PLUS:

- Learning from the EHR for Quality Improvement
- Healthcare Technology Challenges 2020: Defining a Framework for Success
The proliferation of mobile technology in to the daily lives of our workforce has forever changed the expectations placed on technology departments and data accessibility within healthcare. For years information technology departments have been recommending the centralization of data management, access and reporting. The challenge is that the information access requirements evolved faster than healthcare information technology departments’ abilities to adapt systems to meet the needs of a consumer workforce. Fortunately, many information technology departments followed the trends of desktop virtualization and mobile device management with the promise of cost reduction, risk mitigation, and Bring Your Own Device (BYOD) strategies.

22 Workforce: Meeting the Data Accessibility Expectations of the Consumer Workforce

Ryan A. Terry

The tools of mobile computing—smartphones and PDAs, tablet PCs, patient monitoring devices and an avalanche of apps among them—are opening new vistas of opportunity for clinical collaboration. The design of the study was based on a Regionalised Service slum setting to test the feasibility of deploying Mobile Technology for providing primary healthcare services. The proliferation of mobile phone technology has made the world a smaller place where people can interact with each other, irrespective of which part of the world they are in. Mobile phones are generally affordable and available to most of the population, making them more accessible than computers and far more cost-effective than hospital beds. Therefore, mobile technology has the potential to revolutionize health care in developing countries, particularly in the area of health awareness schemes and training of health care professionals. This paper reports the results of a Healthcare IT initiative aimed at using Mobile Phone technology to spread medical care amongst people slum areas. A survey was done in an urban slum setting to test the feasibility of deploying Mobile Technology for providing primary healthcare services. The design of the study was based on a Regionalised Service model.
40 mHealth—Security and Compliance  
By Jeff Brandt  
Security in mHealth encompasses many facets, concerns, misconceptions and fears. From users’ perceptions to data breaches, this chapter will introduce some of the issues that will help you develop insights and strategies as you plan for, develop and implement mHealth solutions. Designers and purchasers of mobile health solutions must take many issues into consideration when developing an organizational mobile health strategy. The sheer speed of adoption of mobile devices and software into our everyday lives has propelled the market to produce quicker, cheaper and more feature-rich devices faster than most organizations can digest. The speed with which these devices evolve also increases the rate of system deprecation. If not managed correctly, this technical liability can be very costly to a healthcare organization. Although we are only at the beginning of what is possible and will be accomplished with mHealth, being cognizant of the opportunity is important. The caveat is that with all new technologies comes new risk. With a well-developed strategy, however, the exposure can be mitigated.

FEATURES

46 Learning from the EHR for Quality Improvement: A Descriptive Study of Organizational Practices  
By Bill Bria, MD; Rosemary Kennedy, PhD, MBA, RN, FAAN; and Dana Womack, MS, RN  
We are entering an era where it is possible that clinical effectiveness research may be accomplished as a byproduct of daily clinical care. It is possible for clinical data analysis to begin at the outset of the implementation of an EHR, but moving the existing culture and expectations of measuring EHR success in terms of “go live” functionally to measurable improvements in patient outcomes will require significant investment, organizational structural changes, utilization of clinical informatics professionals to their full potential, and a willingness to envision a future where care delivery, research, and quality improvement coexist at the bedside. Implementation of health information systems has been a significant focus over the past decade, but now is the time for informatics professionals to collaborate with their technology, quality, and evidence-based practice colleagues to help their organizations transition from “data” and “information” to “knowledge” and actionable insight levels of information processing.

52 Healthcare Technology Challenges 2020—Defining a Framework for Success  
By Stephen Grimes, FHIMSS, FACCE, FAIME  
Over the next 10 years, healthcare technology gives us the possibility of transforming healthcare delivery in ways that can offer unprecedented quality, timeliness, effectiveness, and availability. Some of these technologies include integrated clinical information systems, robotics, imaging, genomics, telemedicine and nanotechnologies. However, these technologies are increasingly complex and integrated. Most organizations do not have the infrastructure to adequately deal with the proper selection, deployment or support of these new and emerging technologies and are therefore woefully unprepared. These healthcare organizations must adopt strategic processes to insure they select technologies appropriate to the mission and goals. These organizations must also evolve existing services such as clinical engineering and information technology into as seamless support service for medical and information technologies by adopting a common governance framework. Implementing a strategic technology selection process and evolving the technology support infrastructure (staff, processes, tools) are necessary to achieve the substantial benefits to patient care and economic.

By Michelle F Magie, MD; Cortney Nicolato, CPHIT; and Manon Mailland Schladen, MSE PMP EdS  
Consumer health informatics is an emerging field that offers the ability to enhance the quality and safety of care by leveraging information and communication technologies to place the patient at the center of care. This is particularly true for patients with chronic complex medical conditions and/or from vulnerable populations, including minorities, the elderly and disabled. Uptake and adoption of such technology has been slow. Strategies are needed to assess barriers and develop successful approaches to promote connected health leveraging consumer eHealth technologies, including interoperability with organizational IT systems, for support of patients and their provider teams to optimize care. Through two case studies and an overview of current evidence and industry trends in personal connected health technologies, this paper will make the case for connected health applications adoption and integration within the healthcare IT ecosystem to support and connect patients and their providers. We will present a model developed by a healthcare system and a software developer for the interoperability of web-based self-care management platforms for seamless 24/7 sharing of personal health information across the continuum of care among the patient, system and non-system providers and organizations which are stakeholders in the US healthcare delivery system.

72 Electronic Patient Plan of Care—Nursing Care Coordination and Patient Care Transitions in Electronic Medical Records  
By Luann Whittenburg, PhD, RN  
This article discusses the new healthcare environment of rewarding patient care quality in organizations that devote attention to outcomes measures and improvement. Since 2004, federal health policy has promoted delivery performance changes to obtain patient care value and quality transparency.1 The Patient Protection and Affordable Care Act (Pub. L. 111–148) was enacted on March 23, 2010 to improve the health of individuals, families, and communities (HHS, 2004). Nursing is moving from task-oriented documentation in Electronic Medical Record systems (EMRs) to a Patient Plan of Care model. Electronic nursing documentation systems are focusing on Patient Plan of Care documentation to monitor and track the progress of patient care. The aim of this article is to describe a replicable method to examine EMR nomenclatures and lexicons using the structured nursing concepts in the Clinical Care Classification (CCC) System to support nursing outcomes measurement and quality transparency in health systems.
Welcome to the 2012 Summer edition of JHIM, the theme of which is mobile health.

Many interesting mobile electronic solutions have been developed in healthcare. At HIMSS12, sessions included application development, adoption frameworks, management of the new BYOB beasts on the block, use cases for effective healthcare management in ambulatory and remote-care settings, as well as the cautionary barriers that must be considered.

Mobile technology penetrates our daily lives, from the use of consumer-influenced devices that keep us tethered to the world around us to the complex work environments that compel us to be more efficient and productive every hour of the day. Healthcare has become more data-driven and our thirst for immediate access to information has propelled mobility into a game changer for healthcare planning and delivery.

As Krohn and Metcalf point out in their column this issue: “We’re experiencing a pivotal event—technology and societal trends are converging to create new communication patterns that connect and coordinate the roles of every healthcare stakeholder, including the patient, provider, payer, employer, pharma, public health...”

In my early nursing career, the adage “the patient is where the chart is not” rang true. It meant that someone was forever hunting down patient charts for updating or to share information with clinicians. With today’s virtual charts, patient information can be in the hands of those who need it as rapidly as it is entered into a system. Now we want it all—integrated and in a form factor that works for us. EHR vendors are racing to create versatile presentation of data on small screens that provide accurate and useful information in the clinical decision-making process.

Access to information and how we use it are driving rapid changes in the technologies required to support and protect data that is everywhere when we need it. The freedom of versatility and ease of access to data using mobile technologies comes with responsibilities. Healthcare organizations have given up paper charts in deference to the electronic medical record in order to comply with HITECH and other reform changes. The reams of green bar financial reports have given way to large computer screens that allow users to manipulate and analyze data in seconds.

Instant and mobile access comes with responsibilities. Evolving regulatory policies, standards, restrictions and sanctions provide the cautionary tone needed to manage and protect the data that is nowhere and everywhere. We have always been required to manage and protect sensitive institutional and patient related information. Yet new threats to privacy demand a more comprehensive and more costly investment for organizations whose resources are stretched.

The technologies are still evolving that will further enhance the availability of information in healthcare. In this edition of JHIM, you will enjoy reading the experiences of those who are exploring new uses with form factors, scalability of the functions, data protection methods, empowered patient smartphone experiences and more. JHIM

Mary Alice Annecharico,
MS, RN, FHIMSS, is Senior Vice President and CIO of the Henry Ford Health System, Detroit. Annecharico recently transitioned from a similar position at University Hospitals, Cleveland, where she was responsible for the implementation of an integrated EHR with an 87 percent physician CPOE adoption rate.

Introducing the JHIM Editorial Board

Following HIMSS12 earlier this year in Las Vegas, I have been working diligently with the editorial staff to create a more interactive and participatory Editorial Board and to continue to develop challenging and provocative themes for future editions of the HIMSS’ highly acclaimed and peer-reviewed publication.

I am pleased to welcome the HIMSS members, both returning and new, who have agreed to serve on the Editorial Board with me:

- Marion J. Ball
- William Bria
- John P. Glaser
- Margaret M. Hassett
- James Langabeer
- Eta S. Berner
- Sharon Klein
- Barbara Hoehn
Big Data
The Next Big Thing in Health IT?

Healthcare has a reputation for being years behind other businesses in adopting information and communications technologies (ICT). Being known as a technology laggard is generally not a sign of strength in today’s global economy, but neither is it a fatal flaw if delays in digital transformation allow healthcare organizations to avoid mistakes made by early adopters in other industries. Learning the lessons of others’ experiences can have real value.

However, as a futurist, I focus on looking beyond today’s preoccupations—like Meaningful Use and ICD-10—to identify “the next big thing” and to estimate its evolution. One noteworthy trend—mobile health—is already getting attention—it deserves as the featured topic in this issue of JHIM. Mobile deployment of information and communications technologies has transformed other industries in the past few years. Now is clearly the time to start creating knowledge about the applications of mobile ICT in healthcare.

Looking one step further down the information highway, I see “big data” as the next trend likely to compete for the attention of healthcare’s information executives. Articles about the exploitation of colossal data bases in other industries now appear in the business press daily. Best-selling books extol the power of companies that amass and analyze consumer data on many different levels (e.g., goods and services purchased, locations visited, subjects searched online) to influence future purchases.

Healthcare’s Gold Mine?
Medical enterprises sit atop an exponentially growing mass of computer-accessible data generated by electronic records, automated claims processing and government program reporting requirements. Some commentators already describe these raw numbers as an untapped gold mine, ready to be turned into actionable—and, therefore, valuable—information. I agree that the trend is worth careful attention. As one CIO asked me at HIMSS12, “What are we going to do with all these numbers?” Lots of vendors will be there with answers to her question.

The prospects of a big push for “big data” are sufficiently strong that we’d better start planning to deal with it. However, the lessons of history suggest that we must prepare ourselves not to overreact. The next big thing is often the next big bubble to burst. We don’t need to look back any further than the global economic crash of 2008. Economies around the world lost trillions of dollars due to defective investment vehicles created by new analytics. Originally peddled as the wave of the future for international finance, “big data” quickly turned out to be a tsunami.

Today’s medical enterprises do not have spare cash to invest in such risky ventures. Nor do they have the luxury of climbing a mountain of numbers just because it is there. Raw data can only be turned into valuable information if they have intrinsic value. We must remember that alchemists have been around for hundreds of years, and they have never succeeded in creating gold out of any material that did not contain gold in the first place.

Real Gold or Fool’s Gold?
My 40 years of experience with health data convinces me that many of our numbers are not worth the silicon they are stored on (or, more accurately in our ICT-lagging industry, the paper they are printed on). Lots of clinical and operational data are recorded incorrectly, and even observations that were recorded correctly are often meaningless. For example, patient records typically contain data on the vital signs of every hospitalized patient, but providers do little to make sure that the measurements are made the same way by every caregiver. Nor are the recorded numbers validated for inter-rater reliability.

We also have a tendency to keep collecting the same clinical data (often because regulations require it) while medical science is identifying new data that are better measures of the underlying conditions we are in business to treat. Again, data on vital signs illustrate the point. Cardiac and respiratory functions are observed at regular time intervals, presumably every four hours, for non-critical patients whose conditions can deteriorate in minutes. Recent research has identified easily detectable changes that precede life-threatening crises for non-critical patients, but current methods for recording and analyzing the vital signs do not provide information that would summon rapid response teams in time to save many patients who are unexpectedly found “dead in bed.”

In addition to collecting vast quantities of inaccurate and meaningless data, medical enterprises stockpile lots of numbers that never will be analyzed. Storage may be cheap, but we could save billions of dollars annually if we had the inclination and freedom (from outdated and/or meaningless regulations) to focus on the efficiency of our data operations. Unquestioning acceptance of big data’s alluring concepts runs the risk of encouraging us to collect
Today’s medical enterprises do not have … the luxury of climbing a mountain of numbers just because it is there. Raw data can only be turned into valuable information if they have intrinsic value.

even more data in hopes that we might find something valuable when we process it. Like successful gold mining companies, we should assay our raw material before we run it through the mill.

BIG DATA’S POTENTIAL BENEFITS

When healthcare data is worth mining, the new analytical tools should be adopted for the specific purpose of ensuring consistently good medical services as inexpensively as possible. Assuming that “big data” will move from being the subject of this single column to the featured topic in a future issue of JHIM, I propose that we begin thinking seriously about our data—paying close attention to the intrinsic value of numbers we will someday be turning into information in new ways.

In other words, my reservations about the arrival of “big data” are based on inherent flaws in our data, not weaknesses in modern analytics and enabling technologies. The healthcare industry’s information executives need to ensure that they do not invest in good technologies to refine bad data. If we continue to build data bases full of flawed numbers, we risk learning more and more about less and less until we know absolutely everything about nothing. To avoid falling into this trap, health IT leaders should start pushing efforts to collect only good data so that “big data” does only big, good things when it arrives. JHIM
Security Risks

Mobile Devices Are Here to Stay, But Challenges Remain

Those of us who experienced the implementation of healthcare applications during the 1990s know that for the most part, physicians did not want to use them. There was a simple reason why: It was easier to write an order on a paper pad and make a note in a paper chart than it was to remember a sign-on, enter a password and navigate a series of screens to enter an order. Let’s face it, when something is not easy to do, the natural thing is to avoid doing it.

Since the 1990s, a number of factors have changed. For starters, the kids of the 1990s grew up using computer technology. It is second nature to them to use new technology. Secondly, the technology of today has simplified the use of tools like electronic medical records (EMR). So the technology of today has simplified the use of tools like electronic medical records (EMR). Secondly, the technology of today has simplified the use of tools like electronic medical records (EMR). So the technology of today has simplified the use of tools like electronic medical records (EMR).

We have recently seen the evolution of the HIPAA rule with the HITECH Act over the past three years in an effort to keep up with advances in technology. In the federal agency arena we have seen updated guidance from the National Institute for Standards in Technology (NIST) and in the private arena the HITRUST CSF (Common Security Framework). So now that the physicians are on board with technology (for the most part), we should begin to see more and more information organizational, administrative, physical and technical controls to protect unauthorized access to ePHI. It is the next natural step in the cycle.

Here are some examples:

Administrative. Strong policies and procedures around the use of portable devices. For example, should personal devices be allowed in the work environment? They can currently distract physicians with personal information, such as a text from a friend during a patient visit, never mind in the surgery suite. Not good. And, they may not have the technical control standards required by the healthcare organization. Ah, but there are apps for that, no doubt. Workforce training should cover the risks and vulnerabilities and sanctions for violations including those involving improper use of mobile devices.

Physical and technical. ePHI will either not be stored on personal devices or the devices will be protected by strong authentication, encryption (including text messages) and a GPS location app that also has the capability to wipe the media. These controls are available today and will continue to improve. And, why not store all data on a secure server rather than on the device itself?

Legal framework. With all of the above said, let's take a look at the current legal and regulatory framework for mHealth devices, which includes six of the federal alphabet soup agencies: the FCC, FTC, FDA, NIST, OCR and ONC. Each of these agencies has one or more direct or indirect controls mobile devices.

- The FCC regulates communications including all private users; they manage all the federal frequency bands.
- The FTC works in the area of consumer protections especially privacy and identity protections; they have a new consumer privacy protection report out on their web site.
- The FDA has regulatory authority over all mobile medical devices, possibly including EHRs.
- NIST writes security guidance for the federal departments and agencies including Special Publication (SP) 800-66, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, and other SP 800 documents to assist with security such as risk assessment, various types of encryption, security controls, plus a freely downloadable NIST HIPAA Security
We have learned over the past 20 years that new technology cycles can initially increase the risk of unauthorized access to data due to new vulnerabilities.
Informatics’ Role in the Future of Nursing
What the Coming Years Hold for Our Profession

The 2012 annual HIMSS Conference & Exhibition in Las Vegas adjourned on Feb. 24, with record attendance and a mind boggling number of pre-conference symposia, educational sessions, posters, virtual learning and networking opportunities and more than 1,000 vendors displaying the latest and greatest health IT solutions.

Even long-time veterans of the industry concede that never before has such emphasis been placed on the value offered by health IT and never before has the expectation been higher. The federal government agrees and is putting money behind its belief that health IT can help reform our struggling healthcare delivery system.

Through the HITECH Act of 2009, billions of dollars are being pumped into the industry to accelerate adoption of enabling technologies by 2015, and to promote its successful implementation as defined by Meaningful Use criteria. Providers—from those working within the largest for-profit integrated delivery systems to community hospitals struggling to stay afloat to the solo practice—are trying to figure out how to receive the government incentive, adopt the technology all while trying to take care of patients in one of the most challenging era’s for both the US economy and its failing healthcare system.

The magnitude of the change related to adoption of health IT notwithstanding there is also significant change simultaneously occurring in the very professional organizations that support the delivery of care. Nursing represents the largest segment of the healthcare workforce with more than 3 million registered nurses in the United States. The nursing profession has struggled for decades with core professional definition around who nurses are, what nurses do, how to educate the next generation of professionals and perhaps most importantly how to raise the voice of nursing and lead the national effort to transform healthcare as we know it.

On Oct. 5, 2010, the Robert Wood Johnson Foundation and the Institute of Medicine (RWJF/IOM) released a landmark report that gets to heart of the crisis within the nursing profession. The Future of Nursing: Leading Change Advancing Health is seen by many as a crucial work for the profession and a call to action for all. This consensus report endorsed by physician and nursing leaders alike explores the issues facing the nursing profession today and offers recommendations for the future. While the details of the recommendations are emerging there is little doubt that nursing informatics professionals will be called upon to offer their expertise in the transformation of nursing.

According to the 1989 Graves and Corcoran definition, nursing informatics is a specialty that combines nursing science, computer science and information science. The American Nurses Association has formally recognized the specialty since 1992 and its credentialing agency, the American Nurse Credentialing Center offers the opportunity for aspiring informatics nurses to gain Board Certification in the specialty.

According to a recent survey released by HIMSS, today's informatics nurses are increasing in number. The results, as compared to previous surveys from 2004 and 2007, continue to suggest that nurse informaticists play a critical role in the implementation of various clinical applications including clinical/nursing documentation and clinical information systems, computerized provider order entry (CPOE) and electronic medical/health records. Furthermore, in comparison to previous surveys, the 2011 salary data suggests a substantial increase for nurse informaticists as the average salary increased by 17 percent from 2007 and 42 percent from 2004. The value that informatics nurses bring is well recognized within the profession as evidenced by the results of this survey. Nursing informatics as a specialty within nursing, therefore is well positioned to assist the profession in meeting the challenges identified in The Future of Nursing.

The Future of Nursing identifies eight key recommendations for the profession to consider, organized into three broad categories of Leadership, Practice and Education. (See Figure 1).

The report shows that nursing practice is challenged on many fronts. One example explored in the report relates to the disparity in practice between Advance Practice
The nursing profession has struggled for decades with a core professional definition around who nurses are, what nurses do, how to educate the next generation of professionals and perhaps most importantly how to raise the voice of nursing and lead the national effort to transform healthcare as we know it.

Registered Nurses (APRN) across the United States. Despite national standards for education and specialty certification of APRNs there is great inconsistency from state to state in how APRNs are allowed to practice. In some states, APRNs are allowed to practice independently, others allow for some autonomy as it relates to prescription writing and many require a collaborative arrangement with a physician to diagnose, treat and prescribe. Even that level of collaboration however, varies from state to state.

As nursing informatics professionals know, the role of technology and informatics to support nursing practice is crucial; regardless of practice setting. In the example cited in the report above with APRNs, informatics can help promote the value of this specialty practice through data and information. APRNs for example may be eligible for Meaningful Use funding under the Medicaid program, as they meet the Medicaid definition of an Eligible Professional. Interestingly, these same practitioners are not eligible for incentive dollars from the Medicare program further accentuating the disparity.

That disparity notwithstanding, APRNs and their nursing informatics colleagues should work hand in hand to ensure that the HITECH incentives are obtained to help support practice. Additionally, and perhaps more importantly, informatics skills and competencies are fundamental to demonstrating outcomes of the care provided by APRNs. Collecting and assimilating the data collected in this practice setting will be essential to measurement and reporting of outcomes. This is also true for every nurse practicing in every environment. Without good data and information to demonstrate the value of nursing practice nurses will not be able to move the profession forward.

**EDUCATION**

Nursing has struggled for decades with entry to practice and the multitude of educational pathways available to enter the profession. The profession has also struggled with the ability of its academic institutions to keep pace with rapid advancements in medicine as well as significant changes in the practice environment and the role of modern day nurse. One of the most challenging issues in the education arena, however, is the aging of our faculty.

**Key recommendations from the report related to nursing education include:**

- Increase the proportion of nurses with a baccalaureate degree to 80 percent by 2020.
- Double the number of nurses with a doctorate by 2020.
- Ensure that nurses engage in life-long learning.

These recommendations are bold and aggressive and will require close collaboration between practice and academia. Informatics competencies will need to be defined for all levels of practice and will need to be built into revised nursing curricula. Deans of schools of nursing will need to move away from thinking about informatics as a standalone course and move toward embedding informatics competencies in all
NURSING INFORMATICS: INFORMATICS’ ROLE IN THE FUTURE OF NURSING

During times of great change stakeholders look to leadership for guidance. Never before in the history of the nursing profession has the need for leadership been greater.

Simulation technology is another great example of how academia and informatics can come together to help achieve the goals identified in the report related to transition to practice. While more and more institutions are implementing simulation laboratory environments few have the informatics experts on staff to be able to thread through the concepts of data, information, knowledge and wisdom to support critical thinking. Rather, simulation labs are implemented with a task- or skills-based focus. Again, informatics experts can help in the design and implementation of effective simulation environments.

LEADERSHIP
During times of great change stakeholders look to leadership for guidance. Never before in the history of the nursing profession has the need for leadership been greater. While there are many great nursing leaders there are few who are able to advocate for the profession at a national level and to directly define, shape and influence public policy.

The key recommendations from leadership include:

- Expand opportunities for nurses to lead and diffuse collaborative improvement efforts.
- Prepare and enable nurses to lead change to advance health.

Nursing informatics leaders and nursing management leaders will need to join forces to collectively address these recommendations. All nursing leaders must understand the implications for informatics in practice and must demonstrate by example.

CONCLUSION
The last of the eight key recommendations from the report is: Build an infrastructure for the collection and analysis of inter-professional health care workforce data

This recommendation speaks directly to the nursing informatics community and is a call to action. Building the infrastructure will require close collaboration with nursing informatics professionals and other members of the inter-professional team who not only understand the underlying data requirements but can offer to assist in translating and mining that data into meaningful information about the workforce. Informatics nurse stakeholders are uniquely positioned to help define national, minimum data sets that can be used as part of inter-professional workforce surveillance. Nursing informatics professionals have a strong history of inter-professional collaboration and will need to embrace, own and be accountable for this recommendation.

These are historic times for the healthcare industry and the profession of nursing. Informatics provides an opportunity to help transform not only the care delivery system but the very professions it relies on to deliver safe, effective and evidence-based care.
Exit Strategy

Ending an Existing Software License Agreement

To keep my column topical, I try to write about issues that frequently arise in my practice. It may not always be clear to me why a certain topic comes up repeatedly during any given period of time, but I trust that if several of my clients are thinking about it, then chances are there are others who are interested.

Lately there have been a number of clients who, for a variety of reasons, are not happy with their software vendors. Some may be having difficulty getting their product to work correctly. Others may be looking to change products. Regardless, the issues that one must consider are similar. Hopefully, you planned ahead when negotiating your license agreement and included language in the contract that will help you at the end of the relationship with the vendor. A word of caution—consult with your legal advisors before taking any action to terminate a contract.

NON-BREACH SITUATIONS

License payments. If you are seeking to terminate with a vendor when there has been no breach of contract, the first thing to look at is the type of license that you purchased. Software licenses are either perpetual or term licenses. If you have a perpetual license, you paid the entire license fee at the beginning of the contract. You will not owe any additional fees with regard to the software license itself. Hopefully, you’ve gotten enough use out of the software to justify the license fee. If you have a term license, you have been paying on an ongoing basis (e.g., an annual license fee) for the term of the agreement. Most term license agreements have an initial term (anywhere from one to 10 years), with renewal terms that are typically one year in length.

Next you will need to determine where you are in the term. Has the initial term expired? If not, how many years are left on the initial term and how much is the license fee for the remainder of the term? Is there any room to negotiate if you agree not to use the software for the remainder of the initial term?

If the initial term has expired, many term licenses are set up to automatically renew for a set term (e.g., consecutive one-year terms) unless either party gives written notice of its intent not to renew a set number of days prior to the renewal date. If the initial term has expired, you may now be licensing the software on a year-to-year basis. You will need to determine from the contract the exact procedure laid out to give notice that you do not want to renew again at the end of your current term (whether that be the initial term or a renewal term).

