A Clear Vision, But A Long and Winding Road

Healthcare technology leaders reveal progress, priorities and challenges for 2020 in the drive toward richly connected care

LexisNexis® RISK SOLUTIONS | Health Care

We checked in on the state of technology in healthcare. This is what we learned.

In our third annual focus groups of healthcare CIOs, all members of the College of Healthcare Information Management Executives (CHIME), the pulse beats somewhere between **“Bring it on!”** and **“Let’s not get too ahead of ourselves.”**

These director and C-level professionals weighed in on a variety of topics ranging from data privacy to the impact of data on patient care quality.

Setting priorities for a new year and looking back at last year’s progress, conversations about connected healthcare are stirring the imaginations of people both inside and outside of hospital walls. But as global technology behemoths speak of mobile health records, personal health data exchange and wearable monitors, a healthy dose of reality resonates among the people charged with making it happen in the patient care environment.

As one health system IT executive put it: ***“Tech giants are talking about these revolutionary ideas. Meanwhile we’re just trying to make sure we have the correct patient contact information.”***

Indeed, the success of connected care begins with the quality and reliability of patient data. Something care providers of all sizes struggle to maintain.

Data governance was just one discussion point in a conversation that took many turns, always pointing back to the goal of connected care. As technologies evolve and external legislative pressures mount, organizations are putting the “pedal to the metal” on exchanging, integrating and securing data, with varying degrees of progress.

BACK TO BASICS

There's no doubt that connected care is an ambitious goal.

No two patients are alike — and neither is their health status. It takes a complex ecosystem of clinicians, organizations and systems to deliver high quality care to each individual.

Security and privacy have always taken top priority, but high-profile data breaches have put these issues on a very public stage.

At the same time, data-sharing regulations governed by Office of the National Coordinator for Health Information Technology (ONC) are generating concern and conversation. These mandates — meant to empower patients with greater choice and accessibility — threaten the data protections health systems work so hard to maintain.

Patient data is the connective tissue that will make the vision of connected care a reality. But it requires a strong data governance strategy — a cross-functional one — to ensure data is captured, correct and shared only as authorized. IT, business and clinical roles must have a voice in the process and lend their support.

Our focus group indicates that this cultural shift is starting to happen in healthcare organizations.

THE CHANGING ROLE OF THE CIO

This year we heard more about CIO accountability than in previous years.
This group talked about their role in providing the tools necessary to deliver high quality care — and how their knowledge can be leveraged to deliver care more efficiently and cost effectively.

2020 PRIORITIES

This year's focus group revealed strong progress in many areas: implementing EHRs, piloting new methods of care, delicately managing infrastructure through mergers and acquisitions...the list goes on. But there's still work to be done.

Top of mind priorities for 2020 include:

Interoperability
(including mobile capabilities)

Cybersecurity

Facilitating Social Determinants of Health Analysis

INTEROPERABILITY

Data exchange continues to be an uphill battle. Marrying new applications with legacy technology is not a new problem — but an increasingly difficult one as the physical and technical footprint of healthcare changes. Smart medical devices, provider consolidation, healthcare consumerization, telehealth — each of these adds a new layer of complexity and risk. Patient data touchpoints may be seamlessly networked — or exist in dribs and drabs across a patchwork of systems.

Interoperability is about building a technology ecosystem around one entity: ***The patient. Or rather, millions of them.***

"We see hundreds of different EHRs across hospital systems. But that doesn't touch the ambulatory market and certainly not post-acute. **What we're trying to accomplish is a full view of all the encounters — everywhere a patient can be. It's not all just about connecting two (EHR) vendors."**

Here's the rub:

Without a common patient identifier, true interoperability remains elusive. Congress seems to be warming up to the idea of a National Patient Identifier (NPI), recently directing the ONC to work with federal agencies to study and report on methods of patient matching.[1] Our focus group participants acknowledged that the concept of NPI feels "scary" to consumers, and expressed skepticism that it will come to fruition anytime soon. However, these executives did agree a common identifier of some sort is essential to correct linking and verification of disparate patient records. "It's a lynchpin to all of this working well and we've got to address that somehow," said one respondent.

[1] HealthITSecurity. "Congress Directs ONC to Support National Patient Identifier Efforts," December 19, 2019

A measured approach

Interoperability is meant to not only connect care providers and information but also create a better patient experience. However, security is priority one; the focus group emphasized that simplified access (for both clinicians and patients) cannot take precedence over privacy.

Thought-Starter:

You don't have to be in limbo waiting for a National Patient Identifier. There are ways to leverage a third-party data partner to create a non-SSN unique identifier for each individual that can be used to help cleanse and aggregate the data across systems.

A few participants mentioned using a master patient index to serve as the common identifier. While leveraging a master patient index is helpful within a single environment, it very quickly breaks down when you have to work across multiple patient indexes.

