Get ready to innovate. Soon you may find that to compete and operate within medical home communities and accountable care organizations (ACOs), you will have to integrate mobile healthcare technologies into your practice. How will this affect the way you practice?

Health information technology (HIT) has come a long way in a short period of time. Just a few years ago, physician pushback to implementation of electronic health records (EHRs) in their practices and hospitals was quite high. Today, however, doctors have little choice but to use the technology available to them.

Not that they care to object anymore. For as they have adopted iPads, smartphones, and other mobile devices in their private lives, those primary care physicians (PCPs) who decried not long ago that electronics interfered with the practice of medicine are now more likely to describe mobile technology as “cool” and “a must-have.”

**A PLETHORA OF DEVICES AND APPLICATIONS**

Laptops, tablets, android smartphones, iPhones, iPads, and USB drives—the options for using mobile technology in healthcare are many and varied. Software applications (apps) run the gamut.
Applications, tools & legislation for mobile device management, security

Many tools are available online for tracking/securing mobile devices and for preventing patient data from falling into the wrong hands. They include global positioning systems that track and locate mobile devices, data loss prevention tools that monitor data and prevent them from being removed from mobile devices, and remote data wipe tools, which enable organizations to simply delete their data from lost or stolen mobile devices, preventing potentially disastrous consequences. You can find information on many of these tools, and on the legislation regulating the use of mobile devices in healthcare, at these sites:

**DEVICE MANAGEMENT APPS AND TOOLS**
- Official U.S. government site for global positioning system
  www.gps.gov
- Rebecca Herold’s Privacy Management Toolkit
  www.privacyguidance.com/eMy_Mgmt_Tools.html
- U.S. National Library of Medicine Gallery of Mobile Apps and Sites
  www.nlm.nih.gov/mobile
- Google Remote Data Wipe for Mobile Devices
  www.google.com/support/bin/answer.py?answer=173390

“It’s not about the toys. It’s about the patients,” says Norman Vinn, DO, MBA, founder, chief executive officer, and medical director, Housecall Doctors Medical Group. “You don’t want to be in a position where, when you’re a hammer, everything starts looking like a nail.”
from evidence-based decision support tools, to updated formularies, to patient education tools for use at the point of care, to clinical laboratory alerts, and many more. Literally hundreds of medical apps are available from which you can choose. Many of them are free. And hundreds more are released each year.

Housecall Doctors Medical Group (HDMG) employs California-based “residents” who practice medicine in the same way hospitalists treat in-hospital patients—except that HDMG clinicians travel to home-bound/access-challenged patients all over Orange, southern Los Angeles, Riverside, and San Bernardino counties to diagnose disease and advise and treat patients in their homes. To accomplish this, HDMG uses a plethora of mobile technologies.

Norman Vinn, DO, MBA, HDMG founder, chief executive officer, and medical director, operates a delegated managed-care model that reduces costs by lowering the number of hospital in-patient re-admissions, emergency department (ED) visits, and skilled nursing days. Medical groups bring in Vinn’s residents to assist them with treating their highest-cost, highest-risk patients. “We’ve measured the before and after utilization [of healthcare] with this population of patients,” Vinn says, “and [the delegated managed-care model] has yielded significant reductions in utilization.”

It has also produced an interesting side benefit: improved patient satisfaction. “Imagine a world that’s almost the antithesis of the old world of ‘Dr. No’ and ‘you can’t do this and you can’t do that,’ ” Vinn adds. “It’s a much more empowering model that delights patients rather than makes them feel that they didn’t get everything they needed.”

HDMG residentialists use mobile-formatted EHRs—customized to the needs of home care patients—to evaluate and treat the whole patient in a home environment and to document that information in real time over a broadband wireless connection to their practice’s office network. Then they move that information to other providers and managers in a timely fashion to improve continuity and coordination of care and smooth care transitions with the goal of pre-empting duplication of services or utilization of unnecessary ED and hospital services.