Therefore, in order to terminate the license and avoid automatic renewal, you will need to provide written notice to the vendor pursuant to the notice provision of the contract the stated number of days in advance of the renewal date.

Maintenance and support payments. Whether you have a perpetual or term license, you are likely also paying for maintenance and support services. Some licenses, especially term licenses, have the support fee included in the license fee, so the maintenance and support services would also be terminated as the term license is terminated (as described above). Most perpetual licenses have a separate maintenance and support fee. The termination of maintenance and support is very similar to the termination of the term license. Maintenance and support services typically have an initial term (anywhere from one to 10 years), with renewal terms that are commonly one year in length. You will need to determine where you are in the term.

If the initial term has expired, maintenance and support services are frequently set up to automatically renew for additional, consecutive terms (e.g., one-year terms) unless either party gives written notice of its intent not to renew a certain number of days prior to the renewal date. Once again, you will need to determine from the contract the exact procedure laid out to give notice that you do not want maintenance and support services to renew again at the end of your current term (whether that be the initial term or a renewal term). Therefore, to terminate maintenance and support services, you will need to provide written notice to the vendor pursuant to the notice provision of the contract the stated number of days in advance of the renewal date.

Other payments. Usually there are also other service fees included in a software license agreement. If we are well into your agreement, you probably paid these fees early on. No additional fees are typically due, but you may want to do an analysis as to whether if you’ve gotten your money’s worth on these initial service payments (e.g., you wouldn’t want to pay a large implementation fee, only to move to another vendor two years later). If there are other ongoing service fees, they are typically structured similarly to maintenance and support services, so the analysis above would likely apply.
There are a number of reasons why you may want to part ways with your software vendor. Understanding the applicable contractual provisions will help you to navigate your way through the process.

**TERMINATION BASED ON BREACH OF CONTRACT**

Another reason to attempt to terminate a contract is because the software is not working. In this case, you may have more options to terminate sooner, but it is definitely not going to be simple. You will need to establish that the vendor breached the contract. If you are in the initial stages of the agreement, you may still have acceptance testing language or a warranty stating that the software will perform in accordance with certain criteria, including the user documentation and specifications.

You will need to review the contract language in these areas to determine if the issue you are experiencing is covered by the warranty and/or the acceptance testing provision. Assuming it is you then need to review the contract to determine if there are any limitations on your remedies for the breach of contract. One area this might occur is in the actual acceptance testing or warranty section itself. If you agreed to any “sole and exclusive” remedies when you negotiated the contract, you may be limited in your remedies to what is stated (e.g., the remedy might be limited to the amounts paid only for the specific product or service at issue). In addition, the limitation of liability section may further limit your remedies if you agreed to limit the vendor’s liability.

**OBLIGATIONS UPON TERMINATION**

Most contracts contain obligations for the parties upon termination. For example, the confidential information section of the agreement may state that, upon termination, each party must return or destroy the other party’s confidential information. This would likely include the software and documentation. Some agreements require the user to provide some sort of written certification that the software and documentation have been destroyed. If your software vendor has possession of your protected health information, your business associate agreement may contain certain requirements of the vendor, which you should consider following up on.

In summary, there are a number of reasons why you may want to part ways with your software vendor. Understanding the applicable contractual provisions will help you to navigate your way through the process so that your organization can cleanly move on to the next vendor. And don’t forget to plan ahead with the new vendor for the eventual, inevitable parting of ways. **JHIM**
Innovation
A Snapshot of mHealth’s Moving Target

It’s not often that we get to witness—or let alone recognize—a watershed moment in US healthcare. But that moment is happening now. In just three years, mobile healthcare has blossomed at incredible speed and stirred tremendous excitement—and hype—within the industry. Few technologies have the potential to radically alter the current paradigm in so many areas—patient care, clinical workflows and healthcare delivery, consumerism, among others—as mobile solutions.

From smartphones and tablets to apps, body sensors and teledicine, these compact, portable tools promise foundational shifts in healthcare quality and delivery that will dramatically impact stakeholders at every level—from patients to C-suite executives—and deliver on the elusive promise of quality care, coordination and cost-savings.

Mobile innovation in healthcare is being driven by the tech sector, by cost-saving initiatives by providers and payers and by overwhelming demand from consumers. The tools of mobile computing—smartphones, PDAs, tablet PCs, patient monitoring devices and an avalanche of apps among them—are opening new vistas of opportunity for clinical collaboration.

It’s an evolutionary cycle. Telemedicine, voice recognition and home monitoring have been around for years, but the current wave of mHealth product innovation is being driven by the convergence of form, function, a burst of entrepreneurship and favorable economics. mHealth devices have made dramatic leaps forward in terms of cost, bulk, weight, durability and performance. And there are thousands of mobile healthcare apps already on the market, with more on the way. They include e-prescribing, medical calculators, decision support tools, personal health records, health and fitness, patient medical and eligibility queries, for starters.

The explosion of mHealth is more than just a technology play. Mobile health solutions support new treatment modalities, such as accountable care organizations (ACO), health information exchanges (HIE) and patient-centered medical homes.

Most significantly, mHealth is democratizing healthcare, giving people the ability to understand and play an active role in addressing their health issues. mHealth provides a mechanism for healthcare consumers—patients with both temporary and chronic health issues, as well as the healthcare conscious, the family caregiver and the “worried well”—to become responsible stewards of their own health.

But if you think mHealth is all about smartphones and iPads, then you aren’t grasping the wealth of mHealth devices and software solutions that are proliferating throughout the spectrum of care, and the revolutionary impact this suite of technologies is having on the industry.

mHEALTH APPS

The potential universe of mHealth applications spans the payer, provider and healthcare consumer markets. There are literally thousands of mHealth apps and software programs available on the market today—with hundreds more hitting the marketplace every month. One 2010 study estimated that more than 7,000 health-related apps are available through Apple alone. Nearly 3,000 healthcare-related apps are available through other mobile providers.

Most mobile apps used by providers are drug and clinical references, but studies show that apps for e-prescribing and clinical decision support are quickly gaining ground.

For example, the Medscape Mobile, an iPhone application, is essentially an extensive and interactive drug reference with images and videos of medical conditions in addition to in-depth and up to date medical news. Yet another popular digital drug guide for smartphone is Epocrates, which is currently used by more than 100,000 physicians.

Skyscape Medical Resources offers iPhone and Android, Blackberry and Windows Mobile applications with contents such as outlines in clinical medicine, a medical calculator and a drug dosing tool.”

APPS, WEB OR MESSAGING?

Beyond apps, many people believe that HTML5 and other standards will allow mobile Web apps to catch up, surpass or merge with the capability of native OS apps that must be developed separately for each platform and tied to a closed-system app store model.

An important quote from Google founder Sergey Brin talked about this merger of Web and native apps at a recent I/O conference. Web apps are now able to go offline, and they can have richer graphics thanks
to HTML5.

“It’s getting similar to app frameworks,” he says. He also notes that there are benefits to using web apps versus native apps, such as the lack of installation, and certain aspects of security. “It’s headed in a positive direction, but these are fairly recent developments,” Brin says.

Another trend that extends beyond the structure of the app is the use of text messaging in public health campaigns. Text-4Baby is a popular program with significant results in prenatal care. Some of the largest campaigns have been HIV campaigns that have sent billions of messages to change attitudes and behaviors.

PERIPHERAL DEVICES

But the mobile health universe encompasses far more than just retail commodities like smartphones and tablets. A large host of peripheral devices already are available on the market, and scores of others are currently in development. What these disparate devices have in common is that they allow providers to perform and patients to receive diagnostic care and treatment remotely—whether the location is the patient’s home or a distant satellite clinic, miles from a central healthcare organization.

Dr. Patrick Soon-Shiong, Chairman of the Chan Soon-Shiong Family Foundation and Chairman and CEO of the Chan Soon-Shiong Institute for Advanced Health, National LambdaRail, the Healthcare Transformation Institute and NanWorks, LLC, summarizes the needs and promise of mHealth including instant access to evidence-based medicine available on a “Medical Information Highway” (Soon-Shiong).

The plan to use mobile technology in conjunction with cloud-based models for a secure, high-speed ecosystem that can influence health—instead of just healthcare. “It includes state of the art semiconductor chips, switches and encryption technologies, augmented reality, novel object and voice recognition technologies, broadband telecommunications services and ultra-low power remote monitoring devices.”

Mobile apps for healthcare will continue to be important, but other devices and peripherals that link to smartphones as a hub form an even broader picture of the capabilities of the mHealth ecosystem. Examples include a digital stethoscope, digital blood pressure monitor (connected), Bluetooth wireless digital weight scale, full body sensor body fat and composition monitor, fingertip pulse oximeter, blood glucose meter, Avacem MOD, armband weight management system, sleep tracking systems, fitness watch with GPS and biosensing and many more.

TELEMEDICINE, REMOTE MONITORING AND ROBOTICS

Another emerging trend that may influence the use of mobile technology is telemedicine. There are several categories of telemedicine: store-and-forward, remote monitoring, and interactive services. Store-and-forward describes acquiring medical data, such as medical images, and transmitting the data to a physician or medical specialist at a remote location. Remote monitoring as a tool of telemedicine is focused principally on disease and condition management. Interactive telemedicine services provide real-time interactions between patients and providers via voice, text and data.

The practice of remote medicine through the use of advanced telecommunications, robotics and other distributive means has influenced everything from doctors who perform consults remotely to specialists linking across the globe using high-resolution telepresence systems and for efficiency in trauma units like the example from University of Miami and Ryder Trauma Center.

Telemedicine also can be used to link eConsults with EMRs. Mobile access using video teleconferencing and telepresence systems will enable real-time, anywhere access for doctors and healthcare workers. This also could make initial record input and dispatch more efficient as patients are being admitted during emergency transport. In some areas of medical education curriculum is being offered and delivered over mobile devices, such as Tuft University’s TUSK system.

COMPLEMENTARY TECHNOLOGIES

There are huge opportunities for complementary vendors to partner and bolt together boutique solutions within a mobile architecture. Several independent health technologies illustrate this point. Real-time location systems (RTLS) are being merged with mobile devices to accelerate patient throughput, manage staff, monitor at-risk family members and schedule utilization of high-value equipment.

Speech recognition tools are being employed via mobile devices for documentation, charge capture, scheduling and notes. Mobile video conferencing mated with robotics has spawned a new market segment—telepresence. In each case—RTLS, speech recognition and video—boutique health technologies are innovating to perform in a mobile environment. mHealth solutions are being designed with the user experience in mind—there are now biometric monitors that capture data via ear buds, mHealth coaches that intuitively modify care plans as new data is obtained, and non invasive diabetes testing and reporting tools. We are constantly learning about new applications of mHealth solutions, of ways that healthcare delivery is being reinvented via mHealth solutions, and ways that mHealth is being married with complimentary technologies to fundamentally alter healthcare’s workflows, economics and the patient experience.

Within the next few years mHealth is likely to evolve in unexpected ways, but one thing seems clear: mHealth is poised to evolve beyond apps and even beyond peripherals and systems. Perhaps it will transition toward more organic and embedded technologies that will advance beyond external cognitive and physical prosthetics, as represented by current handheld mobile phones, into wearable pervasive pill-sized cameras and remote telerobotics now being deployed which were only a dream several years ago.

mHealth will genuinely personalize healthcare by virtue of its convenience, connectivity, clinical and economic coherence. Its organizing principle is alignment—alignment of the inputs to healthcare—the verticals, the venues, the spectrum of caregivers, the technologies, the workflows—within an integrated, interoperable system architecture that is efficient and accessible.
mHealth will genuinely personalize healthcare by virtue of its convenience, connectivity, clinical and economic coherence.

In sum, the mHealth ecosystem is going to change the way that each of us experience healthcare.

mHealth isn’t just a disruptive force in healthcare—it’s a displacement force that is reinventing healthcare delivery. And mHealth isn’t just a collection of apps and devices—it’s evolving through smart systems into its own ecosystem. That ecosystem is still in a formative stage and some prime determinants—standards, security layers, compliance and regulation—will have a heavy influence on the adoption curve and the proliferation of mHealth solutions. JHIM

David Metcalf, PhD, has more than 20 years of experience in design and research of web-based and mobile technologies converging to enable learning and healthcare. Recent efforts include the development of mobile technology strategies for Tufts University and University of Central Florida medical schools. He is co-editor of the 2012 HIMSS book mHealth: From Smartphones to Smart Systems. (Link title to: http://marketplace.himss.org/OnlineStore/ProductDetail.aspx?ProductId=3379).

Rick Krohn, MA, MAS, is President of HealthSense Inc., a consultancy specializing in Health IT corporate strategy, strategic marketing, communications, business development and technology application. He can be reached at 912-220-6563. He is co-editor of the 2012 HIMSS book mHealth: From Smartphones to Smart Systems. (Link title to: http://marketplace.himss.org/OnlineStore/ProductDetail.aspx?ProductId=3379).
ANY OF US have used the term “on demand” to talk about inventory or help for accounting, administrative or clinical support staff. Can we also apply this to the healthcare chief information officer? The short answer is yes, but I know this may not resonate well for some.

On demand means just that, bring the resource in when you need it and move it out immediately when you don’t need it. I have worked the role as a CIO and as a CIO consultant in the healthcare provider setting for more than 25 years. I have many fond memories of the role I played as a hospital and system CIO. Understanding the culture of the organization and being imbedded in the management team are certainly key elements that make up many of our successful CIOs today.

However, the current times for the healthcare CIO are not as they were before, and there are some options that every CIO, CEO, CFO and COO must take into account as they manage their organizations through these “perfect storm” days. Executives today must figure out how to leverage technology and meet the requirements for Meaningful Use, ICD-10, health information exchanges, accountable care organizations, patient-centered medical homes and using social media to link providers and patients.

Having one person oversee all of these initiatives and leverage the technologies while balancing reduced budgets is becoming more than a one person job. Large providers might have the ability to hire more highly skilled staff to support the CIO in these efforts. Smaller providers typically do not have the budgets in IT salaries to support this. I think the time is right to consider CIO skills “on demand” for both large and small provider organizations.

The demands for integrating technology in our healthcare environments can be overwhelming. Healthcare has always been recognized as a laggard in its use of technology—in most cases, 10 years behind or more. You only need to see how we deal with paper for information and the spider maze of insurance company billings to appreciate how far behind we are. Even the government has recognized this and that better patient care and outcomes can be achieved by leveraging technology. Unfortunately, it seems like we are trying to make up 10 years of technology gaps in three years or less.

Here are some real life examples and experiences. A CIO needs to have someone he or she can trust and be at the table when working vendors, consultants and even the senior management team. This can be a seasoned CIO who is available on a full- or part-time basis and is acting as the extra arms and legs that healthcare provider CIOs need these days, typically on one or several major initiatives. Another example is the “Mentor CIO.” Typically, this is a former CIO who has “been around” and is brought in to help mentor a new or up and coming CIO. Having a part-time mentor can be an excellent way to groom your new CIO and make sure that the projects and investments that support the organization’s strategies are adequately spent.

Finally, another example is “I am not sure I have the right CIO.” As the demands increase on the use and dollars for technology, many CEOs, CFOs and COOs want to avoid costly technology disasters and are not sure their CIO has the ability to get them through this “perfect storm”. Bringing in the outside CIO, sometimes working alongside your current CIO can provide the assurance that the executives need, especially when many boards are asking the question, “Are we sure we are doing the right thing in our technology investments?”
I would encourage healthcare executives to consider ‘on demand’ resources for CIOs. This applies whether the need is interim, strategic, project specific, mentorship or just a change in IT direction.

There is another force in the marketplace that is making the on demand CIO attractive. Many seasoned CIOs who used to retire early are now continuing to work for many reasons—the stock market impact on their retirement earnings certainly is one. A significant number of talented individuals are available for short-term projects or part-time work. These are typically CIOs who don’t want to deal with the day-to-day operational issues, but welcome the opportunity to assist with focused efforts.

One thing we are all aware of is that the constant in healthcare is change. When a new CEO comes onboard, they will take a hard look at their technology leader and decide to make changes if they feel the organization needs one. Many times this does not mean the CIO was not a qualified candidate. There are many reasons for change in management teams and the negative perception of someone because they leave an organization is many times, not a negative one.

The counter to the above strategies is to hire a consultant, typically from one of the large consulting companies. This does not always mean that you are hiring the best candidate but typically gives management some assurance since the consultant has the backing of a large firm. Sometimes this can be effective, sometimes not.

In summary, I would encourage healthcare executives to consider “on demand” resources for CIOs. This applies whether the need is interim, strategic, project specific, mentorship or just a change in IT direction. It can be effective both from a cost and strategic viewpoint. The market forces have put the biggest challenge we have ever seen on the healthcare CIO. Additionally, it has also provided good seasoned CIOs that are available to help. We are always looking for innovative ways to leverage technology, let's apply this to the technology leadership as well. JHIM
THE PROLIFERATION of mobile technology into the daily lives of our workforce has forever changed the expectations placed on IT departments and data accessibility within healthcare. For years IT departments have recommended the centralization of data management, access and reporting. These recommendations often came with significant investments in enterprise systems, staff and governance structures designed to control the flow of data to clinicians, researchers and business units.

The challenge is that the information access requirements evolved faster than healthcare IT departments’ abilities to adapt systems to meet the needs of a consumer workforce. Fortunately, many IT departments followed the trends of desktop virtualization and mobile device management, with the promise of cost reduction, risk mitigation and bring-your-own-device (BYOD) strategies. Fundamentally, the aforementioned benefits can be achieved through implementing these strategies. However, today and in years to come, one of the most significant values these tools bring to healthcare will be enabling access to data in a form that the consumer workforce can rapidly consume.

Desktop virtualization and mobile device management (MDM) strategies enables the flexibility to adapt data governance and accessibility models at pace more consistent with the evolving consumer audience expectations. They will achieve this benefit through enabling secure, profile-based, federated data analysis.

Federated data analytics is, at its core, the dissemination of control over report development. IT departments that focus on this approach and leverage their investments in desktop virtualization and MDM will be able adapt to a constantly changing consumer device market while meeting the data accessibility needs of their consumers.

For example, desktop virtualization can enable access to many legacy reporting environments, giving anywhere, any device access to data in a usable form factor. MDM has the ability to leverage vast lists of consumer applications to enable secure access to enterprise data. The combination of these strategies gives data consumers the ability to access information on any device and through the application of their choice. The challenge is re-thinking the function of IT within the governance process.

One federated approach is to rethink data management into a three tiered organizational system. Each tier has its own governance, staff, and function with respect to the delivery of technology and data to consumers. The central tier or inner core noted in Figure 1 is managed and lead by information technology resources, primarily focused on maintaining the integrity, availability of the data, and the development of enterprise wide reporting services for the outer two tiers.

The middle tier, also noted in Figure 1, exists to provide more service line focused
The proliferation of mobile technology into the daily lives of our workforce has forever changed the expectations placed on IT departments and data accessibility within healthcare.

The outer tier in Figure 1 is the consumer level of data accessibility and reporting. This is the tier that is enabled through desktop virtualization and MDM as they are given the most flexibility to modify data variables in an on-demand fashion. These users are given access to the centralized reporting environments that have been created to answer known questions about clinical, business or research challenges, but they also are provided secure access to data through applications and devices familiar to them. This familiarity and level of accessibility will make them highly efficient consumers of enterprise data and change the way information technology can bring benefit the healthcare workforce.

As such, IT departments that adopt federated data accessibility models leveraging their investments in desktop virtualization and MDM will not only meet the expectations of a consumer workforce, but increase the benefit of information technology to the organization. JHIM

**FIGURE 1: Levels of Data Access**

Ryan A. Terry currently serves as a Division Chief Information Officer and Chief Information Security Officer for University Hospitals in Cleveland Ohio. Terry has more than 14 years of experience leading organization redesign, technology, and consulting initiatives for variety global and national corporations. During his career he employed various management, process, and organizational change methodologies to successfully promote the adoption of technology as a means to sustainable culture change. Recently he lead technology components for University Hospitals $1.4 Billion Vision 2010 construction program. A published author, Ryan has written articles on Supply Chain Management, Vendor Management, and technology infrastructure in healthcare. He serves on several CIO Advisory boards for both public and privates sector organizations and is an active member of his community. Originally from the Chicago area Terry has his undergraduate degree from the University of Illinois, Urbana-Champaign and his Master’s in Business Administration from Case Western Reserve, Weatherhead School of Management.
FOCUS  MOBILE HEALTH

Lessons from Project HealthDesign

Strategies for Safeguarding Patient-Generated Health Information Created or Shared through Mobile Devices

By Deven McGraw, JD, MPH, LLM; Helen R. Pfister, JD; Susan R. Ingargiola, MA and Robert D. Belfort, JD

ABSTRACT

Robert Wood Johnson’s Project HealthDesign is exploring a vision of personal health records as tools for improved health decision-making by both patients and providers. In the latest phase, researchers are providing patients with smartphones to aggregate and send observations of daily living (ODLs) to healthcare providers, providing a richer picture of a patient’s day-to-day health status. Patients’ use of mobile devices to generate and communicate health information subjects this information to unique security risks for which solutions have not yet been discussed. When healthcare providers handle electronic, identifiable health information, they are subject to the HIPAA Security Rule. But HIPAA regulates providers, not patients. This paper discusses the factors that should be considered when protecting patient-generated health information created on or shared through mobile devices. It also recommends strategies for securing patient health information on mobile devices and implementing technical safeguards to ensure general device security.

KEYWORDS

mHealth, HIPAA, security, patient-generated health information, mobile device.
TABLE 1: Project HealthDesign Grantee Teams’ Use of Mobile Devices

<table>
<thead>
<tr>
<th>Devices Given to Patients</th>
<th>Information Flow</th>
<th>Use of SMS/Text Messaging?</th>
</tr>
</thead>
<tbody>
<tr>
<td>iPod Touch</td>
<td>ODLs are sent from smartphone to HealthVault through an app on the smartphone.</td>
<td>Yes. Health coaches send and receive SMS messages to patients.</td>
</tr>
<tr>
<td>Smartphones and scales</td>
<td>ODLs are sent from smartphone to HealthVault through an app on the smartphone.</td>
<td>No.</td>
</tr>
<tr>
<td>Smartphones</td>
<td>ODLs are sent from smartphones to project servers (data from sensors flows separately). Patients can access reports through an app on the smartphone.</td>
<td>No.</td>
</tr>
<tr>
<td>Smartphones and sensors</td>
<td>ODLs are sent from smartphones to project servers (data from sensors flows separately). Patients can access reports through an app on the smartphone.</td>
<td>No.</td>
</tr>
<tr>
<td>Sensors and laptops</td>
<td>ODLs are sent from laptops to HealthVault. Reports are generated, which clinicians and patients may view on their laptops.</td>
<td>No.</td>
</tr>
</tbody>
</table>

potential obstacle to more widespread use of such tools by patients to generate and share health information.

Healthcare providers are subject to the Health Insurance Portability and Accountability Act (HIPAA) Security Rule, which outlines the safeguards that must be used to secure electronic, individually identifiable electronic health information (known as ePHI). But HIPAA regulates providers, not patients. When patients generate health information using applications on their mobile devices—whether they share it with their healthcare providers or simply use it to engage in their own self-management activities—the Security Rule does not apply.

Project HealthDesign involves activity that is neither provider activity subject to HIPAA nor autonomous patient activity for which providers could not conceivably be held responsible. Instead patients are collecting and transmitting ODLs and other health information in a research environment administered and overseen by healthcare organizations. This unique environment raises challenging questions regarding the responsibility of these organizations for information security.

As part of Project HealthDesign, each grante team collects a variety of ODLs from patients using different technologies. Table 1 summarizes how each team is using mobile devices to collect ODLs and incorporate them into clinical care. While these activities are part of a research study, it is not hard to envision an environment in which healthcare providers routinely encourage patients to use mobile devices to collect and share clinically relevant information such as ODLs. As reimbursement models for healthcare providers move toward episode of care-based bundling, shared savings incentives and capitation, there will be greater incentives for providers to more actively engage patients in daily self-management and care coordination.

This paper suggests strategies for promoting the security of health information generated by patients and shared with healthcare providers using mobile devices, an area where clear legal standards

Table 1: Project HealthDesign Grantee Teams’ Use of Mobile Devices

- **Project Name**: in Touch, Estrellita, BreathEasy, Crohnology, MD, dwellSense
- **Devices Given to Patients**: iPod Touch, Smartphones and scales, Smartphones, Smartphones and sensors, Sensors and laptops
- **Information Flow**: ODLs are sent from smartphone to HealthVault through an app on the smartphone.
- **Use of SMS/Text Messaging?**: Yes, No
do not exist. The paper draws on lessons learned by the Project HealthDesign grantee teams as they have attempted to strike a balance between data security and clinically effective information exchange by patients. The strategies reflect the unique “middle ground” environment in which Project HealthDesign grantees operate, with patient-generated information not subject to the HIPAA Security Rule, but maintained and transmitted as part of a research study designed, promoted and financially subsidized by healthcare organizations. While this environment may not be frequently encountered today, it may become a more prevalent framework for managing chronic illness in the future. Thus, the strategies discussed herein may have broader application in the future.

SPECIAL RISKS PRESENTED BY MOBILE DEVICES

Mobile devices such as smartphones pose unique risks to health information, such as loss or theft, unauthorized access, malware (viruses) and cloning.6 Since 2009, HIPAA-covered entities have been required to report breaches of unsecured health information affecting 500 or more individuals.7 These breach reports strongly suggest that risks related to the loss, theft and unauthorized access of mobile devices are likely to be more significant than sophisticated external threats. This threat assessment is an important consideration in determining the type of safeguards that are appropriate in properly balancing security and clinical efficacy.

