Q. What is driving healthcare providers to pursue telehealth strategies?

A. While telehealth and telemedicine are often used interchangeably, they are distinct terms. Telehealth refers to a broad spectrum of services including health education and information, remote health monitoring, digital therapeutics, and care delivery services (including telemedicine). Telemedicine involves the delivery of clinical services using telecommunication technology. Examples include teleradiology, telestroke, and telepsychiatry. Virtual care visits are another form of telemedicine that uses consumer-accessible technology such as web browsers and mobile devices that enable consumers to initiate the visit.

Historically, misaligned incentives impeded the progress of telehealth, including the provision of telemedicine and virtual care services. Under fee-for-service reimbursement models, physicians were compensated for driving high volumes of in-person patient visits. The intense focus on reducing healthcare costs has resulted in a shift from fee for volume to fee for value and the provision of healthcare services in lower cost but clinically appropriate care settings. Consumers have responded favorably to virtual care visits as they grow more comfortable with the videoconferencing capabilities of their devices and accustomed to interacting with other businesses online and via video. Many consumers, especially younger ones, favor convenience over traditional in-person visits. Virtual care has expanded from providing urgent care online to delivering a variety of services that range from managing chronic conditions to providing behavioral and mental health services. In a recent IDC Connected Health and Value-based Health Survey, 37% of healthcare providers reported offering virtual care services for behavioral health.

Q. How are healthcare providers making virtual care visits available to consumers?

A. Virtual care combines web video, instant messaging, advanced telephony (e.g., VoIP), and mobile to support real-time visits between physicians or other licensed clinicians and their patients using consumer-accessible technology. Vendors of these services offer the provider network the resources needed to augment the healthcare provider's own staff. Some vendors of virtual care services make their technology platform available to healthcare providers that will staff the service
with their own employed or closely affiliated clinicians. Consumers initiate the visit from the third-party vendor's virtual care services application. Depending upon how the virtual care service provider partnered with the healthcare provider, the consumer may see any clinician on demand (typically for urgent care) or schedule an appointment with a specific clinician.

Another option for providing a virtual care visit is for the physician or clinician to initiate a video chat visit that integrates telemedicine solutions into existing office workflows to recreate the in-person experience. Most of the major electronic health record (EHR) vendors support EHR-based telemedicine by either embedding videoconferencing capabilities into their EHR solutions or partnering with a virtual care service provider. In the latter scenario, two-way data integration is available to schedule appointments, confirm eligibility, and update patients’ EHRs maintained by the practice and the virtual care service provider. Patients are more likely to keep virtual care visits because they are convenient, which improves patient adherence to the care plan and has financial benefits for the practice. Missed appointments or open slots in a clinician’s schedule cost a practice approximately $200 per appointment, according to industry studies.

The technology requirements are similar for virtual care appointments whether a patient initiates the appointment from a virtual care services platform or a clinician initiates it via an EHR-based telemedicine function. Videoconferencing capabilities are made available through web browsers and mobile devices. Robust internet connectivity ensures an optimal experience with little to no video transmission latency. For visits that involve the sharing of medical images, larger bandwidth is essential. Because virtual visits involve protected health information, encryption should be embedded in the workflow so that patient data, whether in motion or at rest as structured or unstructured text (e.g., audio or video), is secured in compliance with HIPAA privacy and security regulations.

Q. Consumers are increasingly using wearable technology to self-monitor their health, wellness, and chronic conditions. How will their use of such devices affect patient care and engagement?

A. As healthcare providers increasingly digitize, the role patients play in their own healthcare is transforming dramatically. Patients are becoming true partners with their care managers and providers. They are now not only able to retrieve health-related information for their own benefit but also capable of measuring, collecting, and sharing increasingly relevant data with the healthcare system on their own. This regular stream of personalized, health-relevant patient-generated data is vital for clinicians to keep patients engaged beyond the clinical encounter and ensure continuity of care. In a 2019 IDC Health Insights survey of healthcare organizations regarding their investment plans for connected health technologies, 56% of payers and 59% of providers reported that they were piloting or using wearable technology for clinical conditions. Increasingly, payers are providing incentives to their members to use wearable devices for both fitness and clinical conditions (70%), and providers are being reimbursed by health plans for monitoring data from wearables for both fitness and clinical conditions (72.5%).