Vinn defines mobile technology as having three distinctly different categories:

- Communication and documentation—fundamentally, this is mobile EHRs and tools for moving information around to the proper stakeholders in a timely fashion;
- Clinical diagnostic—used to treat patients at the point of care; and
- Remote monitoring—transmitting and receiving information on a patient's status when a clinician is not present.
“The reason I put mobile technology into those three buckets,” Vinn says, “is to differentiate what we do currently, what we don’t do currently, and what I think is likely to happen with our residentialist clinicians and other homecare clinicians in the future. [With mobile technology] we can intervene in a timely fashion while onsite and preempt the need for more costly reactive care.”

MOBILE TECHNOLOGY IN THE HOME
HDMG long has used traditional portable medical resources such as mobile x-ray, ultrasound, echocardiogram, and handheld blood analyzer systems to diagnose disease in patients’ homes and to determine whether further treatment at home or in-hospital is warranted. Portable diagnostic systems have been a boon to home-based medical care.

The capabilities of these systems, however, do not always align perfectly with the needs of patients, and they can be exorbitantly expensive to own. Therefore, where the concept of mobile technology’s use in home healthcare is concerned, Vinn’s philosophy is “sometimes, less is more.”

“It’s not about the toys. It’s about the patients,” Vinn says. “You don’t want to be in a position where, when you’re a hammer, everything starts looking like a nail.”

Today’s wireless mobile technologies for healthcare—such as iPads and tablet PCs used to collect, send, and receive patient data at the point of care—are revolutionizing the home healthcare industry.

Since it first became available, Vinn’s residentialist doctors have been using tablet PC and smartphone technology to record patient data onsite and then cut and paste it into the patient’s personal health record (PHR) chart. However, a clinician recently demonstrated how the iPad’s built-in wireless technology establishes a direct two-way, real-time link to the practice’s network and enables clinicians to remotely enter medical data directly into a patient’s chart in real time. This ability really got Vinn’s attention.

“We got into our [computer network] with the iPad just as effectively as with the tablet and keyboard, and the iPad’s ability to shrink and enlarge images overcame certain issues we had with screen resolutions,” Vinn says.

Vinn says that when residents need to find a drug’s formulary or interaction information that isn’t immediately available within the patient’s PHR, they can go online and flip back and forth between applications very quickly. This enabling technology allows them to practice more robust information-gathering in the field. With smartphones, he adds, the residents can look up things online very quickly, and with the iPad’s screen resolution capabilities, the device probably is the future of field-based “anywhere/anytime” medicine.

ROLE IN ACCOUNTABLE HEALTHCARE
As the population of elderly patients increases, so does the cost of healthcare in America. With each new patient, home-based treatment as an alternative to in-hospital care becomes even more viable, and mobile technology plays an ever-increasing role in that scenario.

Built-in cameras enable clinicians to snap high-resolution images of patients’ conditions and transmit them to specialists for diagnosis. Webcams allow physicians to “see” patients’ conditions in real time and “hear” descriptions of their symptoms. Smartphone technology lets clinicians push and pull patient data to and from EHRs.

In fact, with the advent of tablet-based mobile technologies in healthcare and the plethora of evidence-based software applications for clinicians to use in the field, homecare and telemedicine are quickly merging into a single industry.
I think what's likely to happen is a telemedicine angle where—in between face-to-face visits, particularly for home-bound patients regardless of whether they're permanent or temporary—we'll be looking at patients through webcams, and maybe listening to their hearts and lungs, and be able to detect and even record the sounds into the patients' charts,” Vinn says.

You and your colleagues in primary care are under increasing pressure to rein in healthcare costs. ACO and medical home concepts of medicine have changed the manner in which you practice medicine. And adopting mobile technology adds a new layer to that mix.

Vinn believes it's almost inevitable that [PCPs] are going to have to get comfortable with certain degrees of intervention that fall outside of traditional office visits.