STRATEGIES FOR SAFEGUARDING PATIENT-GENERATED HEALTH INFORMATION CREATED OR SHARED THROUGH MOBILE DEVICES

HIPAA Security Rule. Even where the HIPAA Security Rule does not apply, it is a useful starting point for understanding the types of safeguards that may be appropriate. At the same time, any set of strategies must take into account the differences between an environment of provider-generated information, for which the Security Rule was designed, and an environment of ODLs and other information collected and transmitted by patients. Healthcare providers have direct control over their workforce and can require compliance with various security measures, but providers have no

The key Security Rule standards relevant to patients’ use of mobile devices to generate and share health information are listed in Figure 1.

![Figure 1: Key Security Rule Standards Relevant to Patients’ Use of Mobile Devices to Generate and Share Health Information](image_url)

- **Access Control**: 164.312(a)(1)
  - Unique User Identification
  - Emergency Access Procedure
  - Automatic Logoff
  - Encryption and Decryption

- **Audit Controls**: 164.312(b)
  - (R)

- **Integrity**: 164.312(c)(1)
  - Mechanism to Authenticate Electronic Protected Health Information

- **Person or Entity Authentication**: 164.312(d)
  - (R)

- **Transmission Security**: 164.312(e)(1)
  - Integrity Controls
  - Encryption

*We have identified “audit controls” and “integrity” as security rule standards relevant to patients’ use of mobile devices to generate and share health information. However, based on the experiences of the Project HealthDesign grantee teams, there does not appear to be a need for a patient to log and audit the use of his or her mobile device, since it is generally only the patient who will have access to the device (the provider has access to the information sent by the patient from the device). Likewise, there should be no need for a patient to take steps to ensure the integrity of the EPHI the patient stores and/or transmits through the mobile device since the risk of alteration or destruction is low.

The Security Rule also requires providers to assess the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI. In a “risk analysis,” providers must often evaluate and weigh competing concerns. The experiences of the Project HealthDesign grantee teams indicate that securing patients’ health information without overburdening information-sharing by patients is a challenge. Patients do not want to be inconvenienced, and their ability (in terms of knowledge and resources) to implement security measures on their mobile devices is limited. Taking the grantee teams’ experiences into account, the following key questions should be considered in a risk analysis related to the protection of patient-generated health information created on or shared through mobile devices:

- **What is the risk to the patient’s health information?**
- **What is the risk to the patient’s confidentiality, integrity, and availability?**
- **What is the cost to the provider of implementing security measures?**
- **Is the risk to the patient’s health information outweighed by the benefits of using mobile devices to generate and share health information?**

Thus, some specific safeguards are required by the Rule; others are listed as “addressable” specifications.9

The data collected and transmitted by patients via mobile devices is likely protected by HIPAA. However, there may be additional safeguards necessary to protect the health information exchanged through mobile devices. Providers should consider the unique risks posed by mobile devices and implement strategies that are appropriate for the entity’s particular size and organizational structure, as well as the nature of the risks to its EPHI.8 Thus, some specific safeguards are required by the Rule; others are listed as “addressable” specifications.9

The Security Rule also requires providers to assess the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI. In a “risk analysis,” providers must often evaluate and weigh competing concerns. The experiences of the Project HealthDesign grantee teams indicate that securing patients’ health information without overburdening information-sharing by patients is a challenge. Patients do not want to be inconvenienced, and their ability (in terms of knowledge and resources) to implement security measures on their mobile devices is limited. Taking the grantee teams’ experiences into account, the following key questions should be considered in a risk analysis related to the protection of patient-generated health information created on or shared through mobile devices:

- **What is the risk to the patient’s health information?**
- **What is the risk to the patient’s confidentiality, integrity, and availability?**
- **What is the cost to the provider of implementing security measures?**
- **Is the risk to the patient’s health information outweighed by the benefits of using mobile devices to generate and share health information?**

Thus, some specific safeguards are required by the Rule; others are listed as “addressable” specifications.9

The data collected and transmitted by patients via mobile devices is likely protected by HIPAA. However, there may be additional safeguards necessary to protect the health information exchanged through mobile devices. Providers should consider the unique risks posed by mobile devices and implement strategies that are appropriate for the entity’s particular size and organizational structure, as well as the nature of the risks to its EPHI.8 Thus, some specific safeguards are required by the Rule; others are listed as “addressable” specifications.9
• **Complexity and cost.** Does a patient's smartphone come with built-in security tools (e.g., encryption), or would the patient have to buy, download and install third-party software?

• **Patient ability.** Could the patient reasonably install and implement the software?

• **Effect on clinical care.** Will implementing an access measure—like a password—lessen the patient's willingness to report health information?

• **Measure of risk.** Will ePHI included on or transmitted through a patient's mobile device cause the patient harm or embarrassment if breached?

When healthcare providers are providing their patients with mobile devices and encouraging them to share their health information as part of a provider-led initiative, they may take responsibility for implementing certain security activities on the patient's behalf. While patients using mobile devices outside of a provider-led initiative will likely make security decisions with minimal provider involvement, providers can and should be more involved in security when the provider is designing and subsidizing the information exchange. These facts are critical to the risk analysis.

For example, if a provider expects patients will simply not use smartphones that automatically log off after a specified period of time, or if patients will feel inconvenienced by having to input a password, the provider should take these facts into account when determining what security measures to implement directly or to recommend a patient implement. Because the decision to protect the patient's health information ultimately rests with the patient, security measures should be recommended with the likelihood of patient compliance in mind.

**TRANSMISSION SECURITY AND ENCRYPTING DATA AT REST**

Healthcare providers must implement technical security measures to guard against unauthorized access to ePHI being transmitted over an electronic communications network. The Security Rule allows for ePHI to be sent over an electronic open network as long as it is adequately protected. Encryption is the “addressable” implementation specification most relevant to patients’ use of mobile devices to communicate with their healthcare providers.

Mobile devices can transmit data in various ways, such as Internet protocols (used by many of the software applications developed by Project HealthDesign grantee teams), e-mail (which uses traditional Internet protocols), voice (traditional telephone) and SMS/text messaging. Text messaging holds significant promise for bidirectional communication between healthcare providers and patients. However, the sensitivity of patients’ health information and the risk that such information may be inappropriately accessed either while at rest or in transit suggest that encryption should be employed—or at least evaluated—to protect patient-generated health information.

**Figure 2** provides background information related to the encryption of text messages.

The experiences of the grantee teams suggest the following strategies. First, providers that give patients mobile devices should investigate whether they can preset any built-in encryption tools for data at rest. Providers and patients should also investigate the availability, effectiveness, and price of third-party tools that encrypt data being transmitted through text mes-
saging. If implementation of encryption is not feasible, providers giving patients mobile devices should engage in alternative protections, such as limiting the nature and extent of ePHI transmitted via unencrypted channels (e.g., careful wording of messages to and from patients), and direct patients to obtain detailed information through a web portal or other secure means. Further, providers that have supplied patients with mobile devices should offer education and training to patients on the risks of transmitting EPHI through text messages.

**ACCESS CONTROLS AND PERSON/ENTITY AUTHENTICATION**

Healthcare providers must implement technical safeguards to limit access to EPHI only to those authorized. There are a variety of access control methods and technical controls that are available within most smartphones and other mobile devices. The access control implementation specifications most relevant to patients’ use of mobile devices to communicate with their healthcare providers are (i) use of unique user identification (required); (ii) use of automatic logoff (addressable) and (iii) encryption/decryption (addressable and discussed previously). With respect to authentication, healthcare providers must implement procedures to verify that a person or entity seeking access to EPHI is the one claimed.

As the Project HealthDesign grantees learned, convenience and usability are key factors influencing a patient’s willingness to use a mobile device to collect and share patient-generated health information. Patients generally view security measures like passwords and automatic log-off features as obstacles, and they may be resistant to complying with these security measures or their compliance may interfere with the effective flow of patient-generated health information to providers.

With this in mind, healthcare providers providing patients with mobile devices should probably not require patients to password protect their mobile devices. Instead, providers should educate their patients about the risks of unauthorized access to mobile devices, make recommendations about proper access control measures and try to help patients make thoughtful and informed choices. Healthcare providers who have the resources to do so should offer education and training on use of passwords and proper device handling. (Those without such resources should consider providing fact sheets or informally educating their patients during visits.) Healthcare providers may want to ask patients to sign a statement indicating they understand the heightened risks if they do not protect their mobile devices with passwords, enable their device’s automatic logoff function and refrain from sharing their device

### FIGURE 3: Spotlight on Project Health Design Grantees

<table>
<thead>
<tr>
<th>Project Name</th>
<th>Description</th>
</tr>
</thead>
</table>
| iN Touch     | - Project HealthDesign’s iN Touch grantee team is examining the potential of collecting ODLs from youth suffering from obesity and depression. Under the project, participating youth enter ODLs into their iPod Touch, which sends the ODLs to TheCarrot.com via a wireless Internet connection. The Carrot.com generates weekly summary reports based on the ODLs and sends them to the participants’ healthcare providers’ EHRs. The reports are encrypted via SSL when they are transmitted to healthcare providers’ EHRs. To prevent inadvertent or unauthorized access to patient health information, the iN Touch team pre-set the participants’ iPod Touches to automatically lock after five minutes of inactivity. They also installed the Find My iPhone and MobileMe applications on the iPods to help locate and remotely erase data from devices reported lost or stolen, and asked the individual project participants to do their part to safeguard their iPods and their personal information. 
- The iN Touch grantee team also notes that patient’s ability to refrain from sharing his or her phone with family members may depend on socio-economic status. Patients with low-incomes may have only one phone that is used by all family members. Thus, the grantee team did not feel they could stress, as an absolute, not sharing the phone with family members but instead advised participants on the risks of sharing. |
| dwellSense   | - Project HealthDesign’s dwellSense grantee team is developing and evaluating technology to monitor the routines of older individuals who have arthritis and are at risk for cognitive decline. The grantee team has placed wireless sensors that capture routine daily activities (e.g., using a telephone, making coffee, taking medications) throughout patients’ homes. The sensors send data to a nearby laptop computer, which enables the process to occur automatically and unobtrusively. The sensor data is then transmitted from the laptop into a PHR, where custom applications turn it into individualized visualizations for both the patients and their clinicians. 
- Because the sensors are small and unobtrusive, they have limited computing and battery power. As a result, the grantee team undertook a risk analysis and decided not to encrypt the data as it moves from the sensor to the laptop (the data is encrypted as soon as it enters the laptop and remains encrypted thereafter). To do so would have required more computing power and a stronger, larger and more obtrusive battery, which would have to be changed daily. The grantee team took these operational issues into consideration when performing its security measure risk analysis. For example, it looked into a more secure radio signal to combat security risks to the unencrypted data, but this also would have required greater battery power. After a thorough analysis, the grantee team determined that sending unencrypted data from the sensor to the nearby laptop presented a reasonable risk that was worth taking in order to facilitate the project. |
with friends and family. Figure 3 spotlights some transmission security and access control activities undertaken by two Project HealthDesign grantee teams.

CONCLUSION

While the collection and transmission of patient-generated health information using mobile devices is occurring today primarily under tightly controlled research circumstances, all signs indicate that patients’ use of such devices to manage their health will increase. And as reimbursement models for healthcare providers incorporate cost containment incentives, there will be greater interest by healthcare providers in leveraging smartphones and other technologies to prevent costly complications. Project HealthDesign has demonstrated that it is possible to implement workable, technology-forward security protections for information in and shared through smartphones or other mobile devices, and they are critical to facilitate the widespread use of these tools by patients and healthcare providers. JHIM

Deven McGraw, JD, MPH, LLM, is the Director of the Health Privacy Project at the Center for Democracy & Technology (CDT), where she develops and promotes policies that ensure individual privacy as health information is shared electronically.

Robert Belfort, JD, is Partner at the law firm Manatt, Phelps & Phillips, LLP. He advises hospitals, community health centers, medical groups, managed care plans and other healthcare stakeholders on regulatory and transactional matters. He assists clients with managing health information in compliance with HIPAA and state confidentiality laws and advises on Stark law, anti-kickback and other fraud and abuse matters.

Helen Pfister, JD, is Partner at the law firm Manatt, Phelps & Phillips, LLP. She specializes in advising healthcare providers and nonprofit organizations on legislative, regulatory and transactional matters, and is involved in a range of projects involving use of health IT to facilitate the secure and timely exchange of information to improve the quality and efficiency of healthcare delivery.

Susan Ingargiola, MA, is Director at Manatt Health Solutions. She provides strategic business, regulatory and reimbursement advice to healthcare providers, nonprofit organizations and pharmaceutical/biotechnology companies. She specializes in health information privacy and confidentiality laws and health information technology.

REFERENCES

4. 45 c.F.R. Part 160 and Subparts A and c of Part 164.
9. 45 c.F.R. § 164.306(d).
11. 45 § 164.312(e)(1).
13. 45 C.F.R. § 164.312(e)(2)(i).
14. 45 C.F.R. § 164.312(a)(1).
15. 45 C.F.R. § 164.312(a)(2)(i).
16. 45 C.F.R. § 164.312(a)(2)(ii).
17. 45 C.F.R. § 164.312(a)(2)(iv).
18. 45 C.F.R. § 164.312(d).
The healthcare world is being upended by legislation and lawsuits. In the midst of the upheaval, a quiet revolution is taking place that will change the way hospitals, doctors and patients interact. The battleground—your cell phone. Welcome to the mobile health (mHealth) world.

On June 7, 2011, the World Health Organization (WHO) released the latest installment of the Global Observatory for eHealth series entitled mHealth: New horizons for health through mobile technologies. WHO chronicles the adaptation of medical and public-health practice supported by mobile devices, such as mobile phones, patient monitoring devices and other wireless devices. One of the most frequently reported types of mHealth initiatives was mobile telemedicine. Specific concerns arising from the report included data security and privacy, which are naturally the areas of the greatest risk for mHealth adopters.

On June 7, 2011, the World Health Organization (WHO) released the latest installment of the Global Observatory for eHealth series entitled mHealth: New horizons for health through mobile technologies.

WHO chronicles the adaptation of medical and public-health practice supported by mobile devices, such as mobile phones, patient monitoring devices and other wireless devices. One of the most frequently reported types of mHealth initiatives was mobile telemedicine. Specific concerns arising from the report included data security and privacy, which are naturally the areas of the greatest risk for mHealth adopters.

On June 7, 2011, the World Health Organization (WHO) released the latest installment of the Global Observatory for eHealth series entitled mHealth: New horizons for health through mobile technologies.

WHO chronicles the adaptation of medical and public-health practice supported by mobile devices, such as mobile phones, patient monitoring devices and other wireless devices. One of the most frequently reported types of mHealth initiatives was mobile telemedicine. Specific concerns arising from the report included data security and privacy, which are naturally the areas of the greatest risk for mHealth adopters.

On June 7, 2011, the World Health Organization (WHO) released the latest installment of the Global Observatory for eHealth series entitled mHealth: New horizons for health through mobile technologies.

WHO chronicles the adaptation of medical and public-health practice supported by mobile devices, such as mobile phones, patient monitoring devices and other wireless devices. One of the most frequently reported types of mHealth initiatives was mobile telemedicine. Specific concerns arising from the report included data security and privacy, which are naturally the areas of the greatest risk for mHealth adopters.

On June 7, 2011, the World Health Organization (WHO) released the latest installment of the Global Observatory for eHealth series entitled mHealth: New horizons for health through mobile technologies.

WHO chronicles the adaptation of medical and public-health practice supported by mobile devices, such as mobile phones, patient monitoring devices and other wireless devices. One of the most frequently reported types of mHealth initiatives was mobile telemedicine. Specific concerns arising from the report included data security and privacy, which are naturally the areas of the greatest risk for mHealth adopters.

On June 7, 2011, the World Health Organization (WHO) released the latest installment of the Global Observatory for eHealth series entitled mHealth: New horizons for health through mobile technologies.

WHO chronicles the adaptation of medical and public-health practice supported by mobile devices, such as mobile phones, patient monitoring devices and other wireless devices. One of the most frequently reported types of mHealth initiatives was mobile telemedicine. Specific concerns arising from the report included data security and privacy, which are naturally the areas of the greatest risk for mHealth adopters.

On June 7, 2011, the World Health Organization (WHO) released the latest installment of the Global Observatory for eHealth series entitled mHealth: New horizons for health through mobile technologies.

WHO chronicles the adaptation of medical and public-health practice supported by mobile devices, such as mobile phones, patient monitoring devices and other wireless devices. One of the most frequently reported types of mHealth initiatives was mobile telemedicine. Specific concerns arising from the report included data security and privacy, which are naturally the areas of the greatest risk for mHealth adopters.

On June 7, 2011, the World Health Organization (WHO) released the latest installment of the Global Observatory for eHealth series entitled mHealth: New horizons for health through mobile technologies.

WHO chronicles the adaptation of medical and public-health practice supported by mobile devices, such as mobile phones, patient monitoring devices and other wireless devices. One of the most frequently reported types of mHealth initiatives was mobile telemedicine. Specific concerns arising from the report included data security and privacy, which are naturally the areas of the greatest risk for mHealth adopters.

On June 7, 2011, the World Health Organization (WHO) released the latest installment of the Global Observatory for eHealth series entitled mHealth: New horizons for health through mobile technologies.

WHO chronicles the adaptation of medical and public-health practice supported by mobile devices, such as mobile phones, patient monitoring devices and other wireless devices. One of the most frequently reported types of mHealth initiatives was mobile telemedicine. Specific concerns arising from the report included data security and privacy, which are naturally the areas of the greatest risk for mHealth adopters.

On June 7, 2011, the World Health Organization (WHO) released the latest installment of the Global Observatory for eHealth series entitled mHealth: New horizons for health through mobile technologies.

WHO chronicles the adaptation of medical and public-health practice supported by mobile devices, such as mobile phones, patient monitoring devices and other wireless devices. One of the most frequently reported types of mHealth initiatives was mobile telemedicine. Specific concerns arising from the report included data security and privacy, which are naturally the areas of the greatest risk for mHealth adopters.
allow patients to communicate and receive information from their providers to applications that enable providers to monitor patients in real-time.

Additionally, these devices and applications are providing secure communication channels for discussing treatment by the provider with other medical professionals. Of course, there is also the role that smartphones enabled with mHealth applications will play in the retrieval of electronic medical records (EMR). As you will see from the following examples, there is always an “app” for that.

**PATIENT-PROVIDER COMMUNICATIONS**

There is a growing trend in hospitals and practitioner offices to have customized applications to provide patients with services such as scheduling and emergency room wait times. Sometimes the application itself provides and directs the communication automatically. For example, researchers at UNC Chapel Hill, The Justin Smith of Psychological Assessment Resources Inc. and the Children's National Medical Center developed an application that walks a user through a series of questions regarding the likelihood that someone has suffered a concussion. The application can then e-mail that information to a doctor to speed the treatment of the injury.5

**PROVIDER-PATIENT MONITORING AND DATA COLLECTION**

There are some interesting examples of patient monitoring and data collection devices and software that have already received FDA clearance. AirStrip offers smartphone applications that deliver patient monitoring data to the provider's phone.6 The vendor's applications include labor and delivery monitoring, ECG monitoring and overall patient monitoring and providing patient information including lab results, vital signs and medications.

Another example is Mobisante, which recently received FDA clearance for a smartphone-based ultrasound imaging system. The device is a handheld ultrasound probe and interface to allow the user to see and save real-time ultrasound images on his or her phone.6

**PROVIDER-MEDICAL PROFESSIONAL COMMUNICATIONS**

Mobile communication between professionals will happen—with or without a specific application—by virtue of the high concentration of smartphone use by professionals. QuantiaMD is an online physician-to-physician network where physicians interact to ask questions and learn about clinical issues. The network even provides forms and questionnaires to use in assessing patients, all available from a user’s phone.9 Another example is CARE TeleSolutions, a web based service provider for the transmission of high resolution patient images used in clinical diagnosis and reporting from the imaging equipment to the Internet.10

CellScope takes the imaging concept a step further by providing physical equipment that changes a smartphone’s camera into a diagnostic-quality microscope to allow the capture and transmission of images for diagnosis.11

For all of these devices and applications, the key is interconnectivity. But, with the reward of interconnectivity comes risk. Some of these devices and applications are regulated by the FDA, some will soon be regulated and all implicate HIPAA.

**REGULATION BY THE FDA**

The FDA regulates medical devices through one of two processes: premarket notification, also known as the 510(k) process, for Class I and II devices; and premarket approval, also known as the PMA process, for Class III devices. The 510(k) approval process is allowed for devices that are “substantially equivalent” to a pre-existing device already approved and in use. If the device is “new,” or otherwise unlike any currently existing device, the manufacturer must go through the PMA process to demonstrate reasonable “safety and effectiveness,” a much more onerous task.

An even faster process is available if the device is deemed to be a Class I device and not subject to the 510(k) process or the PMA process. These devices include Medical Device Data Systems (MDDS), devices that are “intended to transfer, store, convert from one format to another according to preset specifications, or display medical device data” and that “are not intended to be used with active patient monitoring.”12

Although not specifically addressed in the Draft Guidance, it is easy to imagine mHealth applications that turn smartphones into quasi-medical devices that fall into this definition of Class I devices and are therefore subject only to general controls under the FDA.

Before the Draft Guidance, the FDA regulated mHealth applications as devices when the application turned the smartphone into a medical device. The Draft Guidance now defines a “mobile medical app” as (i) a device intended for use in the diagnoses, cure, treatment or prevention of disease that (ii) is used as an accessory to a regulated medical device or transforms a mobile platform into a regulated medical device.13

The Draft Guidance appears to clarify that it is only those mHealth applications that rise to the level of changing a smartphone into a “medical device” that will be regulated. As stated in the Draft Guidance, “This narrowly-tailored approach focuses on a subset of mobile apps that either have traditionally been considered medical devices or affect the performance or functionality of a currently regulated medical device.”14

However, the FDA has left open the option to “exercise enforcement discretion” toward mHealth applications that are not “mobile medical app[s]” as defined above, but are nevertheless “medical devices.”

**LEGAL RISKS ASSOCIATED WITH MOBILE DEVICES**

Using and manufacturing mobile devices and applications. Generally, manufacturers of medical devices are provided some protection from tort lawsuits under the “learned intermediary” doctrine, where the manufacturer only has the duty to warn the physician (i.e., the learned intermediary) and not the consumer of risks associated with the device,15 and the “sophisticated user” test, where a manufacturer has no duty to warn a user of product dangers if the user “possesses special knowledge, sophistication or
FOCUS: A BRAVE NEW WORLD

expertise in relation to the product.”16

However, these protections are being steadily eroded by state courts. Protection for manufacturers from common-law tort claims has come from an unlikely source: the United States Supreme Court.

In 1996, the Court ruled that a lawsuit against the manufacturer of a medical device that had gone through the 510(k) process was not federally pre-empted because the device had not been found by the FDA to be safe and effective, just substantially equivalent.17 As discussed above, this is the difference between a Class I or Class II premarket notification process and the more stringent Class III premarket approval process.

In 2008, the Court visited a related issue and ruled that a lawsuit against the manufacturer of a medical device was federally preempted because the lawsuit questioned the safety or effectiveness of the device which had received Class III premarket approval from the FDA.18 Therefore, it appears that obtaining Class III premarket approval provides a layer of protection against tort liability for medical device manufacturers.

These protections for manufacturers increase the risk that liability may fall to healthcare providers when devices and applications used for clinical diagnostics are sent home with patients. There is the possibility that the patient will not enter information accurately or completely, and the doctor will make an incorrect diagnostic decision based on that information. Instances such as this could give rise to lawsuits pulling in all the deep pockets: manufacturer, hospital and doctor. The current net of medical malpractice and product liability laws will most likely be implicated and cushion the blow to the manufacturer, hospital and doctor. However, it would only take one instance of unconsolable injury with nominal relief to draw the ire of legislators and policy makers, with uncertain and potentially damaging results.

Additionally, hospitals may very easily find themselves in the undesirable position of being subject to the same liabilities and regulations as device manufacturers. The FDA has indicated that a health care facility that (i) buys software or hardware that is then added to or modified such that it is able to transfer, store, convert or display medical device data and (2) uses the modified device or software (or application) in clinical practice will be considered a “device manufacturer” under section 807.3(d) of Title 21. Such designation brings with it the responsibilities under Part 803 to establish and maintain adverse event files and submit annual reports to the FDA. Even if such devices were to fall under the MDDS definition above, manufacturers of such devices must implement the required general controls of Class I devices for quality systems which govern the methods, facilities and controls for the design, manufacture, packaging and servicing of the devices to ensure that they are safe and effective.19

Classification as a medical device manufacturer surely in most cases will be an unintended consequence of the hospital’s desire to innovate and provide better and more coordinated patient care. For all mHealth devices, there is also the risk of off-label use. Off-label use occurs when a medical device is used in a manner not approved by the FDA. Unfortunately, off-label use can occur innocently, such as when a doctor uses a device or application in a way that benefits the patient and the doctor, but is nonetheless “unapproved.”

In other cases, manufacturers may knowingly promote a device for a certain procedure or function, when it was another device that was actually approved to perform that procedure or function. Both of these instances can lead to litigation.20 It is therefore important to educate the device users as to the official, approved uses of the devices, and to investigate the FDA clearance status and description of any new devices touted by manufacturers.

MHEALTH PRIVACY & SECURITY CONCERNS

The very benefits of mHealth, including mobile access and the ability to share data and images with a few keystrokes, raise serious privacy and security concerns. HIPAA requires covered entities, such as hospitals and physicians, to comply with security and privacy regulations designed to protect patients’ protected health information (PHI). PHI is defined as “individually identifiable health information” that is transmitted or maintained in electronic media or in any other form.21

The HIPAA security standards establish the measures a covered entity must take to ensure the confidentiality, integrity and availability of all electronic PHI created, received, maintained or transmitted by the covered entity.22 A covered entity is also required to implement protections against anticipated security threats; protect against any reasonably anticipated impermissible uses or disclosures of ePHI; and ensure that its workforce members comply with the security standards.