A new trend of "bring your own data" is emerging in healthcare that will support early detection, diagnosis, and treatment.
As the incorporation of sensors into a diverse range of health monitoring devices (portable, wearable, implantable, and ingestible) and connected consumer devices (such as smartphones, personal wellness wearables, and fitness trackers) increases at a fast pace, the role patients play as collectors and repositories of health-relevant data is growing in importance. A new trend of "bring your own data" is emerging in healthcare that will support the early detection, diagnosis, treatment, and long-term management of diseases. With lifestyle-related diseases and healthcare costs on the rise, all healthcare stakeholders have reason to harness patient-generated data for its preventive value. However, despite the benefits of incorporating such data into clinical practice, some factors are impeding its more widespread use. Commonly cited concerns include the reliability of the data from consumer-grade devices, not having the means to upload and store high volumes of data for analysis, and liability concerns.

**Q. What are the primary challenges healthcare providers face with the proliferation of devices connected to the network?**

**A.** Today's digital hospital features a variety of channels for communications between clinicians and between clinicians and their patients. These channels range from simple over-the-top secure texting solutions to clinical communication and collaboration platforms that combine text, email, voice, and video options. Forward-thinking hospitals are providing patients with a tablet during their inpatient stay to communicate with their caregivers, receive updates about their care, access their patient portal, and even be entertained. In some case, patients are sent home with connected remote health monitoring devices to track their biometrics while recuperating. Should the patient's readings indicate the need for clinical intervention, alerts are sent to the clinician to initiate the appropriate follow-up care.

At the edge, the proliferation of endpoints — medical devices, bedside telemetry, medical imaging, remote health monitoring devices, mobile phones, tablets, and wearables including smartwatches — will present multiple challenges to healthcare IT organizations. First and foremost is data security. With all these connected devices, the attack surface is growing exponentially and becoming increasingly borderless. Enterprise-connected devices will require more firmware updates, mobile device patching, and securing of network connections. Managing the increasing number and variety of devices will further tax already overburdened healthcare IT organizations. Of concern is how to secure connected devices that the healthcare provider does not own or control, such as consumer smartphones and tablets. Patients and their families also want to connect to the healthcare provider's Wi-Fi network, which puts more pressure on network performance and security.

**Q. What recommendations do you have for healthcare providers as they deploy telehealth solutions?**

**A.** A solution's performance is only as good as the network that it runs on. Low bandwidth and latency will result in a poor user experience for the patient and the clinician, resulting in abandonment of that visit and overall underutilization of an important investment to provide convenient access to care. Thus, healthcare providers looking to embrace telehealth will need to invest in upgrading their enterprise networks to ensure:
Network performance and reliability. Robust network performance and reliability are essential as more healthcare providers embrace connected health technologies including telemedicine and virtual care visits. High-quality and predictable network connections enable the shift from traditional voice to voice over IP to improve care team collaboration and reduce the telecommunications cost.

Resilience. The ability to meet high and often unpredictable demands for service — and to recover in the event of network failure — is important when providing care online. A high level of uptime is critical for 24 x 7 mission-critical operations and for enabling IT organizations to proactively focus on business priorities rather than maintenance and disaster recovery tasks.

Security. The demand for compute at the edge is growing with the proliferation of Internet of Things (IoT) sensors and devices, and the need for intelligence at the edge creates an expanding attack surface and a nearly borderless environment. Advanced network security and managed security services are essential to protect valuable data assets and thwart cyberattacks.

Healthcare providers should look to partner with technology suppliers that understand the unique business and regulatory environment in which they operate.

About the Analyst

Lynne A. Dunbrack, Research Vice President, IDC Health Insights

Lynne A. Dunbrack is a nationally recognized thought leader in the application of information technology to the business problems of the health industry. Her understanding of the needs of the health industry is grounded in experience over the past 25-plus years working as a consultant and in the field. She also served as the Director of HIPAA Compliance at NaviMedix Inc. (now NaviNet). As program director for IDC Health Insights, Ms. Dunbrack provides research-based advisory and consulting services that will enable health payer and provider executives to maximize the business value of their technology investments and minimize technology risk through accurate planning.
CenturyLink can help transform the patient experience from the hospital room to the edge with adaptive network connectivity and connected services that help healthcare providers harness their data, make predictions, and respond in real time, all while delivering uninterrupted and secure data access. CenturyLink partners with 9 of the 10 largest hospitals and 6 of the 8 largest insurance companies in the U.S. to help them on their transformation journey. We work hand-in-hand to deploy solutions across our extensive portfolio, giving your organization the utmost flexibility to evolve at your own pace. We have the experts and the relationships to help you deliver better value-based experiences. Our adaptive network control solutions enable up to 300% bandwidth scalability, and we are connected to over 2,200 public and private datacenters globally. To learn more visit www.centurylink.com/business.