“Doctors are going to be increasingly compelled to use things like webcams for certain patients,” he says. “There may not always be effective residentialist care in their community, and if you consider the move toward increased accountability of risk—for example with ACOs—everyone's going to be in a scramble to start managing the highest-cost patients in a more effective fashion, and that's going to mean that all bets are off—you do what you have to do to intervene, gain control, and eliminate unnecessary utilizations of limited resources.”

HDMG’s office EHR is server-based rather than an ISP (Internet server provider) model. Until now, access to patient records has been limited by the transmission speeds of the company's in-field residentialists' broadband connections, which Vinn explains has occasionally been spotty and slowed down making the use of mobile technology more user-friendly. With the advent and growing use of 4G technology, Vinn sees this as a moot point, however.

He argues that as these systems become more powerful, and as broadband access becomes more widespread, the use of [mobile technology] can only increase.

“I know a number of other residentialist clinicians [who] are still using paper charts,” Vinn says, “and I can’t figure out how they get along with access to information and movement of information, because that's where the game is won or lost. The future is not ‘he who owns the information wins.’ The future is ‘he who moves the information wins.’

So, Vinn says, anywhere that you can access clinical reference information in a more user-friendly and robust fashion, and populate information and then get it quickly and efficiently to another stakeholder to eliminate redundancy and improve coordination of care, will make the healthcare delivery system better.

EMBRACE CHANGE MANAGEMENT
Adopting mobile technology can be disruptive to a practice. If you are on that path, Vinn advises completing an environmental survey and keeping current on the available technologies. In addition, he encourages addressing the fundamentals of ‘change management.’

Vinn invokes a standard evolutionary euphemism by noting that the species that survives is not the strongest; the species that survives is the one that's best at adaptation. Keys to survival include awareness, adoption, and adaptation.

He urges office-based physicians be open to change, to try new things, and to be flexible, noting that technology is not necessarily complicated. He acknowledges, however, that change can be stressful.

“I think the same thing will happen to clinicians [who] go from paper charts to electronic notes, and to clinicians of the future who will be dealing with Internet access to reference information versus how much they can cram into their heads during medical school and residency,” Vinn says. “That's going to be a change in how business is done.”
Vinn predicts that the future will see a further aggregation of resources and technologies to get better results. It will be a blend of hands-on onsite and clinic care, remote monitoring, and telemedicine.

ENSURE SECURITY AND PRIVACY
The decision-making, however, does not end there. You also must consider how best to protect your mobile devices—as well as the private patient data they contain—from damage and unauthorized access. Additionally, you must comply with current laws regulating the use of patient data on mobile technology.

You now have at your disposal many new information-sharing tools that weren’t available even 1 year ago. This is certainly a good thing from a provider’s perspective. However, you must be aware that risk comes with those new technologies.

Often, the risk involved with using a new information technology is not known until after it’s been exploited by someone with malicious intent, or through accidental exposure of information. As you and other caregivers move to use mobile computing and storage technologies, you must become aware of the types of threats and vulnerabilities that are involved with having patient information used in this way.

LEGISLATION REGULATING MOBILE DEVICES
The Health Insurance Portability and Accountability Act of 1996 (HIPAA) applies to the following:

- healthcare providers who conduct certain transactions in electronic form;
- healthcare clearinghouses; and
- health plans.

HIPAA refers to these organizations as “covered entities.” Under the HIPAA administration simplification security rule, covered entities are required to secure their electronic data transmissions, ensure patient health information privacy, and report any inappropriate access of patient data.

According to Rebecca Herold, CIPP, CISSP, CISM, CISA, FLMI, many physicians mistakenly believe that because HIPAA does not explicitly name specific mobile technologies in the language of the legislation, it does not include them in its requirements.

Herold is owner and chief executive officer of Rebecca Herold & Associates, LLC, an Iowa-based firm that helps organizations evaluate their security and privacy risks and then guides them through the laws and regulations pertaining to their specific industries.