The HIPAA security standards, which are divided into administrative, physical and technical safeguards, organizational requirements and policy/procedure/documentation requirements, run the gamut from basic requirements such as the use of password protection and access controls, to more detailed monitoring and security breach response requirements. mHealth users must familiarize themselves with these requirements and ensure that appropriate measures and policies are implemented. For example, before workforce members are allowed to use mobile medical devices, the hospital or other healthcare provider must ensure that it has policies and procedures in place that govern the use of mobile devices.

The HIPAA privacy requirements also significantly impact the use of mHealth devices and applications. Pursuant to these requirements, only authorized individuals may access, use or disclose PHI, and such access, use or disclosure must be for only specifically enumerated purposes. Any impermissible access, use or disclosure constitutes a HIPAA violation that may subject the institution to significant fines. Additionally, under the breach regulations implemented under the HITECH Act, a breach of unsecured PHI occurs whenever PHI that is not encrypted or otherwise secured is impermissibly acquired, accessed, used, or disclosed, resulting in a significant risk of financial, reputational or other harm to the patient whose PHI was
the subject of the breach. In the event of a breach, the provider must notify the patient(s), HHS, and, in situations involving the PHI of more than 500 individuals, the news media, regarding the details of the breach and take measures to protect against further incidents. The provider may also be subject to significant fines as result of the breach.

The potential for HIPAA violations associated with the use of mHealth applications and devices is staggering. Smartphones can be easily misplaced or stolen. Additionally, many users do not understand the extent to which data is stored in the device's memory, and may assume that deleting an app or e-mail is sufficient to eliminate the PHI. Such users may then discard, recycle, or gift the device to another person—along with all PHI stored on the device. Some providers also chafe at password and encryption requirements that are perceived to slow the needed flow of information.

Healthcare providers must be sensitive to these issues and craft and enforce appropriate policies regarding the use of mobile devices to access or use PHI, including how to ensure PHI is protected in the event that a healthcare team member resigns or is terminated. These issues are especially fraught with peril in situations in which the team member is using his or her personal mobile device to access or use PHI. The use of personal mobile devices itself is problematic; the mHealth world is one of the only environments currently in health care where providers know that unauthorized devices are used to enter information into patients’ medical records, a situation we never thought we would find ourselves in after the issuance of the HIPAA security rules.

Another area of risk is hacking. While smartphones’ vulnerability to hacking and viruses should be well-recognized, smartphones’ vulnerability to hacking of the HIPAA security rules. The real battle will be in situations we have not yet addressed, such as when a patient’s death occurs from malicious hacking or a virus wipes or alters diagnostic information that is used by practitioners to make treatment decisions. Information technology professionals will play a key role in interpreting highly technical encryption standards adopted by HIPAA, as well as monitoring and developing strategies to combat electronic security threats.

CONCLUSION
mHealth issues will continue to multiply as our mobile devices become an even more integral part of our life. The wise healthcare provider cannot embrace this brave new world without a healthy dose of caution and ample preparation. Such preparation requires input from clinicians, information technology professionals, compliance personnel, attorneys, administrators, and health information management professionals. Each of these groups brings an important perspective to bear and must work together to craft and implement reasonable policies that balance the need for privacy and security with the benefits mHealth devices and applications bring to providers and patients.

REFERENCES
13. Draft Guidance, 43689 (“a medical device” is defined as “an instrument, apparatus, implement, machine, contrivance, implant, in vitro reagent …” that is “… intended for use in the diagnosis of disease or other conditions, or in the cure, mitigation, treatment, or prevention of disease,….”).
21. 45 C.F.R. § 160.103.
22. 45 C.F.R. § 164.302, et seq.
23. 45 C.F.R. § 164.400, et seq.

Allyson Jones Labban is a partner in the Greensboro office of Smith Moore Leatherwood, LLP. A graduate of the Duke University School of Law, Labban’s practice focuses on HIPAA and medical privacy issues as well as Medicare/Medicaid billing and regulatory compliance and certificate of need.

Clara R. Cottrell is an associate in the Greensboro office of Smith Moore Leatherwood, LLP. A graduate of Wake Forest School of Law, Cottrell’s practice focuses on business and Intellectual Property issues. Cottrell is an active member of the ABA’s Section of Science and Technology Law.
OVER THE PAST DECADE MOBILE PHONES HAVE REVOLUTIONIZED THE WAY WE COMMUNICATE. THEY HAVE MADE THE WORLD A SMALLER PLACE WHERE PEOPLE CAN INTERACT WITH EACH OTHER, IRRESPECTIVE OF WHICH PART OF THE WORLD THEY ARE IN. MOBILE PHONES ARE GENERALLY AFFORDABLE AND AVAILABLE TO MOST OF THE POPULATION, MAKING THEM MORE ACCESSIBLE THAN COMPUTERS AND FAR MORE COST-EFFECTIVE THAN HOSPITAL BEDS. THEREFORE, MOBILE TECHNOLOGY HAS THE POTENTIAL TO REVOLUTIONIZE HEALTHCARE IN DEVELOPING COUNTRIES, PARTICULARLY IN THE AREA OF HEALTH AWARENESS SCHEMES AND TRAINING OF HEALTHCARE PROFESSIONALS.

THIS PAPER REPORTS THE RESULTS OF A HEALTH IT INITIATIVE AIMED AT USING MOBILE PHONE TECHNOLOGY TO SPREAD MEDICAL CARE AMONG PEOPLE IN SLUM AREAS. A SURVEY WAS DONE IN AN URBAN SLUM SETTING TO TEST THE FEASIBILITY OF DEPLOYING MOBILE TECHNOLOGY FOR PROVIDING PRIMARY HEALTHCARE SERVICES. THE DESIGN OF THE STUDY WAS BASED ON A “REGIONALISED SERVICE DELIVERY MODEL.” THE VISITS TO THE SLUM REVEALED THAT PEOPLE OF THE COMMUNITY ACCEPTED THE USE OF TECHNOLOGY FOR ACCESSING HEALTHCARE. ALTHOUGH THE SLUM DID NOT HAVE A REGULAR ELECTRICITY SUPPLY, PEOPLE WERE ATTUNED TO USE THE MOBILE PHONES ON A DAILY BASIS AND WALKED TO THE NEAREST MARKET AREAS TO CHARGE THEIR HANDSET BATTERIES. THIS HELPED US TO APPROACH THEM WITH OUR CONCEPT OF INTRODUCING TECHNOLOGY, ANALYZE THE MINDSET OF THE PEOPLE OF THE SLUM, UNDERSTAND THE FEASIBILITY OF TECHNOLOGY INTERVENTION FOR HEALTHCARE AND TO COLLECT DATABASE OF COMMON MEDICAL SYMPTOMS TO FORM THE DATABASE OF THE MOBILE PHONE APPLICATION.

KEYWORDS
Health IT, mobile phones, healthcare, mobile phone technology, deploying mobile technology, technology for healthcare, use of mobile phones, e-health, technology intervention, mobile phone application.
MOBILE PHONES have been one of the most striking technological developments in recent decades. This technology has grown not only in performance, but also in the development of networks, and has received a huge acceptance by all sections of the population, both in developed and developing countries. As a result, mobile telephony and its services like SMS has become an important new means of communication, even among low-income groups.

According to an overview by the United Nations Foundation, Vodafone Group Foundation and Telemedicine Society of India (August 2008), there are more than 3.5 billion mobile phones in use across the globe and this figure is set to double in the next decade. Telephony was introduced in India in 1882. India has become one of the fastest-growing telecom networks in the world, and in June 2011, the total number of telephone subscribers in the country was 885.99 million, with 851.70 million of these being mobile phone subscribers.1 The role of telemedicine in clinical care, education, research and training in health sector continues to grow all over the world.

In urban areas, hospital beds are inadequate and available outpatient facilities are stretched by crowds of patients from the neighborhood areas who are in need of medical consultation for minor ailments which could be managed at the community level. This wastes valuable resources which could be utilized for attending to cases which deserve hospital care. Different types of service delivery models have been suggested for providing effective services in the urban areas. We planned to use one of these alternative models, the “Mobile Based Regionalized Service Delivery.” This model consists of a link worker in the community for a group of delineated households, who is trained to attend a sick family member of his group and manage the morbidity with the active help and support of a medical doctor available on a mobile phone. Each hospital will maintain a list of such link workers and will actively support the patients referred by them. This will include verbal advice during initial consultation and further physical support in case of further referral to the hospital and support for monitoring follow up referrals with the link worker.

It is generally believed that the use of mobile phone by link workers for accessing healthcare will improve the quality of the service in poorly served areas and decrease the unnecessary patient visits to the hospitals for minor ailments. This survey assessed the acceptability of technology intervention by the people. Since any software designed for such an intervention should be customized to the commonly occurring ailments in a given community, this survey aimed at collecting information about the common ailments faced in the community being studied.

The survey helped to assess the socioeconomic status of the slum and to observe their acceptance for the intervention of mobile phones for primary healthcare. A slum settlement “Brar Square” was selected for the survey because of previous interactions in the community by one of the co-authors (SG). Six persons from the community volunteered to work with us as “Link Workers” (two males, two females and two as backup) to help in data collection. The slum was thus divided into four sections, one under each link worker. The data was collected by each link worker for the houses/families under him/her and recorded in the data sheets which were designed for the purpose. Detailed information of the population under study and the symptoms commonly faced by them was collected through this questionnaire. (Table 1.)

Additionally, the people were also questioned about their responses to the type of technology service which was to be introduced.

The survey was conducted over approximately six weeks during the summer months. Regular visits (once in 10 days) were made to the area by the doctor in order to maintain contact with the people and to provide primary medical consultation till the time the technology was ready to be deployed.

AHERF tied up with a technology company for development of the mobile phone application. This was a bilingual application which once installed on the mobile phone would work as an SMS facility. The steps for the application to work are as follows:

With the help of the link workers identified from within the community, each resident of the slum would be registered on the software through the mobile phone and would be given a unique ID. This would include registering the mobile number of each person, family details, number of BPL families, etc. So every time a patient needs consultation, only the ID will be entered and patient details would be retrieved. (The link workers would be trained well to use
Over the past decade mobile phones have revolutionized the way we communicate. They have made the world a smaller place where people can interact with each other, irrespective of which part of the world they are in.

For medical consultation a person would seek help of the link worker, who would feed in the UID of the already registered patient and all the patient details would be retrieved. The patient would then describe the symptoms to the link worker who would then use the drop down menus available on the software to fill in the symptoms (up to 10 symptoms at one time can be entered). Then information fed in is sent as a message to the doctor.

The doctor receives the request on his mobile phone and he can then log into his system and responds to the query from the patient after understanding the symptoms. The doctor writes a prescription which is a primary care SOS for the patient, along with the disclaimer that, “This is only a Primary Care SOS and if the problem persists and there is no relief then the patient to visit a nearby nursing home/hospital.” The doctor then clicks “send.” The link worker receives the doctor’s reply as an SMS and conveys it to the patient.

This way the patient is able to get primary healthcare support from certified doctors, without investing time and money in commuting to the hospitals.

Technology. The application is based on J2ME (Java to Micro Edition) format, established for consumer wireless device platform. J2ME is a Java Platform designed for embedded systems (mobile devices). Java ME files implement a profile. Most common of these are mobile information device profiles aimed at mobile devices such as cell phones. There are currently more than 2.1 billion JAVA ME-enabled mobile phones and PDAs.

This technology can be useful in the healthcare system to provide technology to doctors and patients to stay connected without being face to face all the time.

OBSERVATIONS

Basic information about the slum and the people living there was collected at the initial visit. The population of approximately 1,600 people living in 650 houses consists of settlers from the states of Rajasthan, U.P., Bihar and Haryana. From our analyses (Table 2) 400 individuals have an income below poverty line (BPL—defined as per the government of India, poverty line for rural areas is Rs. 276 per month, i.e. people in India who earn less than Rs. 10 per day).
Their source of income and the type of work they do also varied with those from Rajasthan mainly working as daily wage laborers, people from U.P and Bihar mostly doing domestic tasks in nearby houses on monthly payment and those from Haryana mostly working as semi-skilled government employees like peons, drivers, etc.

The literacy level of the community was such that most individuals could read and write in Hindi and a small proportion could read and write their names in English as well. All the children attended local government school till class 10, and went to a government school for higher secondary studies. The healthcare facilities available are “not very satisfactory,” according to the perception of the people of the slum. In case of any medical problem in a family, the male members approached the doctors/quacks for help and the women did not come out on their own to seek medical help. This resulted in a major shortcoming in explaining the symptoms since the women were taking care of the children and can lead to misdiagnosis hence incorrect medication.

‘Mobile Creche’ medical van visits the slum once a week to distribute free medicines based on the prescription shown by the patient and without any verification of the diagnosis. For instance, an antipyretic maybe given in case someone complains of fever, without any determination of the cause of fever. But the van does not stay for more than 10-15 minutes in order to enable everyone to access this service. There are two private clinics in the slum. But, the residents informed that there is no qualified doctor present in the slum. However, these clinics are providing services for their everyday health problems. The charges here are Rs.30 or above for each medicine that is provided.

Under the government’s Rashtriya Swasthya Yojna, insurance cards have been provided to the below poverty line families. This scheme gives coverage of up to Rs.30000 in case of emergency; but the patient has to get admitted at least for two hours, in the hospital to claim money under this scheme and does not provide support for outpatient medical services.

Although many people have mobileity, they have to seek help from the nearby homes to charge their phones or sometimes charge them in nearby market places on payment.

During discussions with the people, it also became evident that they lacked basic awareness of primary health related issues. For example, both males and females were equally unaware of problems, like malnutrition in children, health of women and problems of the elderly. It was explained to them that through the technology intervention they could message and seek doctor’s consultation in order to increase their knowledge and to have better health.

**RESULTS**

The social outcome of the study was that a good rapport was established with the community. There was an acceptance of the technology and people showed confidence in the team by discussing their everyday medical and even emotional issues. A feeling of confidence was established amongst the people with the doctor visiting the slum. The consultant initiated timely advice for appropriate referral for medical problems which could not be managed on an outpatient basis at the site. And, an initial stock of basic medicines used to treat the most frequent symptoms, were made available to the population on a goodwill basis.

The importance of the local population being able to readily access medical help through the mobile phone technology (with the help of volunteers from the local population serving as link workers) was repeatedly reinforced by the doctor at the site.

From the data collected during the survey, the following important conclusions can be drawn:

**Acceptability.** In the community the link workers helped to collect data from 320 families, a total of approximately 1,600 people. This data essentially consisted information about the total number of people in the family, total number of children, financial status, whether or not they are BPL families and have the “RashtriyaSwasthyaYojna”, their mobile number (atleast one number per family). The average number of children per family was three, the average family size five and 80 families of the 320 (25 percent) had BPL cards. All this information was readily provided by the people, which show their interest to use this service, and their eagerness to register their mobile number when the service is launched in the slum. Thus, based on the number of families approached, there was 100 percent acceptability to use the mobile phone as a tool for accessing healthcare.

**Willingness.** The people from the community volunteered to work as “link workers”, and help in data collection for common medical symptoms, which would be fed into the application. Data for about 320 families and 15 common symptoms was collected by link workers as per our guidance. Their willingness to work towards supporting the use of technology intervention was tremendous.

The common symptoms reported by the individuals of all ages were similar to an average community. Common medical problems encountered were upper respiratory infection with or without fever, acute gastroenteritis, skin disorders and gynecological problems (excessive menstrual bleeding, irregular menstrual cycle, lower

**TABLE 3: Details of the Families of the Slum**

<table>
<thead>
<tr>
<th>Family</th>
<th>Average no. of family members</th>
<th>Number of Children per family</th>
<th>BPL (Y/N)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total: 320</td>
<td>5.071875</td>
<td>2.765625</td>
<td>Y = 80, N = 240</td>
</tr>
<tr>
<td>Total number of Families BPL = 80</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Average members per family = 5 (5.07)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Average number of children per family = 3 (2.7)</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Mobile technology has the potential to revolutionize healthcare in developing countries, particularly in the area of health awareness schemes and training of healthcare professionals.

abdominal pain, and other symptoms) which adolescent girls, women in reproductive age group and post menopausal women experienced. (Figure 1)

**EXPECTATIONS OF THE COMMUNITY FROM THE TECHNOLOGY INTERVENTION**

By interacting with the people of the slum during the few months of the feasibility survey, it was clear that the people of the slum expected that with technology intervention for primary health care facilities would improve, as easy consultation would be made available. Their expense of travelling to bigger hospitals for every small ailment would reduce. Medical assistance would be available in much less time. Getting a facility which provided them access to expert consultants from a high end corporate hospital was a great incentive for the slum dwellers.

**Services provided during the survey.**

During the period of the feasibility survey, the team from AHERF provided the following services free of charge:

Weekly visits to the slum area were conducted, where a consultant from Apollo Hospitals provided consultation to the people of the slum in order to help them treat their regular medical concerns. During the consultations, the doctor found that the children were malnourished and parents were poorly informed about issues related to health and nutrition of their child. The doctor educated them about the importance of personal hygiene, sanitation of the environment and nutritional needs of the child.

A weighing scale was provided to the Pradhan, or local community leader and parents were made aware that they need to weigh their children at regular intervals, and take regular medical advice in order to keep their child healthy.

Five basic medicines (paracetamol tablets, zinc with multi vitamins, antispasmodic and norfloxacin with metronidazole) were distributed free of cost. The custody of these medicines was given to the Pradhaan, who was made aware of the medical situation where these could be used.

**ACKNOWLEDGEMENTS**

Great support has been extended by the team from Ozone Technologies in explaining and demonstrating the technology to the people in the slum and extending their help in distribution of medicines and organizing the consultations. Dr. Faruque Ahmad, consultant community medicine and Principal, Apollo Medical College, helped to prepare the project methodology after the feasibility study was done. Last but not the least I would like to thank the Pradhan and other people of the community who provided their support to carry out the feasibility survey.

---

**FIGURE 1: Representation of Common Medical Symptoms**

<table>
<thead>
<tr>
<th>Condition</th>
<th>Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stomach Ache</td>
<td>11%</td>
</tr>
<tr>
<td>Cough</td>
<td>9%</td>
</tr>
<tr>
<td>Asthma</td>
<td>5%</td>
</tr>
<tr>
<td>Malnutrition</td>
<td>11%</td>
</tr>
<tr>
<td>Pregnancy</td>
<td>23%</td>
</tr>
<tr>
<td>Fever</td>
<td>17%</td>
</tr>
<tr>
<td>Constipation</td>
<td>18%</td>
</tr>
<tr>
<td>Chest Pain</td>
<td>6%</td>
</tr>
</tbody>
</table>

Ranjit Roy Chaudhury has served as Professor and Head of the Department of Pharmacology, Dean and Director of the Postgraduate Institute of Medical Education and Research, Chandigarh. In 1978, he started the first DM course in Clinical Pharmacology in India. He developed the “Delhi Model” of
The importance of the local population being able to readily access medical help through mobile phone technology was repeatedly reinforced by the doctor at the site.
Security & Compliance

Insights and Strategies as You Plan for, Develop and Implement mHealth Solutions in Your Organization

By Jeff Brandt

ABSTRACT

Editor’s Note: This paper was originally published as Chapter 8: Security & Compliance in the book mHealth: From Smartphones to Smart Systems, published by HIMSS in 2012.

Security in mHealth encompasses many facets, concerns, misconceptions and fears. From users’ perceptions to data breaches, this chapter will introduce some of the issues that will help you develop insights and strategies as you plan for, develop and implement mHealth solutions. Designers and purchasers of mobile health solutions must take many issues into consideration when developing an organizational mobile health strategy. The sheer speed of adoption of mobile devices and software into our everyday lives has propelled the market to produce quicker, cheaper and more feature-rich devices faster than most organizations can digest. The speed with which these devices evolve also increases the rate of system deprecation. If not managed correctly, this technical liability can be very costly to a healthcare organization. With a well-developed strategy, however, the exposure can be mitigated. This chapter will provide an overview of the components of mHealth security and insight into solutions to secure your products, protected health information (PHI), and the organization as a whole. Please note that this is not a “how to” chapter, but a guide to assist with mHealth security strategy and understanding. This chapter focuses on connected mobile devices, text-enabled cell phones, embedded applications, patient-wearable and implantable devices, smartphones and store-and-forward systems. The reference to “devices” will include all systems that are mobile and collect, transmit and/or receive medical data.

KEYWORDS

Mobile health, mHealth, privacy, security, protected health information, strategy.

SECURITY IN mHealth encompasses many facets, concerns, misconceptions and fears. From users’ perceptions to data breaches, this chapter will introduce some of the issues that will help you develop insights and strategies as you plan for, develop and implement mHealth solutions.

Designers and purchasers of mobile health solutions must take many issues into consideration when developing an organizational mobile health strategy. The sheer speed of adoption of mobile devices and software into our everyday lives has propelled the market to produce quicker, cheaper and more feature-rich devices faster than most organizations can digest. The speed with which these devices evolve also increases the rate of system deprecation. If not managed correctly, this technical liability can be very costly to a healthcare organization. With a well-developed strategy, however, the exposure can be mitigated.

Although we are only at the beginning of what can and will be accomplished with mHealth, being cognizant of the opportunity is important. The caveat is that with all new technologies comes new risk. With a well-developed strategy, however, the exposure can be mitigated.

By definition, mobile provides unethical
users with vast opportunities to exploit. This chapter will provide an overview of the components of mHealth security and insight into solutions to secure your products, protected health information (PHI), and the organization as a whole. Please note that this is not a “how to” chapter, but a guide to assist with mHealth security strategy and understanding.

This chapter focuses on connected mobile devices, text-enabled cell phones, embedded applications, patient-wearable and implantable devices, smartphones and store-and-forward systems. The reference to “devices” will include all systems that are mobile and collect, transmit and/or receive medical data.

Shahid Shah, Enterprise Software Analyst and blogger of The Healthcare IT Guy, provides a list of IT practices that hospitals should utilize. Each one of these points are applicable to mobile.

Don’t marry a mobile platform. Operating systems, platforms, manufacturers and vendors will come and go. mHealth innovations are moving very quickly and the hot devices of today may be gone tomorrow. Don’t get locked in to a device because your users have a favorite. We all have a favorite.

Medical devices that don’t communicate with existing and future enterprise systems. Systems that are not connected or cannot connect easily to enterprise systems are worthless. If you can’t export data to all of your systems, it limits the overall system. If the devices do not utilize standard Internet protocol, they are already behind and will be depreciated.

Application development anchored in legacy systems. You must do your own research on this issue. Perform a deep dive into the architecture of vendor solutions. Beware of becoming locked in to a one-vendor solution. This type of solution can be easier going in, but you may be limiting future options.

HIPAA-centric IT security development. Do not focus on HIPAA for your security requirements. As with FDA requirements, use best engineering practices of planning, designing, developing and testing. If you design for security upfront you will be ready for HIPAA.

STRATEGY
The following is a quote that I often refer to while doing strategic planning, from Sun Tzu, “Strategy without tactics is the slowest route to victory. Tactics without strategy is the noise before defeat.”

Developing an overall strategy for mobile security is one of the most important steps in protecting organizational and patient data. It is also a practice that developers of mHealth should utilize. Strategy documentation can be essential in providing demonstrable example of your diligent in securing PHI.

As a first step, start with a risk assessment of your organization’s projects and needs. The assessment will provide the information necessary to establish security goals. Step two, develop strategies and tactics to ensure that the new system or design is HIPAA-compliant and that patient and provider information is safe and secure.

Steps of Execution:
1. Perform risk assessment.
2. Set security goals.
3. Develop strategies and tactics.
4. Execute.

SECURITY GOALS AND RISK ASSESSMENT
Healthcare security is unique. Unlike other industries’ data breaches, exposure of health data can be difficult or impossible to correct. As I once heard a colleague say, “You cannot undo cancer.” Meaning, that once an individual’s health records are exposed, there is no getting them back; you cannot issue a new card or ID to correct the exposure. Adding mobile devices to the equation increases the risk of PHI exposure, making risk assessment even more difficult. The following are items that should be considered in a strategy to secure PHI.

• What information are you trying to protect? The common answer to this is “protect everything.” Yes, you can utilize this strategy, but it may be costly and detrimental to performance, storage, analytics and budget.

• What security goals are you trying to achieve?

• What security goals are you trying to achieve?

• Who wants your data and why? I am sure you have heard the saying, “Keep your friends close, but your enemies closer.” If you can understand the return on investment of a criminal when it comes to what you are trying to protect, you can build a better strategy and provide better tactics of protection.

• Prioritize your tactics. Tactics normally have costs associated with them, so you must budget your effort.

• Is the device an FDA Classified Medication Device?

• Is the device and/or data a HIPAA Covered Entity?

PERCEPTION
Mobile security is a doctor’s top concern, and a barrier to adoption, stated a Price Waterhouse Coopers’ survey. In the early 1990s, I worked for the first online credit card processing company and we had a saying: “Security is perception.”

People don’t like to hear this, but nothing is truly safe. However, the perception of security is often more powerful than security itself. People need to feel safe, and this is a very important part of security. Most people in the United States feel that they are safe. The majority of people in the United States have no issues with giving a credit card to a waiter they do not know and allow them to carry it away without concern. Waiters are one of the highest perpetrators of credit card fraud. In most developed countries, waiters bring the capture device to your table, so your card never leaves your sight. A healthcare organization’s leadership is responsible for providing an environment of security and trust for their patient and providers.

Mobile has spawned a lot of fear in our society about personal security. This is similar to what credit card companies faced in the 1990s with web purchases. More recently, there have been a lot of publicized data breaches concerning patient records, and unfortunately, most of these breaches could have been prevented with organizational policies and procedures.