CYBERSECURITY

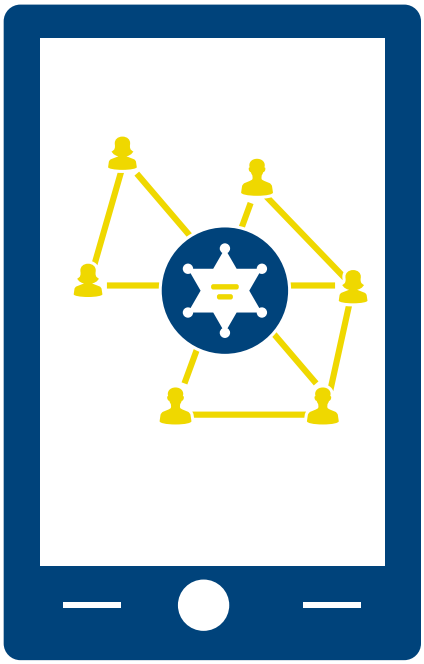
Clearly, healthcare organizations have their hands full as patient touchpoints increase and regulations require broader access to patient data.

"Wild West" of apps

Imagine your department being asked to allow patient data to be viewable on a consumer app you've never heard of. With the new ONC regulations, technology professionals face this very scenario and the focus group had a lot to say about it:

1 "How do you protect the identity of the patient when you don't have full control over who can access it or how they manage it?"

2 "In considering third-party apps we need to not only protect against unauthorized access but also prevent handing it out freely. Are we sharing data appropriately, in a permissible fashion? We've become a bit sloppy as an industry."



The discussion revealed some confusion about who owns responsibility for patient data used in third-party apps. Some interpret the regulations to mean that healthcare IT departments technically aren't responsible if the breach happens downstream. Others believe the regulations put ultimate responsibility on the originator of the data.

Worth noting: CHIME has publicly expressed concern that the regulations hold providers and EHR vendors to a different standard than third-party apps. "This creates an unlevel playing field and further perpetuates the notion that healthcare apps are the Wild West."[2]

[2] FierceHealthcare, "IT experts urge stronger oversight of patient data in the Wild West of consumer apps," December 16, 2019

NEW TECHNOLOGIES IN THE MIX

Digital transformation intensifies the focus on cybersecurity. Health systems walk a fine line to deliver the services consumers and providers want while protecting their data.

"Mobile" takes many forms in these organizations

- Providers implement tools such as patient portals and text notifications to enhance the patient experience.
- In the clinical setting, care teams rely on a growing number of smartphone and tablet-controlled devices to assist with IV infusions and other tasks.
- Telehealth is a vital link to patients who are rural or have limited mobility.

These enablements add significant value but also unprecedented complexity and risk.

Questions around the cloud

Decisions about moving to the cloud don't come easy for this group. Participants said that newer cloud-based EHRs and hybrid cloud/on-prem solutions force them to rethink long-standing ways of doing things.

- "How are the security profiles the same or different? Do we have to change how we manage them? In some cases there are new risks that surface from a hybrid approach."
- "We've gone to a new hosted EMR, so it's changed some of the security issues that we thought we had under control but now have to revisit."

Thought-Starter:

Several members of the group spoke of the constant struggle to balance competing goals of user experience and security. Patients and clinicians alike expect quick and easy system access. This typically leads organizations to favor single-factor authentication in lieu of the best-practice multifactor approach.

However, there are a number of passive, behind the scenes authentication tools that can deliver friction-free access without sacrificing security. **It's the best of both worlds.**

SOCIAL DETERMINANTS OF HEALTH

A year ago this subject was barely on the radar for this audience, and mostly rested on the shoulders of patient care executives.

Today, those charged with managing data, technologies and systems find they have an increasing role in driving health outcomes.

Social factors account for over 1 in 3 deaths a year in the U.S.[3] As part of the value-based care model, organizations are tasked with incorporating social data sets into their modeling to zero-in on those patients needing the most help.

According to focus group feedback, this process is somewhat ad hoc. Most mentioned collecting SDOH data via surveys, often administered at the point of care. However, some aren't yet collecting or aggregating this data at an enterprise level or managing it in a systematic way. Only a few said they have the capability to package it as useful clinical decisioning support and business intelligence for providers. Most are not yet using third-party data to support these efforts.

"I can't directly improve quality outcomes, but I am a piece in the value chain."

[3] Kaiser Family Foundation, Beyond Health Care: The Role of Social Determinants in Promoting Health and Health Equity, May 10, 2018

Thought-Starter:

Surveys are helpful but problematic when used as the sole collection method.

Consider using third-party data alongside clinical and patient-supplied data to develop a more holistic picture of the individual. **For instance, adding certain socioeconomic data attributes can help you better predict 30-day hospital readmissions.** Be sure to analyze data at the address level; zip codes often cover a broad range of income levels, crime rates and other factors, making it difficult to truly understand a patient's environment.

IN CLOSING: CONNECTING CONVERSATIONS

Health system technology departments can't achieve the vision of connected care by working in isolation. It requires a true team approach. Leaders from all parts of the organization have to be willing to participate in tough conversations about data governance and data security — and take ownership as appropriate.

Focus group participants report good results when rallying support from stakeholders across the enterprise: Information Security, Privacy, Operations, Compliance, Clinical and Accountable Care. By bringing the right people to the table, they are better able to find solutions that meet multiple objectives:

Satisfying patient experiences

Reduced risk

Improved operational controls & efficiencies

"(Collaboration is about) asking questions, making sure there's a strong business case — and that investments are aligned to that and not just to the whims of a director."

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 Group plc (LSE: REL/NYSE: RELX), a global provider of information and analytics for professional and business customers across industries. RELX is a FTSE 100 company and is based in London. For more information, please visit www.risk.lexisnexis.com and www.relx.com.

LexisNexis® RISK SOLUTIONS | Health Care