“What [physicians] need to realize is that HIPAA was written back in 1996 and the security and privacy rules were finalized in early 2001 to 2003,” she says. “HIPAA didn’t cover those things explicitly because they did not exist at the time. Additionally, these regulations do not provide explicit requirements for specific technologies because of the fact that technologies and new practices evolve so quickly.”

Herold says that covered entities should keep in mind that at the core of [healthcare] security and privacy regulation requirements is the need to assess the risk to patient health information and other types of patient data. With this in mind, she continues, PCPs have to understand that they’re required under these data protection regulations to identify all types of risk—beyond those that might be explicitly stated—and then to apply the appropriate safeguards around those risks.

EVALUATING THE RISKS
What risks are involved with using mobile technologies and those nifty apps that enable information exchange between physicians, clearinghouses, and health plans? The most basic risk—one that happens to virtually every organization—is the inevitable loss of mobile devices (see “Security on the go,” Medical Economics, July 10, 2011, pp. S4-S9; MedicalEconomics.com/securityonthego).

Mobile devices are handy, small, easy to carry around, and extremely easy to lose. It’s not uncommon to see people leave behind their laptops, iPads, or smartphones in restaurants. This ease of loss should be a strong motivator. If you use these devices in your practice, you must ensure that nobody can get to the data on those devices and that you’re able to track them if they are lost.

PATIENT DATA LOSS AND THEFT
In addition to data loss, data theft can occur. Thieves love mobile devices because 1) the hardware itself is valuable, and 2) even more valuable are the data that’s on them. Although some thieves quickly
sell the hardware for a quick buck, others take the time to first copy the data before selling the mobile device, and then they sell the data as well.

“All [these] valuable data [have] oodles of personal information that other thieves can use to commit identity theft,” Herold says. “[These] data also [are] sold to marketing companies because [they have] all sorts of good information that can be incorporated into marketing data bases that they then sell.”

Because of these two basic threats—the threat of losing the device and the threat of criminals stealing them—doctors, nurses, insurance providers, and all their business associates need to take precautions.

The number one way to protect data on mobile devices is to encrypt them, using a strong-encryption method.

“A lot people hear the word ‘encryption’ and they get scared because it’s a techie term and it sounds hard to do,” Herold says. “The fact is, encryption tools have become easy to use and transparent to the person using them. A lot of good options are out there, and many are inexpensive.”

Healthcare providers and insurance workers often keep important data on mobile devices, and, unfortunately, sometimes they fail to make backup copies of the data. That’s a very dangerous practice, because if you’re relying on just one copy of these data, not only will you lose all your data if the device is lost or stolen, but if you physically damage your mobile device, the data can be lost forever.

Physical damage can happen at any time with no expectation or foresight, so it’s imperative that users of mobile technology make backups of their important data and store them in a safe location.

**CONTROL ACCESS TO YOUR NETWORK**

Data can be modified or corrupted in ways that render them inaccurate. These inaccuracies could lead to incorrect health decision-making.

You don’t want incorrect diagnoses or incorrect medicines prescribed to patients as a result of data being inappropriately changed. You must ensure that only staff members who need access to patient data have access to them.

Appropriate access requires strict controls to the mobile devices used by caregivers. These include logins, passwords, and biometric technology (for example, thumb prints), all of which block unauthorized access to mobile devices and to the data they contain. However, through either inept security (such as keeping a sticky note with your user name and password inside your mobile device case) or through the clever use of password-cracking tools, criminals often figure out the device password and can still gain access to the data. That’s why it’s doubly important that you encrypt your data.

Then there’s the vulnerability of the network itself. “You also need to make sure that they can’t gain access through your mobile device to other places they should not be going,” Herold says. “For instance, some people have their smartphones or laptops configured to automatically log into their office or hospital network. So you need to ensure that your mobile device is not configured in a way that gives a direct path to some other system you would not want unauthorized people to get to.”