A majority of the breaches are what I call “sneaker theft,” where the medical records were carried right out the door on USB thumb drives, portable drives, smartphones or stolen laptops with unencrypted PHI. (See more on encryption in a section
mHealth innovations are moving very quickly and the hot devices of today may be gone tomorrow. Don’t get locked in to a device because your users have a favorite. We all have a favorite.

later in this chapter.) For example, more than 600 patient records stored on a laptop computer were taken from Onslow Memorial Hospital in Downey, CA.7 In another case, more than 360,000 health records, which were stored on a laptop, were stolen from an employee’s vehicle9.

Massive Data reported that EMR records are more vulnerable to physical theft than hacking. It’s not some kid in sitting in front of his computer in a Third World country who is stealing health records; it’s the lack of security policies that are allowing these breaches to occur.

Written policies are the first line of defense in securing systems. These simple policies can achieve not only the perception of security, but true security.

Here are a few best practices:

• Develop an extensive policy.
• Post policies in employee areas.
• Place policies in your employee handbook.
• Set the policies on USB devices (you may want to consider disabling).

You also should consider having all employees acknowledge via signature that they have read and understand the policies, which should then be kept in their files.

DATA STORAGE
There are multiple options for data storage on mobile devices. Each type of storage has different security features, concerns and threats. Most important to remember is that PHI is secure. There are an array of strategies that can be implemented to reduce the chance of a breach. The weakest link in the security chain is where a breach will most likely occur: This is where skilled software and network engineers come into play as part of your risk assessment.

Here is a list of PHI storage scenarios for mobile devices:

• Cloud.
• On-device storage, memory.
• Secure Micro SD Card (Secure μSD).
• Client-server, no on-board storage, behind firewall.
• Store-and-forward.
• Hybrid, both on-board and remote storage.

CLOUD STORAGE
There has been much discussion and confusion on the topic of “the cloud.”. Cloud storage has been around and providing safe storage for many years. The primary difference between cloud and client-server is that with the client-server model, the business that runs the application owns and controls the hardware (servers).

Cloud service is hosted by a third party. The major advantage is that additional server capacity can be added as needed. One of the true benefits of the cloud is that the cost of maintenance is reduced, nor does the organization need to hire a team of experts to administer the system. The other advantage is that with the cloud, the organization has a team of experts who focus primarily on the administration of the servers and infrastructure.

I almost always recommend the cloud over internal servers. Security in the cloud is normally better than that found in individual organizations and can be provided at a fraction of the cost. However, you must perform your due diligence to ensure that the selected vendor is HIPAA-compliant and provides security for your patients’ PHI. Note, most apps and mobile systems do not have to be HIPAA-compliant, so you must delve into the terms and conditions to verify PHI security.

ON-DEVICE STORAGE
Systems required to provide PHI when the Internet is not available utilizes on-device storage. PHI is physically stored on the device in a self-contained database or file. Examples of these systems are: offline, store-and-forward or when a permanent copy of the data remains on the device, such as in mobile PHRs.

To secure PHI on these systems, applications should be password protected and the data encrypted. There are many different encryption schemas available (e.g., open AES-256). Systems developed for export from the United States must comply with the US Department of Commerce and restrict the encryption to 56k.

Note: PHI encryption is an important area to focus on when performing your due diligence for product evaluation. Many smartphone apps have no encryption features. Password protection is different than data encryption.

CLIENT-SERVER, NO ON-BOARD STORAGE
True client-server applications, also known as thin-clients, reside on devices like laptops, and normally do not have or utilize on-board storage (i.e., a browser). The device is a client to the server; all requests for data or storing of data are facilitated via a server-side application and database. Normally, client-server applications and their clients are protected via a firewall. Since there is no access to storage on the device and the clients themselves are
behind a firewall, the security model is traditional intranet. Wireless devices are the exception—devices must be secured and managed. Breaches are still an issue, so precautions must be taken to avoid theft and wireless snooping.11

**STORE-AND-FORWARD**

This technology is often used when a device is temporarily off-line (not connected to the server), and is similar to on-board storage. When the device is connected to the Internet or local area network (LAN) the data on the device is uploaded and downloaded to and from servers.

A prime example of store-and-forward use is the medical home. Caregivers download patient data to the device before they leave the office and collect PHI data during the home visit. The collected data is then uploaded onto the firewall-protected server when the caregiver returns to the office. Downloaded and collected PHI is stored on the device, so data security must be implemented.

**HYBRID**

Hybrid devices are a combination of on-board and remote storage. Data is either synced between the device and the server DB or the system utilizes a master-slave replication algorithm where the device is the slave to the server DB (e.g., the server data is considered to be the correct data and all devices are secondary, so syncing is not necessary). The hybrid model does not guarantee protection from a breach; encryption and other tactics to secure PHI is needed.

**DATA TRANSMISSION**

Wireless devices that share data must incorporate a security strategy when transmitting data to and from the server. There are several different schemes that can be used to accomplish this.

Mobile devices that are not wireless can utilize store-and-forward technology to transfer data without having to broadcast data over a carrier’s wireless system. The mobile device is connected to a PC or docking station in order to transfer the data behind a secure firewall. Some devices utilize Bluetooth, Wi-Fi, or solutions like ZigBee to transmit data. Again it is the administrator’s responsibility to ensure that the chosen solution is secure.

Secure socket layer (SSL) or a virtual private network (VPN) may be used to move data safely over the Internet. These solutions can significantly reduce throughput when used in a wireless configuration. This drawback is expected to resolve as wireless transmission speeds increase and costs decrease. Currently, the most efficient way to transmit data via wireless is to encrypt the data before it is transmitted and decrypt it on the receiving side.

De-identified PHI can be transmitted without being secured, but it is not recommended unless you are sure that the algorithms being utilized for de-identifying PHI are proven. It only take three pieces of demographic data to identify a person.

**ENCRYPTION**

Any PHI stored on a device or transmitted over the air must be encrypted to inhibit unauthorized users from accessing protected information. Encryption is the action of converting readable text to unreadable text and back again by utilizing mathematical algorithms. The action of converting encrypted data back to readable data is called decrypting.

There are multiple encryption algorithms available to secure PHI. The challenge is to make sure that the data is always protected, end-to-end. My company utilizes AES-256 bit, which is considered military-grade encryption. Mobile devices must encrypt the PHI when it is on the device and only decrypt it for viewing by the intended user. The Department of Commerce regulates encryption and the export of devices and software that contain encryption.12

**DEVICE MANAGEMENT AND PHYSICAL SECURITY**

Device management is one of the biggest challenges in mHealth. But there are systems on the market that will assist in managing mobile devices for both individuals and enterprise users. The primary step in mobile security is to make sure the mobile data stores are secure, and then focus on the physical security of the devices themselves. Countless breaches have been facilitated by the lack of physical device security. Consider, each time a device leaves your building your customers’ PHI and much of your internal records also are leaving the building.

Mobile devices must be managed differently than larger, fixed or physically secure devices. Mobile devices are more difficult to asset manage. Many mobile devices can now be tracked, located and accounted for via GPS. Remote system data removal (wiping) and tracking is available for both individual and enterprise users of smartphones. Companies like Gadgettrak13 offer solutions to not only remove data from your stolen phone or tablet, but also to track them with GPS and remotely enable the cameras on smartphones and laptops to help retrieve the devices. Apple, for example, offers enterprise-level phone management support. Policies should cover usage and security of these devices.

**LEGAL ISSUES**

Wireless devices are fairly new to healthcare and there is no single regulatory agency or organization that covers all aspects of mHealth. The FDA regulates devices that fall under the description of a medical device.

**TERMS AND CONDITIONS**

Terms and conditions of a product is an area in which to consult an attorney. Whether drafting a terms and conditions policy for your organization’s products or reviewing a vendor’s terms and conditions, it’s important to understand what is in this document and how it effects and protects your organization and its PHI. The following are items usually contained in terms and conditions documents:

- Terms of use.
- Contracts.
- Liability.
- Indemnification.
- Responsibilities.
- Privacy policy.
- Data use.

**HIPAA AND HITCO**

Health Insurance Portability and Account-
ability Act (HIPAA) of 1996 and the Health Information Technology for Economic and Clinical Health (HITECH) Act provides transmission guidelines, privacy and security standards and laws for protecting patients’ health records.

HITECH covers culpability for abuse and violations associated with HIPAA. HIPAA laws only apply to certain “Covered Entities.” It would be wise to know if your product or service is a considered a Covered Entity. The HITECH Act is the “teeth” of HIPAA.

The following is from the CMS web site on Cover Entities. The Administrative Simplification standards adopted by the US Department of Health & Human Services (HHS) under HIPAA apply to any entity that is:

- A healthcare provider that conducts certain transactions in electronic form (a “covered healthcare provider”).
- A healthcare clearinghouse.
- A health plan.

An entity that is one or more of these types of entities is referred to as a Covered Entity.

FOOD AND DRUG ADMINISTRATION

The FDA has regulated medical devices for many years, but has focused mostly on hardware and embedded software. In February 2011, the FDA released its Final Rule on Medical Device Data Systems (MDDS), which affects systems that manage data collected by a medical device.

Essentially, if a system, app or mobile devices transmits or displays data from a medical device the system is likely a Class I medical device, or MDDS, and must pass FDA certification. The other aspect of this ruling is that if the data that a device displays, manipulates or transfers was originated from an FDA-classified medical device at any time in the transfer chain, then that device also is an MDDS. The FDA issued a Draft Guideline on Mobile Medical Applications (July 2011) to help to clarify some of the confusion in the industry.

The following is a list of items covered in the draft:

- Mobile platforms.
- Mobile applications.
- Mobile medical applications.
- Regulated medical devices.
- Mobile medical app manufacturers.

When performing due-diligence on a product your organization is building or buying it, check with the FDA to determine if the product is a medical device, deemed a medical device or is connected to one.

The FDA is here to protect, guide and assist. I have spoken to several people that have experience with FDA certification and they suggest that you contact the FDA directly to get clarification. Contact numbers are listed on www.fda.gov.

ORGANIZATIONAL SECURITY POLICY

An organization’s internal policy on mobile device utilization is the first defense against a security breach. Once you have performed a risk assessment and determined who would most likely benefit from compromising your data, you can evaluate what parts of your security plan should be covered with policy.

Following are several tactics to consider when formulating policies:

- Are devices supplied by the employer or employee?
- Lost device procedures.
- Are devices used for combination private and professional use?
- Are the devices user-configurable?
- Can users load apps on smartphones? (Trojan horse malware have been loaded on smartphones via free apps.)
- Is it a closed-loop solution, behind a firewall (i.e., Wi-Fi, NFC)?
- Enforcement procedures and guidelines.

AUTHENTICATION

Username and password. Username and password authentication is one of the simplest protection schemes to implement, and most users are comfortable with it. Unfortunately, it provides minimal security for PHI and there are many issues with the management of users’ credentials.

TWO- AND THREE- LEGGED AUTHENTICATION

Both authentications are based on the “OAuth” standard. Without getting into the low-level details, two-legged authentication is when permission has been given and the tokens for access are stored, but without the user having to give permission each time they access the system. Only tokens are stored, not usernames and passwords. The owner of the data can revoke this access at anytime. Google explains this authentication, as a “dance,” which is a great description that involves the user, the site that is authenticating the users and the authenticating site.

Three-legged authentication involves access being shared with a third party via the owner’s permission. For example, when you login to one web site via another (i.e., Twitter via your Google’s credentials).

The following is a list of credentials that may be utilized for device authentication:

- Universal unique identifier (UUID).
- International mobile equipment identity (IMEI).
- International mobile subscriber identity (IMSI)
- North American Numbering Plan (NANP).
- Electronic device ID.
- Secure micro-SD card (Secure μSD).
- NFC and embedded secure elements (eSEs).

UUID

Currently all cell phones have a UUID embedded/stored in read-only memory (ROM). UUIDs are not guaranteed to be absolutely unique, but the probability of uniqueness is high (see the Birthday Paradox below).

Direct linking of personal information to a UUID is not considered a best practice. However, it is sometimes used a part of a set of identifiers (complex key) to provide a more unique identifier. One issue with the UUID is that it is created and stored differently, depending on the manufacturer’s operating system or device. Apple states, “For user security and privacy, you must not publicly associate a device’s unique identifier with a user account.” Google Android does not have the rule because the user can reset the ID, which eliminates the association.
IMEI
IMEI is a unique device identifier that is set by device manufacturers and embedded into the phone or device’s ROM and is often printed on the phone itself. Other numbers that can link a user to a phone are the electronic serial numbers and mobile equipment identifiers.

IMSI
IMSI is stored on all cell phones, normally on the SIM phone of GSM and R-UMI (removable user identity modules) on CDMA phones. It is used to identify users on networks.23

NANP
The North American Numbering Plan (NANP) is a unique 10-digit number that is used in 19 North American countries, including the United States and US territories, Canada and the Caribbean Islands.24 These numbers can move with the consumer, if they wish to change devices or carriers. This number can be used as demographic data to help identify the user.

ELECTRONIC DEVICE ID
An electronic device ID is a token that is used for identification. There are multiple concepts and algorithms to support these authentication systems. An example of an electronic device ID is the storing of a token on a drive or ROM at a specific location randomly selected by the authentication system. Each time an authentication is requested, the secret location is accessed to retrieve the token and authenticate the device and/or user.

Secure Micro SD Card (Secure μSD). Secure digital memory cards are utilized on mobile devices. Vendors or organizations can provide their preloaded SD cards to utilize a higher level of authentication.25

PREPARE FOR THE WORST
No one wants to think about data breaches, but they do happen. Being prepared for the worst is one of the best strategies for protecting your patients, providers and organizations. There are legal “breach notification” obligations under the HITECH Act that stipulate the procedures and timing of notification in the event of a breach.26

Remember to always expect the best, but prepare for the worst. We have the obligation to secure our patients’ PHI at all times, both to the extent of the law and to the best of our ability. JHIM

Jeff Brandt graduated from the University of Oklahoma with a bachelor’s degree in computer science. He is enrolled in the biomedical informatics graduate program at Oregon Health Sciences University, Portland. Mr. Brandt held the position of Adjunct Instructor of Database Design at Oregon State University. With more than 20 years of experience in healthcare, mobile data/telecom, online banking and the Internet industry, he serves as Chief Technology Officer of Communication Software, which provides consulting services for such clients as Siemens, Warner Music, Cybersash/ Verisign and the Mississippi State Department of Health. He also developed the first secure medical apps for both iPhone and Android.

REFERENCES
1. McNickle M. Five health IT practices hospitals should avoid. mHimss. Available at: www.mhimss.org/news/5-health-it-practices-hospitals-should-avoid#comment-41.
2. Shah S., BS Computer Science, MBA.
3. Tzu S. The Art of War. 544 BC
19. Google. 2-legged OAuth for the OpenSocial REST API. Internet Identity Research. Available at: https://sites.google.com/site/oauth2/goog/2leggedoauth/opensocialrestapi.
Learning from the EHR for Quality Improvement
A Descriptive Study of Organizational Practices

By Bill Bria, MD; Rosemary Kennedy, PhD, MBA, RN, FAAN; and Dana Womack, MS, RN

**ABSTRACT**
An exploratory, descriptive study was conducted to understand current organizational structures and practices related to clinical data analysis for purposes of quality improvement in acute-care settings. Materials and methods included an informal survey of a convenience sample of US-based informatics professionals. The findings suggest sub-optimal use of clinical EHR data for quality improvement, a need for methodologies to assist the prioritization of quality improvement efforts, increased perseverance to ensure that all quality improvement projects go through the full improvement lifecycle, and a need for refined organizational structures and strategies related to secondary uses of EHR data.

We are entering an era where it is possible that clinical-effectiveness research may be accomplished as a byproduct of daily clinical care. It is possible for clinical data analysis to begin at the outset of the implementation of an EHR, but moving the existing culture and expectations of measuring EHR success in terms of “go-live” functionality to measurable improvements in patient outcomes will require significant investment, organizational structural changes, utilization of clinical informatics professionals to their full potential and a willingness to envision a future where care delivery, research and quality improvement coexist at the bedside.

Implementation of health information systems has been a significant focus over the past decade, but now is the time for informatics professionals to collaborate with their technology, quality, and evidence-base practice colleagues to help their organizations transition from “data” and “information” to “knowledge” and actionable insight” levels of information processing.

**KEYWORDS**
Quality, informatics, data, electronic health records, health information systems, acute care, clinical data analysis.
ing, many healthcare facilities with implemented EHRs remain at the “data” and “information” levels of clinical information processing when they have the potential to operate at the “knowledge” and “actionable insight” levels.3

Implementation of an EHR is a foundational component for clinical quality improvement, but the journey to high-quality, efficient care requires a multifaceted strategy that includes leadership, culture change and inter-professional involvement.4 Progress toward the six dimensions of quality identified by the Institute of Medicine (safety, effectiveness, patient-centeredness, timeliness, efficiency and equity) is slowly being made, but the task of improving individual care is hardly completed.5

Clinical analytics must become a pervasive activity in healthcare settings to transform hospitals into learning organizations that continually use EHR data to improve how care is delivered. However, a review of literature reveals that there is a paucity of research regarding hospital organizational structures and practices related to the secondary use of EHR data for clinical quality improvement.6 While a universal definition of clinical data analytics has not yet been established, within the industry, clinical analytics refers to the capture and use of discrete clinical data to identify and measure quality, patient safety or service line efficiencies and improvements.7

The identification of factors associated with clinical outcomes has traditionally been the purview of academic research organizations, and dissemination of new knowledge has historically occurred through conferences and peer-reviewed journals. However, the increased volume of structured clinical data within the EHR, combined with the evolution of the EHR into a quality improvement tool presents healthcare facilities with the opportunity to invert the “bench to bedside” knowledge dissemination paradigm, and combine knowledge creation with care delivery. Additionally, organizations have an opportunity to transition from a reactive stance of addressing mandatory quality reporting mandates to a proactive stance of achieving organizationally driven quality improvements. Objective

A key characteristic of high-performing organizations is the ability of every employee to articulate the meaning of quality in their organization and the impact they each have on quality.9 Recognizing that aggregate clinical data analysis and the application of findings to care delivery is key to clinical quality improvement, the authors conducted an exploratory descriptive study to address a gap in the literature regarding current organizational structures and practices related to clinical data analysis and analytical support of quality improvement, and to inform the design of future related studies.

Materials and Methods

Data gathering for this exploratory, descriptive study was accomplished through an informal survey of US-based informatics professionals. Survey questions were developed by health information technology professionals and face validity was established through peer review. Questions solicited information regarding clinical data analysis team structure, perceived value of clinical data analysis, the role of leadership, and opportunities and barriers related to quality improvement efforts. Convenience sampling of an informal sample of US-based informatics professionals was accomplished through distribution of a web-based survey to four prominent health informatics Listserv subscribers. Employment by a US hospital or hospital-based clinic was a criterion for participation in the survey.

Analysis of findings was accomplished through descriptive statistics and content analysis. Descriptive statistics were used to summarize multiple-choice questions, and content analysis was used to identify themes within free text responses.

SAMPLE DEMOGRAPHICS

A total of 87 complete survey responses were received from an unfixed sample during a three-week period during June and July, 2011. Survey participants represented a variety of organizations including community hospitals (40.2 percent), academic medical centers (33.3 percent), children’s hospitals (5.8 percent), Federal/VA hospitals (5.8 percent), general medical/surgical facilities (4.6 percent) and otherwise classified organizations (10.3 percent).

Multiple hospital bed sizes were represented, including 500+ beds (44 percent); 400-499 beds (14 percent); 300-399 beds (11 percent); 200-299 beds (14 percent); 100-199 beds (13 percent); and 0-99 beds (4 percent). Nursing informatics was the largest professional group represented (25.3 percent) by study participants, followed by directors/managers of informatics (19.5 percent); clinical analysts (11.5 percent); chief medical information officers (10.3 percent); and other roles (33 percent).

RESULTS

Organizational structures. Participants indicated that executive roles focused on technology infrastructure are more frequently present than roles with blended clinical and analytical skills (Figure 1). More than 75 percent of participants report having a chief information officer (CIO) in

![Figure 1: Existence of Selected Executive Roles in Participant Facilities](image-url)
place within their organization; less than 60 percent have a chief medical information officer (CMIO); and less than half report the existence of a Chief Quality Officer (CQO) or chief nursing information officer (CNIO). Nearly 13 percent reported that none of these roles currently exist within their organization.

More than 72 percent of respondents report having a clinical data warehouse in place for two or more years, but only 62 percent report existence of a permanent clinical data analysis team to support of safety and quality initiatives. Nearly 5 percent report that they have no clinical data analysis support (Figure 2).

When permanent analytical team is present, participants indicate that these teams are led by a CQO or other quality leader (40.7 percent), a chief medical officer (16.7 percent), CMIO (14.8 percent), CIO (7.4 percent) or other roles (20.4 percent). Reasons given for the absence of a permanent team include lack of staff with appropriate expertise (48.5 percent), clinical data analysis not a top priority (24.2 percent), preference for temporary teams (6.1 percent), lack of funding (6.1 percent) and lack of adequate technology (6.1 percent). Persons or teams that perform clinical data analysis in support of care improvement efforts are also frequently responsible for producing the organization’s mandatory quality reports (69 percent).

Prioritization practices. Participants indicated that regulatory and payer compliance, sentinel events and opportunities to reduce cost are primary drivers for quality improvement initiatives. However, less than 45 percent of organizations represented have a formal, repeatable process for prioritizing focus areas for improvement initiatives. Participants that reported having a repeatable process for prioritizing clinical improvement initiatives most frequently listed Plan, Do, Study, Act (PDSA) as their methodology.

Participants had variable perceptions of the value that facility leaders place on clinical data analysis, ranging from very valuable (36 percent) to valuable (39 percent), neutral (19 percent), somewhat valuable (5 percent), and not valuable (1 percent). All participants felt that clinical data analysis was highly important to quality improvement efforts, but they consistently were only moderately satisfied with current analytical support (Figure 3).

Quality improvement. While 72 percent of respondents report having a clinical data warehouse in place for two or more years, suggesting that the majority of respondents have fairly mature health information systems in place, improvement projects are challenged to go through the full traditional improvement lifecycle of problem identification, baseline measurement, improvement plan development, plan execution and re-measurement and evaluation. As depicted in Figure 4, nearly half (44.7 percent) of respondents report that only 50 percent to 75 percent of their quality improvement projects go through the full improvement lifecycle, and an additional 30 percent report that less than half of their improvement projects go through the full improvement lifecycle.

While nearly all (>97 percent) facilities report laboratory and pharmacy systems in place, higher level functionality to support decision-making based on the data these
To achieve the nation’s healthcare quality aims of better care, affordable care and healthy people, analysis of aggregate clinical data for purposes of knowledge creation and quality improvement must become pervasive in healthcare settings.

systems lags notably. Only half reported a rules engine or clinical decision support capability in place, and 21 percent do not yet have a clinical data repository (CDR) or data warehouse in place.

When asked about challenges related to improvement initiatives, participants identified baseline measurement (24.1 percent) and re-measurement and evaluation (33.3 percent) as the most problematic phases of the improvement lifecycle (Figure 5). Notably, the phases identified as most problematic are phases that rely heavily on clinical analytics.

DISCUSSION
Although many clinicians believe that they are practicing up to date, evidence-based medicine, wide practice variations suggest that clinical practice often falls short of the best evidence available. The healthcare information age, now experiencing its greatest growth phase in the history of the United States, has the potential to eliminate this “evidence gap” through dissemination of best-known clinical practices to clinicians through clinical decision support tools delivered via the electronic health record and other information instruments.

The lack (<45 percent) of formal, repeatable processes for prioritizing focus areas for safety or quality improvement initiatives within organizations suggests that prioritization of improvement initiatives is not occurring consistently in US hospitals. Indicative of a culture that focuses primarily on “hot spots”, survey respondents indicated that regulatory/payer compliance, sentinel events and opportunities to reduce cost are primary drivers for safety/quality improvement initiatives. But to achieve the nation’s goal of timely, effective and affordable care, analysis of aggregate clinical data for purposes of knowledge creation and quality improvement, concurrent with care delivery, must become pervasive in healthcare settings.

Adoption of methodologies for prioritizing and tracking initiatives through the full care improvement efforts is imperative, as
Clinical analytics must become a pervasive activity in healthcare settings to transform hospitals into learning organizations that continually use EHR data to improve how care is delivered.

While the need for an EHR implementation and governance infrastructure is widely recognized, an organizational “analytic governance” infrastructure is equally important. To realize anticipated benefits of widespread EHR adoption, healthcare facilities must implement analytic governance processes that include data management, prioritization and governance of clinical improvement initiatives, prioritization and execution of clinical data analysis, followed by reprioritization (Figure 6).

Analytical activities must span multiple functional areas within acute care facilities. The existence of organizational “silos” such as clinical, quality, research, finance and health IT present a significant challenge to the creation of a consistent, vital informatics infrastructure to support effective use of clinical data. Successful transformation of US health entities into learning health organizations will require that technologies become progressively more invisible, while the core foci of clinical (patient care), research (new knowledge), quality (continuous quality improvement) and finance (compliance and revenue) become the dominant drivers of coordinated informatics activities.

The study also highlights the importance of contextual factors influencing clinical data analytics such as leadership and culture. This finding is consistent with the literature showing the multi-dimensional impact of cultural influences which operate across multiple levels within the organization. Moving the existing culture and expectations of measuring EHR success in terms of “go-live” functionality to measurable improvements in patient outcomes will require significant investment, organizational structural changes, utilization of clinical informatics professionals to their full potential, and a willingness to envision

---

**FIGURE 6: Clinical Analytic Governance**

- Continuous Data Acquisition & Analysis
- Analytic Governance
  1. Manage data acquisition streams
  2. Prioritize improvement focus areas
  3. Prioritize analytics
  4. Execute data analysis

---
More than 72 percent of respondents report having a clinical data warehouse in place for two or more years, but only 62 percent report existence of a permanent clinical data analysis team to support of safety and quality initiatives.
Healthcare Technology Challenges 2020
Defining a Framework for Success

By Stephen Grimes, FHIMSS, FACCE, FAIMBE

ABSTRACT

Over the next 10 years, healthcare technology will give us the possibility of transforming healthcare delivery in ways that can offer unprecedented quality, timeliness, effectiveness and availability. Some of these technologies include integrated clinical information systems, robotics, imaging, genomics, telemedicine and nanotechnologies.

