Data analytics. Several participants said the ability to data mine and partner with clinical operations is an essential part of surviving and thriving in an era of value-based payments. Analytics allow organizations to risk stratify patients, analyze payer mix and more.

"We're working diligently to ensure we provide the highest quality care at the lowest cost," one participant said. Setting accurate risk adjustment targets requires the ability to analyze data for encounters that span the entire care continuum. One participant called into question the accuracy of these targets, citing a noticeable gap between data the health plan uses to set the targets versus claims data the hospital submits.

Data quality continues to be a barrier even for organizations in this mature phase of EHR employment. "As we're on this data analytics journey, we find that the data integrity is one of the biggest limiting factors and challenges in getting good, accurate insights," said one participant.

2. Patient engagement. During a new age of healthcare consumerism, engaging patients is a strategic initiative for healthcare executives. In addition to offering virtual care and telemedicine options, they're trying to personalize the healthcare experience. They want to give patients the ability to communicate with providers via email, telephone, mobile app, text and web interface. They also want to enhance the user experience by providing interactive—not generic—content via the portal and mobile apps.

There was also talk of patient-owned medical records available in a universal electronic format where patients—not providers—decide who accesses their data. This raises questions such as: Will the record be accurate and up-to-date? Can organizations trust the information, and might it put providers at risk for medical errors? What if patients choose not to share the information? And, will all patients truly be up to the task of managing their own health data? Some said definitely not, especially those who are chronically ill or those without Internet access for example. Others have a different opinion. "We do think this is the future. We're watching what's happening," said one participant.

The takeaways

These days, there are many topics vying for healthcare executives' attention, and the need to break down silos and reach across department lines are the only way organizations can reach their goals. There's also an overarching theme of healthcare consumerism that drives much of what they do. Protecting, sharing and ensuring the accuracy of patient health information in the EHR is about doing what's right for patients—not just complying with a regulation. When organizations take this approach, they gain patient trust and loyalty.

For more information, call 866.396.7703 or visit
risk.lexisnexis.com/healthcare

Health Care

About LexisNexis® Risk Solutions

LexisNexis Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX (LSE: REL/NYSE: RELX), a global provider of information and analytics for professional and business customers across industries. For more information, please visit www.risk.lexisnexis.com and www.relx.com.

Our healthcare solutions combine proprietary analytics, science and technology with the industry's leading sources of provider, member, claims and public records information to improve cost savings, health outcomes, data quality and compliance and minimize exposure to fraud, waste and abuse.