**VIRUSES AND MALWARE**

Viruses can quickly shut down a network, and keystroke loggers (devices that record every keystroke and send those data to another location) can provide criminals with all the passwords they need to gain access to your private patient data. Therefore, installing anti-virus and anti-malware software on all mobile computing and storage devices is a must. Doing so will help you prevent malicious code from getting in and taking control of your network. Along the same lines, installing a personal firewall on all mobile devices prevents things from coming in that are not blocked by the anti-virus/malware software.

**TRACKING YOUR MOBILE DEVICES**

Knowing which individuals in your organization are using mobile devices is critical in the event that your firewall gets breached and your patient data inappropriately accessed or stolen. In addition to the HITECH Act—which requires healthcare providers and their business associates to report all instances where private patient data are lost, stolen, or inappropriately accessed—each state has its own data breach laws.

“It’s very important to know when protected health information has been inappropriately accessed or released to someone who shouldn’t have access to it,” Herold says. “You have to report this. It’s a legal requirement.”

But how can you know when data...
have been breached if you don’t even know where those data are located? Inventory tracking of mobile devices is crucial. You need to know:

- who is using them;
- what data are on them;
- how they’re being used;
- who is responsible for them; and
- who owns them (many organizations allow individuals to use their own personal mobile devices).

Someone must be assigned the ultimate responsibility for ensuring that all of the safeguards (for example, encryption, firewall, and anti-malware and anti-virus software) are implemented on all of the mobile devices in use in your organization. Everyone using these mobile devices also must be educated on how to protect the data and on their responsibilities should the device be lost or stolen.

“HIPAA requires that someone has been assigned responsibility for security and privacy,” Herold says. “Depending on the organization, this may or may not be the same person. However, someone must have the ultimate responsibility so that [he or she] can then develop the policies that govern all the policies that need to be in place.”

EDUCATE YOUR STAFF

So that people know how to safeguard and secure these mobile devices—and the data they contain—policies must be in place for them to follow, along with supporting procedures specific to each of the business activities for which these devices are used.

A good training and awareness program should be in place to inform mobile device users on the proper procedures for using mobile data as well as their responsibilities for protecting them and reporting if they are lost or stolen. These educational programs should be ongoing and not simply an introductory program given upon hiring.

Multiple studies have shown that, even after people are trained on how to secure these devices, memories fade very quickly. To reinforce understanding and knowledge of how to secure mobile devices and the mobile data, remind staff members of this information.

“You can’t have security and privacy without effective training and awareness. It’s critical,” Herold says. “You’re also committing a huge regulatory and compliance violation by not having it. You can have all the technology in the world, but if you don’t have training and awareness, you’re going to get into hot water pretty quickly.”

Finally, be sure to inform the business associates to whom you outsource activities (that is, those who aren’t your employees but who work for other types of healthcare organizations) of your data access policies and procedures for securing data on mobile devices. Ensure that they have the same or comparable safeguards in place to protect your data.

“Whenever you outsource processing of any kind, you do not outsource your responsibilities,” Herold says. “You still maintain some responsibility for [those] data, even when you send [them] to another entity to do some type of business processing.”

FOLLOW YOUR HOSPITAL’S LEAD

The security and privacy officers at the hospitals where you’re affiliated can provide invaluable guidance. Find out what they’re using to secure their own patient data on mobile devices, and what policies they have in place to govern their activities when they push their patients’ data out beyond their hospital’s firewalls to attending physicians.

Herold also suggests that physicians join organizations such as the American Health Information and Management Association and the Health Care Compliance Association, as well as security- and privacy-specific organizations such as the International Association of Privacy Professionals and the Information Systems Security Association.

Also, be sure to study the pertinent government Web sites (see “Applications, tools, and legislation for mobile device management and security” on page 29), such as the U.S. Department of Health and Human Services, to fully understand your responsibilities as a covered entity to secure the access to, and protect the privacy of, your patients’ private health data.

The author has spent more than 10 years as a reporter and writer covering information technology in healthcare. He is a former editor-in-chief of Health Management Technology magazine. Send your feedback to medec@advanstar.com.