However, these technologies are increasingly complex and integrated. Most organizations do not have the infrastructure to adequately deal with the proper selection, deployment or support of these new and emerging tools. These healthcare organizations must adopt strategic processes to ensure they select technologies appropriate to their missions and goals. These organizations must also evolve existing services, such as clinical engineering and information technology, into a seamless support service for medical and information technologies by adopting a common governance framework. Implementing a strategic technology selection process and evolving the technology support infrastructure (staff, processes, tools) are necessary to achieve the substantial benefits to patient care and economic sustainability.

KEYWORDS

Clinical engineering, medical technology, healthcare technology, governance, technology assessment, infrastructure.

WE ARE in a period of great change in healthcare. Much of what we have seen in recent years and much of what we are likely to see is attributable to the healthcare industry’s adoption and use of rapidly evolving technologies, including medical devices/systems, information systems and telecommunications. These tools are critical to existing and future gains with respect to the quality, timeliness and effectiveness of patient care. That healthcare technology has and will continue to play a critical role was acknowledged in the Institute of Medicine’s seminal report *To Err is Human*, where it was stated that going forward, “technology ... has to be recognized as a ‘member’ of the [healthcare] work team.” In the IOM’s 2010 report *The Future of Nursing*, they acknowledge “there is perhaps no greater opportunity to transform [healthcare] practice than through technology.”

We have come to heavily depend on technology—this “member” of the healthcare team—and our ability to deliver care can be severely compromised when this team member is not ready and available. We also note that these technologies, on which we
have become increasingly dependent, have come at the expense of significant increases in both healthcare complexity and cost.

**Increased complexity.** A Networking and Information Technology Research and Development (NITRD) program report from 2009 describes how “older generations of mechanical, analog and electromechanical devices ... have been largely replaced by devices and systems based on information technologies” and how these devices/systems are “often connected to other devices in increasingly complex configurations, potentially creating systems of systems that span scales from tiny ... to ultra-large.”

Formerly passive technologies have largely been replaced by new systems of systems (SoS) that actively control critical physiological processes and functions.

**Increased cost.** Healthcare technologies are major contributors to increasing healthcare costs. Technology-associated gains have come at a significant financial cost to this industry. The 2008 U.S. Congressional Budget Office (CBO) estimates that nearly half of the annual double-digit increases we have experienced in health care over the previous decade are the direct result of our adoption and use of new technologies. One of the largest U.S. healthcare enterprises, Kaiser Permanente, reported that between 1997 and 2007 their spending on health technologies and related procedures increased by 830 percent.

By the end of 2011, annual spend by the U.S. healthcare industry for information technology is expected to reach $40 billion ... with an estimated 24 percent compound annual growth rate (CAGR) between 2012 and 2014. Estimates are that industry will spend an additional $105.8 billion for medical devices/systems for that year. These numbers help put in perspective the relative size of the financial implication of technology on healthcare costs—and also indicate how the technology spent is portioned between information and medical technologies, as depicted in Figure 1.

Fully realizing the benefit of new medical devices/systems, information systems and telecommunications technologies will require that we understand and address the full impact of these technologies, including the consequences of increased complexity and cost, as well as the increased benefits.

In what follows, we more fully lay out some of the most promising categories of evolving healthcare technology as well as some of the key elements in a new infrastructure paradigm that is designed to similarly evolve with and appropriately support these new technologies.

**THE PROMISE OF HEALTHCARE TECHNOLOGY**

Technology has the potential to play a transformational role in healthcare delivery. If appropriately selected, deployed and used, technology can be a major enabler for clinicians in advancing patient care. It can positively influence work processes, facilitate seamless exchange of data and provide critical information to clinicians, enabling them to deliver more appropriate and timely patient care.

Healthcare technologies available today or in the near term have the prospect of significantly improving the quality, timeliness, and effectiveness of patient care; patient and staff safety; and business operations (e.g., management, scheduling, billing). Examples of technologies that either now impact or over the next ten years will impact patient care in a significant way include:

- **Integrated clinical and information technology systems.** Information technology promises to play a greater role in the clinical aspects of healthcare, in addition to the business aspects. The number of diagnostic, therapeutic and information systems is rapidly rising with an overall synergistic effect. Benefits gained from integrating these systems can far exceed the benefits available when individual devices and systems are used in a standalone mode.

- As a consequence of our ability to increasingly integrate and use clinical and information technologies to gather growing amounts of data from medical devices about a patient’s condition, there has been a corresponding need to process that data into information in a way that is meaningful to the diagnostician and therapist without causing them to suffer “data overload.”
New knowledge-based or evidence-based expert and decision-support systems are designed to collect data and suggest diagnoses and courses of treatment based on pre-selected rules for decision-making within specialized domains of knowledge.

Intelligent communication technologies can insure the right information gets to the right provider at the right time to insure the right patient gets the right care.

Increased reliability for critical patient care applications will be achieved by the incorporation of autonomic capabilities similar to the human body’s involuntary nervous system (i.e., that allows the human body to adjust to environmental changes, external attacks and internal failures). As autonomic features are incorporated, these critical systems will increasingly:

1. Be self-aware.
2. Adapt to environmental changes.
3. Continuously adjust to optimize performance.
4. Defend against attack.
5. Self-repair.
6. Exchange resources with unfamiliar systems.
7. Communicate through open standards.
8. Anticipate users’ actions.

The use of autonomic systems will enable us to realize the benefit of increasingly complex technologies that, without their autonomic abilities, would quickly overwhelm us with their need for management and support.

Integration has the potential to bring healthcare resources to any near or remote location and to facilitate medical data, voice and video communications between a combination of patients, providers and payers.

Digital imaging. Advances in imaging technology enable clinicians to view physical details that were not discernable with earlier imaging systems. New systems can even evaluate biologic processes and events as they occur in vivo. New images offered through advanced technologies give functional images of blood flow and metabolism essential to diagnoses and to research on the brain, heart, liver, kidneys, bone and other organs.

Telemedicine & telehealth. Improve-
ments in telecommunications, information and medical technologies are greatly expanding opportunities for the application of telemedicine and telehealth. With the availability of high-resolution imaging, non-invasive telemetric sensors, robotics and high-speed broadband connections, providers have the capability of remotely monitoring, diagnosing and treating patients in a manner that both makes optimum use of clinicians’ time and delivers care when and where needed by the patients.

Robotics. Use of robotics in patient treatment can facilitate both remote access by a provider to a patient as well as access to areas on or in the patient that may be otherwise difficult or impossible to reach by traditional methods. The provider’s ability to operate more accurately may be enhanced, the patient’s recovery time may be significantly reduced and access may be greatly improved.

Accuracy. Robotic systems can perform procedures (e.g., surgery) more steadily than the human hand and with much greater control. Complex procedures will greatly benefit from the increased steadiness and control offered by these systems.

Minimally-invasive procedures. Because robotic systems can operate in much smaller and more confined spaces than the human hand, these systems can be much less invasive and consequently require less recovery time and reduce the likelihood of complications (e.g., infection and blood loss).

Remote procedures. Robotic systems are being utilized to treat patients when it is not feasible to have an operator at the patient’s side.

Micro- and nanotechnologies. Microscale analytic systems are under development that will provide a “laboratory on a chip.” The result will be a highly portable platform that is capable of remote screening and, as a consequence, accomplishing earlier detection in the disease process.

Micro-scale diagnostic sensors are available that offer the ability to do minimally intrusive, continuous physiologic monitoring of ambulatory and non-acute patients.

Micro- and nano-sensors under development can serve as probes and detectors at an organ, tissue, cellular, or even molecular scale. Micro- and nano-scale devices are being designed to function as artificial organs and surgical instruments.

Nano-particle vectors are being developed to aid in drug delivery and DNA modification level.

Genomics. Technologies under development will screen and identify individuals who possess genes that predispose them to certain diseases. Knowing who is predisposed to what disease will enable us to focus our preventive efforts on those most at risk. As our understanding of the genome improves, we will have the ability to develop treatments that target affected genes while other treatments can be optimized for an individual patient based on what we know to be effective for someone of their genetic make-up.

If managed well, these technologies have the potential to make possible the efficient delivery of better quality healthcare at affordable costs in a greater variety of venues to a population that has been underserved. If not managed well, these same technologies can financially drain healthcare organizations, create workflow nightmares and pose major risks to the care and safety of its patients.

THE CHALLENGE OF REALIZING THE PROMISE

While healthcare technology has the potential to greatly enhance our ability to deliver safe, effective and timely patient care, these benefits are not automatic.

Technology must be strategically applied and aligned with the organization’s mission and goals. The spectrum of healthcare technologies available now and in the near future leaves healthcare providers with a broad range of choices. These provider organizations must select from among those technologies based on an evaluation of their relative benefits and the degree to which the application of any of these technologies contributes to the organization’s stated mission and goals. Anticipated benefits (e.g., improvements in care outcomes, patient/staff safety,
increased revenue, reduced costs, operational efficiencies, demographics served, market perception) should be based on available evidence.

Effective technology implementations require process and workflow changes. To gain planned benefits, virtually all significant technology implementations require changes in workflow processes. In fact, often a major goal of new technology implementations is to achieve safer, more efficient and effective workflows. To insure these desired improvements are achieved, those processes and workflows should be analyzed and adequately planned with all relevant stakeholders (e.g., managers, users) prior to technology implementation.

Metrics enabling the organization to monitor the benefits gained must be established and employed. Prior to selecting and deploying new technologies, the organization should identify appropriate metrics to employ in determining the degree of success in achieving each of the anticipated benefits. The use of such metrics in assessing improvements in care outcomes, patient/staff safety, increased revenue, reduced costs, operational efficiencies, demographics served, market perception will help validate the planning process or focus attention on those process areas in need of improvement.

Technology also presents risks that must be anticipated and addressed if potential benefits are to be fully realized and the potential adverse affects are to be avoided. Some factors contributing to these risks and some consequences include:

Increased complexity associated with new healthcare technologies. Healthcare technology has grown considerably more complex over the last 20 to 30 years. The evolution of healthcare technologies can be summarized in three key trends:

- Most electronic medical devices are designed with microprocessors and essentially operate as special purpose computers.
- Computerized medical devices have an increasing number of features/options that enable them to collect, process and store increasing amounts of medical data. Given this increased complexity, clinician training (and re-training) on operating procedures, safety precautions, basic troubleshooting and backup procedures are critical.
- There is a growing trend to integrate and interconnect/network disparate medical (and information) technology devices and systems to facilitate an increased exchange of medical data. A 2010 survey conducted by the College of Healthcare Information Management Executives (CHIME) concluded that 23 percent of medical devices in respondents’ medical device inventories were already networked and an additional 8 percent, while not yet connected, were network-capable. These interconnections further compound the complexity of these systems.

New technologies applied with without requisite changes in processes and workflows. New technologies usually require workflow and process changes and often are acquired specifically because of anticipated improvements in safety and efficiency. Failure to plan for new workflow processes or involve key stakeholders in implementing needed process changes can result in new technology implementations that are less safe, less efficient and more costly than the old technologies they replaced.

Introduction of new vulnerabilities: Single points of failure (SPOF) on clinical systems that can affect multiple patients. Discrete devices and components are generally more reliable today than their predecessors of 20 or even 10 years ago. However the interconnection of these devices/components often creates complex, integrated clinical systems potentially affecting many more patients than the standalone device. The interconnection also often introduces new vulnerabilities by incorporating devices/components that are single points of failure (SPOF). If these SPOF devices/components do fail, they have the potential to take down an entire system and affect the care and safety of many patients as well as business operations.

Increased dependence on new technologies. Due to the enhanced benefits these systems offer, clinicians’ dependence on the information maintained and transmitted by systems for effective and timely diagnosis is likewise increasing. This dependence on integrated systems can have major implications on the clinician’s ability to deliver patient care and on business operations if those systems should fail. And some systems are likely to fail with the potential for dire consequences for patient care, patient/staff safety, or operations, particularly if adequate steps are not taken to identify and mitigate the associated risks.
The bottom line is that no organization can afford to acquire and deploy major new healthcare technologies without first giving appropriate consideration to the strategic clinical, operational, and financial implications of that acquisition.

**Feature: Strategic Planning**

Today’s healthcare technologies have major implications for patient care, operations and finances. Because of their impact on patient care, their level of technical integration and their need for support, the deployment of any new healthcare technology can easily have a ripple effect on a wide range of an organization’s clinical, support and business operations.

Corresponding to their growing impact on operations, healthcare technologies can also have a major impact on the organization’s financial resources. In recent years, costs associated with healthcare technologies have been responsible for nearly 40 percent of the healthcare cost increases faced by providers. Inadequate consideration of all technology costs relative to technology’s benefits can significantly compromise both the quality of an organization’s financial investments as well as the hoped for benefit gains. The bottom line is that no organization can afford to acquire and deploy major new healthcare technologies without first giving appropriate consideration to the strategic clinical, operational, and financial implications of that acquisition.

To address the challenge of identifying new healthcare technologies for acquisition, some provider organizations are establishing a form of “strategic healthcare technology assessment” committee. This committee would be multidisciplinary and may include:

- Department chairs
- Chief Medical Officer (CMO)

**Strategic Technology Planning Services**

Today’s healthcare technologies have major implications for patient care, operations and finances. Because of their impact on patient care, their level of technical integration and their need for support, the deployment of any new healthcare technology can easily have a ripple effect on a wide range of an organization’s clinical, support and business operations.

Corresponding to their growing impact on operations, healthcare technologies can also have a major impact on the organization’s financial resources. In recent years, costs associated with healthcare technologies have been responsible for nearly 40 percent of the healthcare cost increases faced by providers. Inadequate consideration of all technology costs relative to technology’s benefits can significantly compromise both the quality of an organization’s financial investments as well as the hoped for benefit gains. The bottom line is that no organization can afford to acquire and deploy major new healthcare technologies without first giving appropriate consideration to the strategic clinical, operational, and financial implications of that acquisition.

To address the challenge of identifying new healthcare technologies for acquisition, some provider organizations are establishing a form of “strategic healthcare technology assessment” committee. This committee would be multidisciplinary and may include:

- Department chairs
- Chief Medical Officer (CMO)
The role of such a committee is to serve as a the healthcare provider’s gateway for new and emerging healthcare technologies (generally limited to those with an impact of capital-plus-first-year-operating impact of $100,000) by proactively examining which of these technologies provides benefits that best meet the mission and goals of the provider organization. These benefits may fall into one or more of the following categories:

- Improved care outcomes.
- Improved patient/staff safety.
- Regulatory compliance.
- Improved efficiency and workflow processes.
- Improved revenue, particularly revenues improvements associated with pay for performance (P4P) initiatives.
- Reduced costs.
- Broader demographic served.
- Market perception (reputation).

This committee should:

- Focus on—and provide the greatest weight to—evidence-based reviews of new technologies and seriously consider those that most further the service objectives of the organization.
- Charge appropriate stakeholders with the task of analyzing and planning workflow processes associated with effective deployment of new technologies and reporting findings back to the committee.
- Establish appropriate metrics to determine how well the new acquisitions achieve each of the benefits predicted... and should in turn adjust their decision-making processes when anticipated results are not subsequently achieved.
- Adopt a long, strategic view of its role and should promote the concept that healthcare technologies are not departmental, but organizational, assets that need to be properly integrated technically and operationally if the anticipated benefits those technologies are to be fully achieved.
- Avail itself of appropriate staff expertise, particularly from senior experts in clinical engineering and information technology who can identify required infrastructure associated costs (e.g., facilities, staffing, supplies, training, service/support); and conduct a risk analysis to identify vulnerabilities and the degree to which they can be reasonably mitigated.

HEALTHCARE TECHNOLOGY SUPPORT SERVICES

To achieve the promise of the new technologies, healthcare providers also need to develop an infrastructure that is conducive to the appropriate selection, efficient deployment and safe use of those technologies.

The increasingly complex nature of and expanding role of healthcare technology requires a corresponding increase in sophistication of that infrastructure. Infrastructures (i.e., support staff, services, processes, facilities, utilities) that were adequate to support technologies of 20 to 30 years ago are not adequate to support technologies of today let alone provide the support those healthcare organizations will need to deal with technologies in the near future. Going forward, healthcare organizations need to plan for the continual evolution of their infrastructures to meet the new challenges associated with these converging technologies. These organizations need to insure their infrastructures are both prepared to address the substantial increases that has occurred in deployed technologies and also better allocated between the support of medical and information systems (e.g., where the value of medical technologies acquired by U.S. healthcare organizations is reported to be more than twice the value of health IT acquired by those organizations).²

A critical aspect of the evolution of an effective infrastructure is the successful integration and collaboration between clinical engineering (CE), information services (IS) and telecommunications to support their converging technologies. Medical device/system support in healthcare organizations has traditionally been the domain of CE services. Information technology support has usually been addressed separately by IS. The reality of today’s medical and information technology convergence is that CE and IS must harmonize their efforts if they are to effectively support these increasingly linked technologies.

Close collaboration and some integration is vital. It is also vital that healthcare organizations realize that, while the technologies are converging and the support model (i.e., clinical engineering, information services, telecommunications) needs to adapt (Figure 2), it is important that the best elements of each be preserved in the adaption and integration process. This is particularly critical when the CE and IS...
are brought together in a shared reporting relationship. Because CE is usually significantly smaller (i.e., staffing, budget) than IS in most organizations, clinical engineering is more vulnerable to loss of its unique character in any “merger.” Among the most important aspects of a typical clinical engineering service to preserve is their focus on the nuances of technology application at the point of patient care. As a consequence of their professional training and experience, clinical engineers (CE) and biomedical engineering technicians (BMET) generally understand those nuances to include:

- Patient safety issues.
- The benefits and risks of medical technology on the patient.
- Their primary role as supporting the clinicians who are responsible for delivering care.
- The interface between patient, device, clinician and environment.
- How response time in addressing medical technology issues can have a significant impact on patient safety and the delivery of care.
- Regulations and best practices associated with the use of medical technology in patient care.
- The management of medical device hazards and recalls.

Support of medical devices and systems cannot be rendered safely or effectively without this patient-centered perspective. However, converging technologies bring new challenges into the medical technology support arena and the move from what were primarily discrete medical devices to integrated systems requires another level of technology sophistication for those who are involved in the selection, deployment and support of those integrated medical systems.

It remains critical to retain the patient focus when supporting these systems, but it also is critical to appreciate that these medical technology systems are typically more complex and may have implications for more than one patient’s care or safety. Some of these medical systems may even be considered “life critical” in the same sense that some business systems are considered mission critical. Effectively supporting these integrated medical systems requires not only the above-described “patient focus” but also an understanding of the complexity inherent in a system of interconnected devices collecting, exchanging, and processing patient data. Those charged with the primary support of these integrated medical systems must evolve their service paradigm and their skills to account for the fact that these technologies are an integration of medical and information systems.

**SHARED GOVERNANCE FRAMEWORK**

The reality of medical and information technology convergence has led to a growing number of healthcare organizations to bring their clinical engineering and information services together under a common organizational framework in order to foster collaboration and coordination of efforts on technology issues in an increasingly common workspace. While there is growing recognition of the need for collaboration, the industry has yet to arrive at a consensus on how best to achieve it beyond changing lines on the organization chart.

The best solution for effective collaboration (regardless of reporting relationships for CE and IT) is likely to be found in the adoption of a common governance framework such as the *Information Technology Infrastructure Library (ITIL)* or ISO/IEC 20000-1:2005 Information Technology – Service Management.

In *The Gartner Group’s* 2008 report on “Top 12 Actions for the CIO,” they insist that healthcare organizations who have not done so seriously consider the adoption of ITIL. As a proven set of IT best practices, Gartner says ITIL provides a framework for delivering services in healthcare organizations where those information technology services are increasingly critical to all aspects of the organization’s operations. An advantage in adopting either ITIL or an ISO/IEC 20000-1 governance model is that both clinical engineering and information technology share common elements in those models. By adopting and adapting elements in such standard governance models, clinical engineering services map well to the respective processes in informa-
tion services (Figure 3). Both clinical engineering and information services could and should retain their unique aspects (i.e., clinical engineering’s focus on patient safety and the clinical environment) but through a shared governance model, both would have a bridge that could help ensure seamless support for converging technologies.

A spectrum of service elements make up a comprehensive clinical engineering or medical technology service (Figure 4). Ideally every healthcare provider would have access to these services to insure effective support. In practice, many healthcare providers fragment the responsibility for services and assign or leave the responsibility for some elements to other departments or vendors. As a result of this fragmentation, some of these service elements are either delivered inconsistently or not delivered at all. As the number of complex, integrated, converged systems increases, the need to consolidate infrastructures and offer a comprehensive CE and IS that work together seamlessly becomes vital.

Adopting one of the aforementioned governance frameworks can help identify any gaps critical gaps in the infrastructure and insure there is effective integration of medical and information technology services.

NEW HYBRID ROLES

Another consequence of the need for evolving infrastructures is likely to be new hybrid of roles that build on critical elements from both clinical engineering and information services. Among the most important of these growing new hybrid professionals are:

- Clinical systems engineers (CSE) who will focus on strategic planning and management services associated with increasingly complex integrated medical systems.
- Clinical systems support specialists (CSSS) will focus on technical services such as installation, configuration, repairs of these integrated medical systems.
- Radiofrequency spectrum managers (RSFM) will focus on monitoring and managing the influx of an increasing number of electromagnetic energy sources that compete for available spectrum and that, without effective management, could have a severe adverse affect on patient care or safety.

Figure 5 is a Venn diagram that illustrates the relationship between clinical engineering (medical technology service management) professional domains (i.e., technology management, professional engineering and engineering technology) and their sub-and cross-specialties.

Position descriptions outlining possible roles, responsibilities, and qualifications for clinical systems engineers (CSE), clinical systems support specialists (CSSS), and radiofrequency spectrum managers (RFSM) are provided in Table 1.

A STANDARD FOR CONDUCTING RISK MANAGEMENT ON MEDICAL DEVICE NETWORKS

A recently adopted ANSI/AAMI/IEC standard establishes guidelines and also defines key roles necessary for managing the challenges associated with increasingly complex and integrated medical technologies. The standard, ANSI/AAMI/IEC 80001-1:2010 Application of risk management for IT networks incorporating medical devices, outlines a risk management approach to managing the acquisition, deployment and support (addressing the entire life-cycle) of these integrated medical technologies. Among its most significant provisions, the standard defines these required roles and responsibilities:

- The health delivery organization’s top management (i.e., management of the organization owning/operating the system) is responsible for
  1. Establishing policies.
  2. Providing adequate resources (e.g., financial, staffing) to conduct meaningful risk management.
  3. Periodically review the performance of the risk management process.
- The medical IT network risk manager (e.g., clinical systems engineer) is responsible for the execution of the risk management process and for ensuring the safety, effectiveness, data/system security, and interoperability of integrated medical technologies—and for engaging appropriate stakeholders in this process and reporting results to senior management.
- The manufacturer be responsible for providing:
  1. Instructions on integrating a medical device into an IT-network.
  2. Information regarding any known risk vulnerabilities.
  3. Information on device security features that would be useful in any mitigations.

Taken together with an appropriate governance frameworks like ISO 20000 (on which 80001-1 was in part based) and ITIL, this standard’s refocusing of clinical engineering (and appropriate IT) resources on a
**TABLE 1: CE-IT Hybrid Roles**

<table>
<thead>
<tr>
<th><strong>Clinical Systems Engineer (CSE)</strong></th>
<th><strong>Clinical Systems Support Specialist (CSSS)</strong></th>
<th><strong>Radio Frequency Spectrum Manager (RFSM)</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Coordinates an organization-wide program to insure the effective deployment, integration and support of interconnected medical systems</td>
<td>Responsible for providing engineering support of specialized medical devices and systems (e.g., cardiology, neurology, surgical, monitoring). This support may include installation, integration, clinical training, operation, diagnostics, technical service, and vendor management in these specialized areas.</td>
<td>The RFSM is responsible for enterprise-wide management and monitoring of the radio-frequency environment.</td>
</tr>
<tr>
<td><strong>Responsibilities</strong></td>
<td><strong>Responsibilities</strong></td>
<td><strong>Responsibilities</strong></td>
</tr>
<tr>
<td>Maintains current inventory of networked and integrated medical systems (including catalog of services, features, interconnections)</td>
<td>Maintains accurate inventory (including configuration information) of all devices, systems and components in their environment</td>
<td>• Maintaining an inventory of all RF systems operating in or affecting the clinical environment.</td>
</tr>
<tr>
<td>Coordinates security management process including risk (e.g., criticality &amp; probability) and vulnerability analysis and related documentation associated with interconnected/integrated medical systems</td>
<td>Coordinates deployment of new medical technologies in assigned areas including planning, needs analysis, evaluations, installation, integration and training</td>
<td>Managing deployment and operation of RF systems so as to assure regulatory compliance and to minimize adverse interactions between devices and systems.</td>
</tr>
<tr>
<td>Coordinates with stakeholders a process to prioritize, develop and implement plan to manage/mitigate identified risks associated with interconnected/integrated medical systems by applying appropriate administrative, physical &amp; technical safeguards</td>
<td>Manages other special projects associated technologies considered for or currently used in assigned area(s).</td>
<td>Advising in selection of compatible RF systems.</td>
</tr>
<tr>
<td>Maintains the integrity of FDA approval for interconnected / integrated medical systems</td>
<td>Monitors operational effectiveness of medical devices and systems in assigned area(s) and insures devices/systems are effectively maintained by judicious application of scheduled &amp; corrective maintenance, upgrades and overhauls as appropriate</td>
<td>Planning for/F allocation, deployment, integration and upgrades as necessary.</td>
</tr>
<tr>
<td>Works with stakeholders to insure effective deployment, integration, and support of new medical systems into legacy systems and non-medical elements of the organization’s information infrastructure.</td>
<td>Monitors and adopts automated hardware/software tools to monitor and manage device &amp; system performance</td>
<td>Obtaining requisite licenses/permits and insuring all are kept current.</td>
</tr>
<tr>
<td>Works to assure systems are deployed into an optimum (i.e., secure &amp; supportive) environment.</td>
<td>Develops or acquires and deploys administrative, technical and physical safeguards to maintain integrity and availability of clinical information maintained or stored by medical devices &amp; systems</td>
<td>Investigating reports of possible adverse RF effects on devices/systems and identifying appropriate corrective action as necessary.</td>
</tr>
<tr>
<td>Continually reviews system components to determine which are obsolete or otherwise no longer adequately supportable and then plans for and implements component upgrades/replacement in a timely manner.</td>
<td>Develops and provides operational and service training to clinicians and support personnel on devices and systems in assigned area(s).</td>
<td>Educating users and monitoring user practices associated with RF system in order to assure their safe and effective operation.</td>
</tr>
<tr>
<td>Identifies and manages appropriate software upgrades, security patches and anti-virus installs for interconnected/integrated medical systems according to industry best practices</td>
<td>Provides consultation to clinical staff on capabilities and limitations of available technologies</td>
<td><strong>Qualifications</strong></td>
</tr>
<tr>
<td>Manages Root Cause Analysis (RCA) and Failure Mode Effects Analysis (FMEA) on incidents involving integrated medical systems and reports findings to appropriate stakeholders for follow-up action</td>
<td>Represents technology perspective for assigned area(s) as needed at meetings with other stakeholders</td>
<td>Bachelor’s of Science degree in Electrical Engineering (relevant training may substitute).</td>
</tr>
<tr>
<td>Monitors and adopts industry “Best Practices” to insure integrity, availability &amp; confidentiality of data maintained and transmitted across interconnected and integrated medical systems</td>
<td>Monitors medical device hazard/recall reports for their assigned area(s) and insures appropriate follow-up (e.g., communication, corrective action, follow-up)</td>
<td>5 years of experience in Spectrum Management, RF safety, license application process.</td>
</tr>
<tr>
<td>Educates stakeholders on security and other implications associated with the proliferation of interconnected and integrated medical technologies.</td>
<td>Monitors regulatory developments affecting devices &amp; systems in assigned area(s) and identifies/coordinates implementation of appropriate compliance measures</td>
<td>Knowledge of RF related rules, regulations and best practices.</td>
</tr>
<tr>
<td>Supervises clinical engineering, clinical systems support specialists and other staff as necessary in clinical systems integration and infrastructure support (e.g., hybrid reporting structure, project supervision)</td>
<td>Maintains technical library and database with information critical to the support of devices and systems in assigned areas</td>
<td>Strong communication and team building skills across functional areas.</td>
</tr>
<tr>
<td>Qualifications</td>
<td>Qualifications</td>
<td>Proficiency with standard desktop applications such as Microsoft Word and Excel.</td>
</tr>
<tr>
<td>Baccalaureate degree in Biomedical or Clinical Engineering (Master’s preferred)</td>
<td>Bachelor’s of Science degree in Biomedical or Clinical Engineering, Engineering Technology or related area</td>
<td><strong>Works with Stakeholders</strong></td>
</tr>
<tr>
<td>5-10 years experience in clinical engineering and information systems</td>
<td>3 years experience in Biomedical or Clinical Engineering and clinical systems support</td>
<td>Clinicians (system users including physicians, nurses, technologists, etc).</td>
</tr>
<tr>
<td>Project management and planning skills/experience</td>
<td>Strong communication and team building skills across functional areas.</td>
<td>Manufacturers/vendors.</td>
</tr>
<tr>
<td>Strong communication and team building skills across functional areas.</td>
<td>Effective educator, mentor and role model.</td>
<td>Information Services.</td>
</tr>
<tr>
<td>Certification (completed or in process) preferred in one or more of following:</td>
<td>Demonstrated project management &amp; planning skills</td>
<td>Procurement/purchasing/materials management.</td>
</tr>
<tr>
<td>Certified Clinical Engineering (CCE)</td>
<td>Certification (completed or in process) preferred in Clinical Engineering (i.e., Certified Clinical Engineer / CCE) or Certified Biomedical Equipment Technician (CBET)</td>
<td><strong>Works with Stakeholders</strong></td>
</tr>
<tr>
<td>Certified Information Systems Security Professional (CISSP) by (ISC)²</td>
<td></td>
<td>Clinicians (system users including physicians, nurses, technologists, etc).</td>
</tr>
<tr>
<td>Cisco Certified Network Associate (CCNA) or Network Professional (CCNP)</td>
<td></td>
<td>Manufacturers/vendors</td>
</tr>
<tr>
<td>Microsoft Certified Systems Administrator (MCSA) or Engineer (MCSE)</td>
<td></td>
<td>Information Services</td>
</tr>
<tr>
<td>Works with stakeholders</td>
<td></td>
<td>Procurement/purchasing/materials management</td>
</tr>
<tr>
<td>Information Services (including network support, disaster recovery)</td>
<td></td>
<td><strong>Responsibilities</strong></td>
</tr>
<tr>
<td>Clinicians (system users including physicians, nurses, technologists, etc)</td>
<td></td>
<td>• Advise in selection of compatible RF systems.</td>
</tr>
<tr>
<td>Medical system manufacturers/vendors</td>
<td></td>
<td>• Planning for RF allocation, deployment, integration and upgrades as necessary.</td>
</tr>
<tr>
<td>Risk management</td>
<td></td>
<td>• Obtaining requisite licenses/permits and insuring all are kept current.</td>
</tr>
<tr>
<td>Information Security</td>
<td></td>
<td>• Investigating reports of possible adverse RF effects on devices/systems and identifying appropriate corrective action as necessary.</td>
</tr>
<tr>
<td>Procurement/purchasing/materials management</td>
<td></td>
<td>• Educating users and monitoring user practices associated with RF system in order to assure their safe and effective operation.</td>
</tr>
<tr>
<td>Clinical engineering</td>
<td></td>
<td><strong>Qualifications</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Bachelor’s of Science degree in Electrical Engineering (relevant training may substitute).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>5 years of experience in Spectrum Management, RF safety, license application process.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Knowledge of RF related rules, regulations and best practices.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Strong communication and team building skills across functional areas.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Proficiency with standard desktop applications such as Microsoft Word and Excel.</td>
</tr>
<tr>
<td></td>
<td></td>
<td><strong>Works with Stakeholders</strong></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Clinicians (system users including physicians, nurses, technologists, etc).</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Manufacturers/vendors.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Information Services.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Procurement/purchasing/materials management.</td>
</tr>
</tbody>
</table>
While convergence of clinical, information and telecommunication technologies in healthcare has been rapidly accelerating for more than 20 years, the development of integrated services by healthcare providers to effectively handle the acquisition, deployment and support of these converged technologies has severely lagged.

Evolving technology is a steamroller that is even now changing the healthcare delivery landscape. All of us now have a short time to decide whether we’ll be part of the steamroller—or part of the road.

CONCLUSION

There is an opportunity for current and emerging technologies to play a major role in transforming healthcare delivery. We have mentioned clinical information systems, robotics, imaging, genomics, telemedicine and nano-technologies as being among the transformational technologies that can help achieve unprecedented improvements in the quality, effectiveness, timeliness and availability of patient care. However these technologies are often complex and require an unprecedented level of integration. Successfully achieving our patient care goals requires new strategic processes and an evolution in the infrastructure necessary to support these complex, integrated technologies. When selecting new healthcare technologies for deployment, we have discussed how organizations must adopt a strategic approach and insure appropriate consideration is given to the overall impact (e.g., clinical, operational, financial). We have also discussed how healthcare organizations must also look to evolve their technology support infrastructures to insure clinical engineering and information technology services share a common governance and that they are organized and staffed to adequately meet the challenges of the increasingly complex and integrated technology environment.

risk management approach to their support of medical technologies can substantially help clinical engineering and IT make the necessary paradigm shift to more relevant support models.

Stephen Grimes is a Chief Technology Officer with ABM Health, a Boston area based healthcare technology consulting, management and service organization meeting the needs of over 250 clients throughout the U.S. There he specializes in technology management, medical and information technology convergence and integration issues and in medical device security and risk management. Grimes has nearly 35 years experience with hospitals, shared service organizations, and healthcare consulting firms. He is a nationally recognized authority on topics ranging from future challenges facing clinical engineering and healthcare technology integration to medical device security and risk management. He is a frequent speaker and author and serves as a healthcare technology management consultant to the World Health Organization (WHO) and Pan American Health Organization (PAHO). Grimes is a member of the American College of Healthcare Executives (ACHE) and a Fellow Member of the Healthcare Information and Management Systems Society (HIMSS) where he chairs the Medical Device and Patient Safety Task Force. He is also a Fellow of the American Institute of Medical and Biological Engineering (AIMBE) and a Fellow of the American College of Clinical Engineering (ACCE) where he is a Past President. Grimes is a graduate of Purdue University’s Biomedical Engineering Program. Grimes is the 2010 recipient of the joint industry ACCE HIMSS Excellence in Clinical Engineering and Information Technology Synergies Award.

REFERENCES

1. Institute of Medicine. To Err is Human: Building a Safer Health System, Committee on Quality Health Care in America;2000.
7. The Medical Device Market: USA—Opportunities and Challenges, Espicom Business Intelligence, June 2011. Available at: www.espicom.com/Producat2.nsf/Product_ID
12. Ibid. 6,7
Quality healthcare depends on the availability of the right information, to the right people, at the right time to enable them to make the best possible health-related decisions. Lack of complete and accurate information to guide healthcare decision-making has been associated with decreased patient safety and poorer health outcomes, as well as increased resources utilization. Positive health outcomes for chronic medical conditions increase as a result of health status surveillance and coordination of care, activities which are information intense, and performing them successfully depends on effective exchange of data. The World Health Organization acknowledges eHealth as the cost-effective and secure use of information and communications technologies to support health and health-related fields, including healthcare services, health surveillance, health education, knowledge and research. eHealth technology has been categorized as having three main overlapping functions: to enable storage, retrieval and transmission (sharing) of data; to support clinical decision making; and to facilitate remote care. eHealth technology is broadly classified as organizational and/or provider health informatics.

Abstract

Consumer health informatics is an emerging field that offers the ability to enhance the quality and safety of care by leveraging information and communication technologies to place the patient at the center of care. This is particularly true for patients with chronic complex medical conditions and/or from vulnerable populations, including minorities, the elderly and disabled. Uptake and adoption of such technology has been slow. Strategies are needed to assess barriers and develop successful approaches to promote connected health leveraging consumer eHealth technologies, including interoperability with organizational IT systems, for support of patients and their provider teams to optimize care.

Through two case studies and an overview of current evidence and industry trends in personal connected health technologies, this paper will make the case for connected health applications adoption and integration within the healthcare IT ecosystem to support and connect patients and their providers. We will present a model developed by a healthcare system and a software developer for the interoperability of web-based self-care management platforms for seamless 24/7 sharing of personal health information across the continuum of care among the patient, system and non-system providers and organizations which are stakeholders in the US healthcare delivery system.

Keywords

Personal health records, diabetes, spinal cord injury, chronic conditions, mobile devices, connected health.
and consumer health informatics. To date, a large body of publications in this field has focused on organizational electronic health records. Less robust evidence exists on leveraging eHealth technologies for self health management of patients with chronic conditions. This paper will focus on consumer-centric health informatics.

Consumer health informatics is a rapidly evolving field that offers abilities to enhance care quality and safety by leveraging information and communication technologies to enable patients to be at the center of their care. This patient-centric approach to health information management obviates many issues of patient privacy, data property rights and system interoperability that currently challenge provider-to-provider information sharing across and among systems of care. Accordingly, the Office of the National Coordinator for Health Information Technology (ONC) has included a consumer-focused technology, the personal health record (PHR), among its evolving health informatics technology infrastructure portfolio.

A PHR is defined as a standards-based, interoperable, electronic record of an individual's health-related information that is controlled by the individual. Individuals with chronic, complex medical conditions and their family members or custodial caregivers bear the brunt of managing care outside healthcare provider facilities. Diabetes mellitus, hypertension and spinal cord injury may be considered prototypes for the development of management strategies for chronic medical conditions. These disorders share common needs relative to health information sharing typical of the majority of common chronic medical conditions (e.g., comprehensive, up-to-date clinical lists).

Yet each condition also has divergent needs for health information (e.g., data provided by devices which support self-care). The case studies we present leverage one instance of a web-based personal self-care management platform to delineate how consumer eHealth informatics may be used to support diabetes, hypertension and spinal cord injury self-management, including among minorities and the underserved, as illustrative of disorders which require chronic care management. Lessons learned will be presented in the context of a broader overview of the current health IT ecosystem, industry trends and current evidence on usability and the impact of personal health technologies on outcomes to inform developers, clinicians and researchers working in the field of consumer health informatics.

THE TECHNOLOGY PLATFORM

The patient-centered eHealth technology PHR (eHealth2go) used by the patients in our case studies is being deployed in a regional health system in the Mid-Atlantic United States. It is a comprehensive health self-care management platform which is powered by Get Real Consulting’s InstantPHR technology. The platform resides in, and is provided security by, Microsoft HealthVault (HV). When the record is in use, it is pulled down onto a local server where it is accessible to the patient and, with his/her permission, to caregivers and/or providers. No data is stored on the local servers. Use of HV-partnered devices (e.g., blood-glucose meters) to enable data entry to the PHR is encouraged. A prototype companion web-based mobile technology application was made available to the patient presented in Case #2. Platform applications support the three main components of eHealth technology functionality, namely storage, retrieval and sharing of protected health information (PHI), support for self-care management decisions and facilitating remote care. Exhibit 1 lists specific platform functionalities with examples of data which may be relevant to each in the general medical PHR and in the PHR of the diabetes or spinal cord injury patient.

Case studies. Both case studies received approval from the MedStar Health Research Institute Institutional Review Board.

Methods. Patients volunteering to participate in a pilot program evaluating usability, usefulness and uptake of the PHR were supported in setting up their record.

---

![EXHIBIT 1: Consumer eHealth Technology Functionalities](image-url)
Consumer health informatics is a rapidly evolving field that offers ability to enhance care quality and safety by leveraging information and communication technologies to enable patients to be at the center of their care.

Instruction in processes for signing up for an e-mail account if the patient did not already have one, for a HV account and the PHR were provided by a program staff member who served as a health navigator. Patients were guided through the required processes for entering PHI into their PHR. Instruction in how to upload device drivers and to download data from them was provided.

**Case Study 1: Use of a Web-Based PHR in the Diabetes & Cardiovascular Disease Prevention Self-Management Microcosm**

AC, a 62 year old African American male with type-2 diabetes and hypertension (high blood pressure—BP). He was referred to the diabetes clinic of an urban tertiary care hospital for management of uncontrolled high blood glucose (BG) and BP. He expressed frustration at his BG and BP being out of control: “No matter what I do, I do not get better. I feel tired, I have no energy and I feel that I have no control over my own health.”

He had been taking the maximum-recommended doses of two oral diabetes medications, and two additional types of pills, each once daily, for BP management. His hemoglobin A1C, a measure of long-term BG control, was 13 percent, which correlates with an estimated average glucose of 326 mg/dL over the preceding two to three months. This A1C value represents uncontrolled diabetes, falls far short of the American Diabetes Association national Standards of Care target of 7 percent, and is associated with a significant increase in long-term risk for diabetes co-morbidities, including eye, kidney and nerve disease, heart attack and stroke. An average BG in the 300s is well above the ADA clinical targets of 70-130mg/dL before meals and under 180mg/dL after meals. His blood pressure was 188/101mmHg, also well above the ADA standard care goal of 130/80mmHg. He had never received diabetes education, had limited prior experience with computer use and had never used a computer to access health-related information.

AC provided informed consent to participate in a diabetes clinic program which seeks to engage high-risk individuals with uncontrolled diabetes in self-management. A diabetes educator helped him obtain an e-mail address and taught him basics of logging in, navigating the Internet, etc. She also supported him in setting up his PHR and instructed him in use of the applications. An HV supported BG monitoring device was provided, drivers were uploaded to his record and he was instructed in how to download sugar readings from his meter to the PHR. He was also shown how to view diabetes education resources (e.g. the plate method for controlling meal portion sizes by food group) in the PHR, how to print reports and encouraged to take PHI reports to his primary care provider (PCP) visits. This approach reflects the patient-centered, collaborative approach to self-management prescribed in both the chronic Care (Coleman et al., 2009) and the Medical Home Models (Bates & Bitton, 2010). At subsequent visits, special emphasis was placed on looking at BG patterns and BP results and reviewing data points within healthy targets and outside of target ranges for each.

In time, AC felt empowered to have more say in his medical care as he reviewed his PHI displays in the PHR. He changed PCP as he grew to feel that not enough action had been undertaken earlier to help control his conditions. When his new PCP wanted to wait a month before making changes in BP meds, he showed her data from his PHR and a new BP medication was added to his regimen that day. Looking at his BG data displays in the PHR allowed him to see how many were outside of range and really opened his eyes to the relationship between what he ate/drank, his activity levels and his BG readings. Overall, he was able to more clearly see the relationship between diet, exercise and changes in medication on the one hand and his BG and BP values on the other. This led to a greatly enhanced sense of empowerment as he was able to see that his lifestyle behaviors clearly mattered and influenced his overall health and well-being. He made changes to his diet and starting walking regularly. This information was so valuable to him that he would go to a friend’s house regularly to update his PHR, as he did not have a computer at home.

At the end of a three-month period, his diabetes was well controlled, with his A1C having come down to 6.6 percent. His BP control was trending between 130-140/80mmHg and he is working with his
PCP to have further adjustments made to his BP medication regimen. He continues to update his PHR and says he will recommend it to others.

The self-care management platform was successfully adopted as a tool to support eHealth literacy and diabetes and hypertension care by an African American male who had little prior computer experience and did not own a computer. A health navigator provided the required education to enable him to use the platform independently to support self-management and to share PHI with his PCP. This strategy enabled the patient-centered healthcare team to move toward targeted control of AC’s chronic medical conditions.

**Case Study 2: The Utility of a PHR in Health Self-Management for Persons with Physical Disability—Spinal Cord Injury**

ML, a 46-year-old, unemployed, college-educated male with a C5-6 spinal cord injury (SCI), worked with program staff to explore the usefulness of a PHR in helping him manage his health after disability. As is typical for his level of injury, ML is paralyzed and has only limited use of his arms and hands. Numerous chronic medical conditions tend to follow paralysis. In addition to coping with mobility constraints, ML faces the challenge of preventing/managing skin breakdown, bone loss, chronic infections, including recurrent urinary tract infections (UTI), hypertension, obesity and bowel function.

The PHR framework described in Case Study 1 was used as a point of departure for tailoring a PHR for use after SCI. An SCI self-management guide provided a roadmap to help ML create a PHR to meet his specific needs. Like the diabetes educator in Case Study 1, the staff member working with ML provided on-going help and guidance for developing and implementing his PHR.

Data types used by people with SCI to monitor the most common health threats are often more qualitative than quantitative. For example, UTIs are a chronic problem after SCI. Risk is monitored at home through observed changes in urine color, odor, and subtle perceived changes in general well-being since neurologic impairment blocks the pain and sense of urgency that signals urinary problems to persons without SCI. Tracking these subjective warnings of infection doesn’t provide the same clear and quantifiable management pathway as does, for instance, tracking of BG values in diabetes. ML, therefore, chose not to log these data in his PHR although he could have done so. ML was motivated to develop his PHR for the ability it provided him to alert health care providers, particularly in emergency situations, to the needs of his relatively uncommon condition and his specific personal health history. He recounted numerous prior experiences where his health had been compromised because he was too ill to self-advocate and his special needs as a person with SCI went unrecognized. Furthermore, ML takes almost a dozen medications prescribed by a frequently changing group of providers.

He was delighted to find that his PHR and pharmacy interoperated perfectly in the HV ecosystem and that his medication list was continually updated whenever a medication or dosage was modified. ML noted, “What I do now when I have to go to the hospital in an emergency is to ask the EMT tech to put ALL my containers in a bag and bring them with me. This will be so much more efficient!”

ML readily adapted to using his PHR. In contrast to many persons with chronic conditions, particularly those who are elderly, people with SCI have been shown to be receptive to using technology and assistive technology to facilitate computer interaction is a common component of post-injury rehabilitation. ML preferred to navigate his PHR with the speech recognition and touch technology he was accustomed to using on his mobile device (Android). ML reviewed multiple web-based emergency provider applications that interoperated with his PHR, but he did not believe that people helping him in an emergency would have sufficiently easy and unrestricted access to the Internet to retrieve his information promptly. He chose, therefore, to augment his online PHR with an affordable ($20), waterproof USB dog tag device with a warning of his high-risk medical status engraved on the cover and his complete PHR downloaded and saved to the device memory. ML’s desire to maximize the portability of his personal health information for emergency use, in full awareness of a somewhat diminished guarantee of privacy, is consistent with the health information...
access preferences expressed by other persons with physical disabilities.11

Subsequently, ML was indeed transported to the emergency department (ED) to resolve a crisis situation. During this episode, as had been his experience in the past, ML suffered from temporarily diminished capacity and had difficulty communicating his situation to ED staff. The ED doctor took the dog tag PHR from around ML’s neck, inserted it into an ED USB drive and displayed all of ML’s medications, relevant history and “special handling” instructions. “How cool is that!” ML reported the doctor having remarked. ML was promptly admitted to the hospital where his medical problem was appropriately addressed.

DISCUSSION

The broad-ranging potential utility and value of PHRs in both the management of chronic medical conditions and in bridging PHI transmission to the acute-care setting (ED or hospital), which have historically each siloed data, for persons with chronic conditions are highlighted by the case studies presented. While it is beyond the scope of this paper to review all of the body of literature on PHRs, our case studies illustrate some concepts which we feel should be emphasized and will be of interest and importance to developers, providers and researchers working in this space.

The PHR supported each of the three main functionalities delineated for eHealth technology tools. Namely, use of the PHR enabled patients to: store, retrieve and share PHI; support self-care management decisions and facilitated remote care. Considerations in usability, evidence for the impact of PHRs on health outcomes, using diabetes and hypertension which were comorbidities in Case Study 1 as examples, and addressing disparities in the uptake of personal eHealth tools should also be considered in further initiatives which target development and deployment of PHRs.

PHRs and Storage, Retrieval and Sharing of Personal Health Information.

One key function of the PHR is to serve as a life-long resource for an individual’s composite health information drawn from a wide variety of sources.4 Placing PHI under the individual’s own control, as was done by the patients in our case studies, assures that PHI can be made available when and where it is needed for care. We believe that the PHR has the potential to serve as a personal health information exchange.

The most salient sources of PHR health information, according to NAHIT, are records imported from those maintained by healthcare and service providers, individuals’ personal health data from medical devices, information manually generated by individuals for self-management or to alert care providers, and information from insurance providers. Over the past several years, interoperable, standards-based patient connected health platforms (e.g., HV), have become freely available to consumers and providers, and have the potential to be imported through web-based data repositories, such as HV, for storage in the PHR.

Providers can be granted access to view stored PHI when and where it is needed 24/7 as patients move across the continuum of care, and particularly across health care settings that do not share systems. These concepts are illustrated in Exhibit 2.

PHRs will enable movement away from the current paradigm of dependence on memory of PHI to reliable data storage. For example, a reliable medication list is a cornerstone of medical management for chronic conditions. Patients are often asked to list their active medications at care encounters and may do so from memory with varying
degrees of accuracy or may present all of their medications for the provider to sort through and list. The first step in moving to more accurate medications recall is for the patient to keep all of their medications on a paper list. eTechnology moves this list to an electronic format, as shown in Exhibit 3. This concept was clearly useful in Case Study 2 where the patient was taking multiple medications for management of his chronic conditions secondary to SCI. The PHR facilitated keeping an updated list and sharing it with providers.

Information which can be stored and retrieved from the PHR in this way includes lists of data such as demographics, medical conditions, allergies, immunizations and medications; images and reports, for example x-rays, CT and MRI scans, ECGs, consultation records and advanced directives.

PHRS AND SUPPORT FOR SELF-CARE MANAGEMENT DECISIONS

PHRs are more than static repositories for personal health data. By integrating data, knowledge, software tools and education content, PHRs support active patient engagement in better health care and better health. PHRs have also been classified as a health self-management intervention because of the values of patient-centeredness and consumer-empowerment that underlie them. Healthcare frameworks that are characterized by a strong focus on health self-management, notably the Chronic Care Model (CCM) and Medical Home Model, increasingly include PHRs in their paradigms for patient engagement. A survey conducted and published by Lake Research Partners in 2010 demonstrated that people with chronic health conditions, particularly those with multiple health conditions, perceived PHRs as particularly relevant to managing their health.

Consumer eHealth informatics, as exemplified by the PHR, enables informed individuals who are actively engaged in the daily management of their chronic conditions as the “change agents” in a healthcare system which is challenged in meeting the needs of this burgeoning population. The CCM emphasizes the patient-provider relationship and leverages self-management and information technology as key elements to success in achieving mutually agreed upon health outcomes. Self-management is viewed as a collaboration among patients and providers which enables resolution of patient-defined problems, participation in decision making and self-management education focused on development and application of problem-solving skills and self-efficacy. Improved health outcomes are reported when practices implement more than a single component of the CCM. These components can each be supported by PHR functionalities. Additionally, leveraging the role of social media via the PHR platform for freely sharing ideas and experiences with other patients with similar conditions offers a potentially rich benefit to patients managing chronic illness that has yet to be examined systematically.

eDecision support tools enable physicians to implement evidence-based best practices and to attain clinical benchmark indicators for care. In consumer health informatics, the analogous functionality is self-management support. Patients with chronic health conditions are asked to perform tests and record data that will provide information to guide health management. For example, in the care of diabetes, daily fingerstick BG testing provides data that the patient can use to guide adjustments to insulin doses using a methodology known as pattern management.

An example of self-care management functionality in PHRs enabling improvement in behaviors is illustrated in Case 1 where the patient was able to move from handwritten BG logs to a graphic display of his readings. This presentation allowed him to see and understand the relationship between BG patterns and his eating and physical activity behaviors. This concept is illustrated in Exhibit 4. The graphic display of the BG readings is overlaid on a background where the target BG range is shown in green. The tabular display aligns BGs with time of day obtained. These representations allow the patient to readily see BGs which lie outside his/her target range by time of day, facilitating recognizing their
relationship to meals and/or changes in physical activity.

**PHRs to Facilitate Remote Care**

Persons with chronic medical conditions work with their healthcare providers in different ways based on their underlying healthcare needs. Therefore, it is not surprising to observe that the patients whose cases were just presented used their PHRs differently. In the case of AC, the diabetes clinic served as his medical home, introduced him to PHR technology and engaged him in its use. He collected the same information, for example, BG and BP, at home as the clinic or his PCP would collect during visits. Additional data, whether transmitted electronically to his record at the clinic or on paper to his PCP, enhances quality of care by facilitating safe and effective medication adjustments. Further, by becoming more involved and knowledgeable about the management of his diabetes through use of the PHR, the patient became a more effective self-advocate which also contributed to his better health.

Current healthcare systems provide no comparable “SCI Clinic” to help SCI patients manage their health. Consequently, ML was on his own to engage his various providers in the use of his PHR, a tool they were unlikely to have anticipated using in working with him. The SCI patient was concerned primarily with sharing unexpected information with health care providers emergently. The relative frequency with which providers encounter patients with diabetes and the relative rarity of their encounters with patients with SCI also influence priorities of these patients for maintaining data in their PHRs. It would not occur to a person with diabetes to include an explanation of that condition and its implications in the summary data of his/her PHR. That however, is exactly what preoccupies persons with SCI and provides a large part of the motivation they may have for shepherding their own health information.

Managing medication information, central to health maintenance in both diabetes and SCI, is a self-management task that bridges these and other chronic conditions. The American Health Information Community Consumer Empowerment Workgroup flagged interoperability of medication information as essential to the broad adoption of PHRs. Subsequently, a standardized medication profile became the priority and principal deliverable of the ONC Workgroup. It should not escape notice that the most efficient exchange of data ML was able to carry out in his PHR was the automated updating of his pharmacy data. In the case of both AC and ML, however, the pivotal central position of the patient to his own care was the factor that bridged information exchange between human beings and information systems.

PHR technical architecture may be designed for web-based and/or mobile platforms which can be, and increasingly are interoperable with a wide variety of eHealth platforms, including organizational eHealth technology platforms (i.e., EMRs and patient portals). This evolution positions PHRs to play an important role in facilitating sharing of key PHI across the spectrum of care among patients and providers to support care.

**Considerations in Usability and Usefulness**

One of the most prominent barriers to successful implementation of Meaningful Use of health IT are systems with poor usability (specific to the interface design), and systems which are not useful to the intended user groups. The former (usability) results in confusing and hard to use systems, and the latter (usefulness) results in a lack of motivation to use the system. Although IT designers often attribute the low usage rates to “slow uptake” or “lack of knowledge that the system exists” the real reason likely resides in the lack of usability and usefulness of the system.

In a recent systematic review and evaluation of web-accessible tools for management of diabetes and CVD risk factors, Yu, et. al reviewed 57 studies, of 12,626 citations, which met the criteria that they provided education or assessed outcomes. Usefulness, sustainability and usability were evaluated. Tools for mobile devices were excluded. Methodological quality and ratings for clinical utility and sustainability were variable and there was a high preva-
We envision a near future when all Americans ... will have a patient-centered web-based PHR which fully leverages, and allows seamless transfer of PHI among, organization/provider and consumer eHealth informatics platforms and will serve as the center of a personalized health information exchange.

Evidence of usability errors. Only six percent of tools were free of usability errors and fully 60 percent had three or more errors. Common usability errors included limited usage of visual elements to facilitate learning and lack of intuitiveness in navigation and expected next steps.24 Greater improvements in patient outcomes were seen with greater use of the tool and other intervention characteristics which enhanced use were peer or counselor support, email or phone contact and updates regarding the tool. Lack of intuitiveness in navigation was evidenced in our first case study, where the patient required significant support from a health navigator to sign up for and set up his own PHR. This observation and the high prevalence of usability errors in the Yu meta-analysis support the premise that eHealth technology tools, certainly in their present state of development, cannot be successfully deployed without involvement of a human element (i.e., support by a health navigator who can train the patient to fully leverage the platform to support self-management and outcomes). High prevalence of usability errors highlights the need to ensure that to provide useful and usable formats, eHealth technology tools should undergo usability testing prior to release to the public. This analysis highlights how human factors professionals can assist the healthcare community by lending their expertise on designing, assessing and implementing people-centered systems.

Evidence for the Impact of PHRs on Health Outcomes.

There is a small, but growing body of evidence demonstrating clinical impact of PHRs as tools in chronic diseases management. Several of these reports focus on diabetes, again as a prototype chronic medical condition that requires a high level of patient engagement in self-management to enable improvement in blood glucose control, as was seen in the patient in Case Study 1. Pre-visit use of online PHRs linked to an EMR increased rates of DM-related medication adjustment from 15 percent to 53 percent, p<0.001, compared with active controls.25 In a recent report the WellDoc DiabetesManager®, a care management system which provides mobile application coaching and patient/provider web has reported outcomes for a cluster-randomized clinical trial conducted in 26 primary care practices where 39 physicians participated and 163 patients were enrolled and included in the analyses. A 1.2 percent greater reduction in A1C, p<0.0001 was seen in the maximal care intervention group when compared to controls receiving standard care alone. Maximal care patients received a patient-coaching system and provider clinical decision support.26 The patient in Case Study 1 also had hypertension. Kaiser Permanente has generated evidence in a 6-month randomized, controlled trial among 348 subjects with uncontrolled hypertension that an intervention incorporating a PHR can significantly impact BP control. Usual care was compared to an intervention using the American Heart Association’s “Heart 360” PHR platform, BP device and instruction; alerts to patient and provider; and a PharmD who adjusted BP medications using communication via e-mail and/or phone. Intervention participants had an absolute reduction systolic BP that was -11mmHg greater than in controls and were 50 percent more likely to have SBP at goal at the end of six months.27 Each of these studies deployed a combination of strategies for leveraging technology to enhance provider interactions. Further studies are clearly needed to generate rigorous data which will define strategies for best practices around the design and deployment of PHRs.

Addressing Disparities in Uptake of Personal eHealth Technology Tools.

Evidence suggests that for certain groups the Internet is already playing a significant role in individual healthcare empowerment.18 Unfortunately, the adoption of technologies, specifically with minority and vulnerable populations, including the elderly and those with low income, are not at the levels one would hope.28 Interest is growing in understanding the potential role of health IT in addressing healthcare disparities among these high-risk groups. With Health IT leaning in the direction of connected health, those who receive their care through the public health system and/or those with or at risk for chronic diseases can be supported in embracing the digital age of healthcare in a mean-
A1C than controls.31 These reports provide evidence that minority and underserved patients can be successfully engaged in the use of self-care management technology to improve diabetes outcomes. Further studies area also needed in this area.

**CONCLUSIONS AND OVERARCHING THEMES**

Efforts by developers, clinicians and researchers to improve usability and usefulness and reduce disparities in uptake and adoption, and further studies to provide evidence for best practices for the design and deployment of PHRs will be prerequisites to their ubiquitous dissemination and use.

Pillars to Connected Health success, as illustrated in these case studies, will revolve around four areas of focus. First one must create meaningful patient experiences in which content will be personalized and relevant to the individual's health experiences, be controlled by the patient, and result in simple yet effective experiences. Second, reliable clinical data is absolutely necessary for safe and effective health management. Data entry must be automated whenever possible lessening dependence on the patient to manually enter PHI. Integration with other technologies which generate and/or store data, like medical devices, EMRs and web-accessible repositories of health information will facilitate data entry automation. The third area is promotion of collaboration with and among healthcare providers and caregivers. This requires arming providers, patients and/or caregivers with timely and appropriate alerts and reminders which are generated by the technology platform and creation of electronic venues for collaboration. This will also create opportunities for research and quality improvement initiatives leveraging PHR technology.

Finally, it is important to meet individual eHealth technology users in the space where they live and feel comfortable. In this regard, mobile health technology, or mHealth is here to stay and should be embraced. Meeting patients on common ground may best be accomplished by focusing on what have to-date been considered non-traditional methods of care delivery, including a pivotal role for personal health technology in engaging the patient as a change agent in his/her health care.

Michelle Magee, MD, Associate Professor of Medicine, Georgetown University School of Medicine, serves the MedStar Health Diabetes, Research and Innovation Institutes as a clinician, educator and health services researcher.

Cortney Nicolato, CPHIT, currently serves as Vice President of Healthcare Strategies for Get Real Consulting, a vanguard in the Health IT/connected health community. She also sits on the HIMSS Personal Health Information Technologies Workgroup.

Manon Maitland Schladen, MSE PMP EdS, is a senior researcher at MedStar Health Research Institute. She co-directs consumer training for federally-funded spinal cord injury projects.
FEATURE: CONSUMER HEALTH INFORMATICS

REFERENCES


5. American Diabetes Association Standards of Medical Care in Diabetes-2012 Diabetes Care; 35(S1): S1-63.


Electronic Patient Plan of Care

Nursing Care Coordination and Patient Care Transitions in Electronic Medical Records

By Luann Whittenburg, PhD, RN

ABSTRACT

This paper discusses the new healthcare environment of rewarding patient care quality in organizations that devote attention to outcomes measures and improvement. Since 2004, federal health policy has promoted delivery performance changes to obtain patient care value and quality transparency. The Patient Protection and Affordable Care Act (Pub. L. 111–148) was enacted on March 23, 2010, to improve the health of individuals, families and communities (HHS, 2004). Nursing is moving from task-oriented documentation in electronic medical record (EMR) systems to a patient plan of care model. Electronic nursing documentation systems are focusing on patient plan of care documentation to monitor and track the progress of patient care. The aim of this paper is to describe a replicable method to examine EMR nomenclatures and lexicons using the structured nursing concepts in the Clinical Care Classification (CCC) system to support nursing outcomes measurement and quality transparency in health systems.

KEYWORDS

Patient plan of care, electronic medical record, EMR, nursing documentation, quality, outcome measures, structured nursing data, ISO, CCC.

THE EMR, with data centered on the patient and delivered electronically, is a communication method that involves coordinated physician and nurse processes to describe and document patient care delivery and transitions of care. The use of the EMR has impacted medical error rates, test and treatment decisions to avoid duplication and patient care variations.4,5,43

“Armed with data points from the point of care, nurse informaticians and chief nursing officers, will be able to quantify, for the very first time, the value of nursing’s contribution to the quality of patient care in America.”49

BACKGROUND

The aim of the Patient Protection and Affordable Care Act (ACA) is to increase the value of healthcare to patients and society. This new national health environment rewards value and quality, devotes greater attention to outcomes measurement, with outcomes improvement essential to the success of providers and organizations across the healthcare industry.

Nurses invest a great deal of professional time and effort to document interventions, actions, advocacy and decisions;
yet, what a nurse documents is rarely being used to advance nursing research or practice. Florence Nightingale understood the importance of nursing documentation as the foundation of care. Nurses are responsible for patient care 24 hours a day, seven days per week, 365 days a year and “spend a great deal of time managing and documenting patient information.” Time spent by nurses gathering, coordinating and documenting patient information can be as high as 50 percent of nursing hours. And, while a patient’s medical record may reflect medical problems; nursing documentation of the care delivered and the many patient actions performed by the nurse are typically never recorded. There is a critical need to leverage nursing documentation to study nursing practice and outcomes and without electronic standardized, coded

Structured data is the first step in the implementation of an EMR clinical decision process required to promote evidence-based practice in nursing; for without structured data, there is a duplication of information and a decline in data interoperability for internal and external exchange. Without standardized data, hospital costs could increase with an accompanying loss of critical patient care information needed for longitudinal studies, clinical trials, population health surveillance, disease management intervention and the prevention of patient illness. Nursing documentation were documentation models of nursing concepts from the CCC moves nursing away from nursing terminology standard, the CCC system

NURSING PRACTICE
The impact of EMRs on nursing documentation has been seen in documentation fields. In EMR documentation, when an appropriate nursing concept was missing, nurses had the opt-out option of free-text data entry. Often the configuration of an EMR limited nursing documentation rather than providing the means to document structured nursing interventions and practice. Essentially, the EMR format determined the collection of nursing information. An EMR designed with pre-coordinated questions (task lists) with mandatory fields that must be answered often produce data that appeared “normal” or “without problems.”

NURSING DOCUMENTATION
Today, the importance of including patient preferences in decisions regarding care is increasingly supported by all professions and pre-coordinated task lists lack flexibility for this new healthcare environment. Traditionally, healthcare organizations expected EMR vendors to provide nursing content. Therefore, nursing data was often represented using different terminologies. Often EMR nursing content (nomenclature and lexicon) were developed by nurses employed by the organization and were based on evidence-based guidelines in the nursing literature. This EMR nursing content frequently appeared as templates for documentation that was not editable. The nursing templates were used to structure the EMR content for each nursing care documentation entry. These EMR templates used for nursing care documentation were documentation models concentrating on specific EMR content (i.e., a meta-model). In each template, the pertinent information to document was provided by displaying specific data elements in pick-list or list box. A pick-list is a list of template data elements displayed in a data window. A data window is a system interface on the display screen that accepts device input from a mouse or trackball that allows the nurse to select a data element or object on the screen. A list box is similar to a drop-down list. The list box displays or drops down data elements for the nurse to select. Once a data element is selected, the list box converts to an inactive state and displays only the selected value.

NURSING CARE PLAN
Hardiker, Bakken, Casey and Hoy view nursing terminology as being designed to communicate information about patients, families and groups and as a means to support the acceleration of improvements in U.S. healthcare quality. Nursing terminology does more than communicate information on the patient’s status, care and condition; nursing terminology also exchanges data about the care nurses provide using the nursing process: assessment, diagnosis, outcome identification, planning, implementation and evaluation.

In 2007, the selection of a national nursing terminology standard, the CCC system was the beginning of the move to patient plans of care documentation for care coordination and care transitions. The EMR is needed to support the continuous and efficient shared understanding of a patient’s care history that simultaneously aids interdisciplinary communication and decision-making about the future care of patients. The EMR may have multiple purposes within an organization, such as fulfilling legal documentation requirements, accreditation, accountability and financial billing; whereas the primary function of nursing documentation is to communicate continuity and quality outcomes are visible and nursing research has a source of information about patient care outcomes.

According to Hammond et al, 2010, “If data collection is structured around the data needs of the community collecting the data, there is an incentive for timeliness and accuracy. If the nurse understands the
Nurses invest a great deal of professional time and effort to document interventions, actions, advocacy and decisions; yet, what a nurse documents is rarely being used to advance nursing research or practice.

importance of the data and how data will be used, collecting and entering accurately and completely becomes important. Z3

CIMINO: IDEAL TERMINOLOGY CHARACTERISTICS

Researchers have identified the ideal characteristics of a terminology system for the structured data capture, storage, analysis and reporting in a health information system. The characteristics are: “domain completeness, granularity, parsimony, synonymy, non-ambiguity, non-redundancy, clinical utility, multiple axes, and combinatorial.” Zielsorff recommends terminologies have uniqueness and context-free identifier (i.e., each term must have a definition, be arranged hierarchically with the ability to map terms to other standard classifications).

The CCC is a free, public domain, unified, poly-hierarchical nursing terminology of atomic-level concepts following the nursing process of nursing diagnoses, interventions and nursing outcomes. The use of the CCC system for the classification of nursing knowledge in standardized nursing concepts allows nurses to systematically construct a common document for the communication of the nursing diagnoses of patients, nursing interventions performed and to communicate the resulting nursing care outcomes. With standardized, coded nursing concepts, nurses are able to determine which nursing interventions work best for a given patient population. As the nursing profession systematically collects electronic information about nursing care, the profession gains evidence-based practice data to identify those clusters of nursing interventions that typically occur together for certain types of patients. This information may be useful in determining the cost of nursing services, planning for nursing resource allocation and constructing critical paths and plans of care.33

CLINICAL CARE CLASSIFICATION SYSTEM

The CCC system was developed by Saba and colleagues from nursing research at the Georgetown University School of Nursing. The project was initially called the Home Care Project research project (1988-1991). The research was funded by the Health Care Financing Agency (HCFA), now the Center for Medicare and Medicaid Services (CMS). The purpose of the research was to develop a method of predicting nursing resource needs and measure outcomes of nursing care.46

The CCC research team consisted of home health experts, a statistician, a systems analyst and a national advisory committee. Saba and colleagues conducted a pilot study, designed a framework and established a methodology. The study methodology was applied to a national sample of home health agencies (HHAs) that provided all services and products used to restore, maintain and promote physical, mental and emotional health to Medicare home health patients.51

GOVERNMENT-FUNDED RESEARCH

The CCC system was developed from retrospective research data from 8,967 patient records from a sample of 646 HHAs randomly stratified by staff size, type of ownership, and geographic location. The HHAs represented every state in the nation, including Puerto Rico and the District of Columbia. The CCC system is a nursing terminology of discrete atomic-level data elements that encompasses nursing diagnoses, interventions and outcomes capturing the essence of patient care in all healthcare settings.

The CCC system describes the six steps/standards of the | assessment, diagnoses, outcomes identification, planning, implementation and evaluation in a coded, standardized framework to support the exchange of nursing information and makes available for data retrieval and analysis the contribution of nursing care to patient outcomes for improved healthcare services and nursing visibility in the EMR database.

The CCC system describes nursing practice in a coding structure designed for retrieving data from computer information systems. Saba explains that “the CCC System uses a five-character structure to code the two terminologies: (1) CCC of Nursing Diagnoses and Outcomes and (2) CCC of Nursing Interventions and Actions. The CCC coding structure is paced on the format of the International Statistical Classification of Diseases and Related Health Problems: Tenth Revision; Volume 1, WHO, 1992. The coding strategy for each terminology consists of the following:

- First position: One alphabetic character code for Care Component (A to U);
- Second and Third positions: Two-digit code for a Core Concept (major category) followed by a decimal point;
- Fourth position: One-digit code for a subcategory, if available, followed by a decimal point;
- Fifth position: One-digit code for:
  - One of three Expected or Actual Outcomes and/or;
  - One of four Nursing Intervention Action Types.”
NURSING CONCEPTS

The use of standardized, coded concepts is an important framework for patient care documentation. Standardized, coded terminology to improve documentation systems using the nursing process is important for the visibility of the nursing profession.

Standardized, coded nursing concepts are a set of agreed upon symbols (numeric or alphanumeric) used in representing concepts to allow the exchange of terms in an understandable and agreed upon manner. The CCC system uses a standardized framework consisting of 21 Care Components for classifying two interrelated terminologies: 1) the CCC System Nursing Diagnoses and Outcomes; and 2) the CCC of Nursing Interventions and Actions. Nursing actions known in the CCC system as nursing intervention action types are modifiers that “focus on the specific action needed to carry out nursing interventions. The action types provide the measures used to determine status of the care process and provide the evidence for clinical decision making.”

Berman, et al. defines nursing actions as an action a nurse performs to achieve client goals. The four CCC intervention action types are:

Assess: “Actions to collect and analyze data on health status” and “refers to evaluating the presenting problem/condition—signs and symptoms—at the time of the examination of patient.”

Perform: “Actions to perform hands-on-care-treatments, interventions, services, activities and/or procedures to patient.”

Teach: “Action that refers to educating or instructing- the patient and/or caregiver” and “provide knowledge and skill.”

Manage: “Actions that refer to managing care—indirect actions on-behalf-of-the patient and/or caregiver.”

CLINICAL REQUIREMENT

The conceptual framework for nursing documentation is the American Nurses Association (ANA) Nursing Process. The standardized, coded nursing intervention and action type concepts of the CCC system share the ANA philosophy that nursing care uses a “common thread uniting different types of nurses who work in various areas of nursing practice is the nursing process—the essential core of practice for the registered nurse to deliver holistic, patient-focused care.” This common thread is the nursing process which is based on the natural science principle that humans have needs and that the satisfaction of needs is a central motive for human existence.

The ANA nursing process framework is based on the human existence “needs theory” adapted for nursing and nursing research. The nursing needs theory was first articulated in 1978 by Yura and Walsh. The nursing process is the total of nursing activities including assessment (identifying human needs), intervention (administering to human needs) and evaluation (validating the effectiveness of the help given). Yura and Walsh (1978; 1983), at the Catholic University of America, Washington DC, reflected that human needs result from internal tension and organized the ANA nursing practice framework on the assumption that all basic human needs are relevant to nursing and would be similar across all areas of nursing.

The matching of standardized, coded nursing concepts for the coordination of nursing care has been discussed in the literature since early 1990.

The exchange of EMR nursing documentation during any patient care transfer or transition from one healthcare practice setting to another is challenging between or across systems. Reusing the data enables data interoperability and standardization and simplifies the administrative burden of data collection. Facilitating the automation between various coding systems used in healthcare reduces the costs of providing care and improves the quality of the data and the timeliness (availability) (ISO, 2010). Many patients with complex medical histories have multiple diagnoses, medications, allergies and healthcare providers across numerous practice settings. The use of the national nursing terminology standard, the CCC system, as an integrator for the exchange of nursing data and documentation supports the mandate of the regulatory and accrediting organizations to reconcile patient-centric information during every transfer of care, discharge or admission. The CCC also supports CMS data quality, transparency and integrity criteria for meaningful use reconciliation when patient-centric data is exchanged across system boundaries for patient care coordination and healthcare quality by using the nurse process recognized for professional nursing.

The partnership of nursing and technology is vital for designing nursing practice environments. A nursing terminology standard that identifies each of the six steps of the nursing process for a patient plan of care exchange between and among EMRs supports the transitions of care based on professional nursing requirements. The exchange of EMR data using the nursing process facilitates the provision of patient-centric care for the entire healthcare team. A unified system of nursing data represented by following the Nursing Process presents professional decision-making that is available to reduce costly healthcare duplication and contribute to patient care outcomes and may assist in avoiding the medical errors that cost thousands of lives each year (IOM, 2001).

A recent study (Postpartum Nursing Records: Utility of the Clinical Care Classification System, n.d.) revealed EMR nursing documentation fields focused 48 percent of data elements on the CCC Action Type: Perform with 10 percent of EMR variables addressing the nursing documentation of patient education/teaching; and 4 percent addressing patient care management or indirect patient care actions. The study concluded an EMR was unable to currently fully describe the complexity of nursing care without the inclusion of a standardized, coded, nursing terminology that follows the nursing process containing all the required data elements of effective and professional nursing practice.

REPLICABLE METHOD TO EXAMINE EMR NOMENCLATURES AND LEXICONS

Several researchers describe content analysis as involving interconnected processes: 1) identifying the specific characteristic of the concepts to be measured, (i.e., the content analysis unit) and 2) applying explicit rules for the identification, coding
and documentation of concept characteristics. The replicable method to complete the interconnected processes for the use and reuse of data between EMR nursing documentation elements and the nursing concepts of the CCC system for the examination of EMR nomenclatures and lexicons is described in ISO Technical Report: 12300 (ISO, 2010) with the content analysis unit the EMR template. A deductive content analysis process is applied when the concepts to be described are pre-established.40 The deductive method also allows the investigator to describe the degree of consistency between EMR nursing intervention documentation fields/templates and the nursing concepts of the CCC System. The use of a “degrees of equivalence” scale as addressed in the ISO report is the key to establishing such replicable method to associate the nursing intervention concepts in the EMR with the CCC System though a level of meaning (ISO). The EMR words/phrases identified by action verbs should also include “linguistic variation”7 such as synonyms of CCC Action Type modifiers: (a) assess; (b) perform; (c) teach; and (d) manage. The ISO report allows various data to be compared and linked to support data information exchanges and reuse between EMRs. The ISO report result would be replicable maps (matched relationships) between two documentation systems (EMR and CCC) that define the cardinality and degree of equivalence between the concepts and the rules used to enable the matching of the documentation (ISO, 2010).

The ISO report also provides guidance for healthcare organizations charged with creating or applying mappings for clinical requirements. The ISO report identifies issues and discusses the potential in and the limitations of applying conceptual maps. The ISO report establishes and harmonizes the basic principles for developing, maintaining and using mappings and provides the needed guidelines for good practice.

**CONCLUSION**

Quality improvement expectations have been placed on EMRs to promote Since 2004, federal policy has been to promote improvements in health delivery performance and increase transparency in the quality of healthcare delivered in the United States. After a decade, and with approximately 35 percent of healthcare facilities now using an EMR, nursing has discovered the EMR is does not likely mirror the traditional medical record53-55 and that coded, structured nursing documentation with a nursing process framework is needed to exchange nursing data to add transparency to nursing’s contribution to patient care continuity and quality outcomes. The ISO report and the CCC system each supports the implementation of the patient plan of care model for the exchange of nursing between and among EMRs. The use of structured nursing data increases the value, quality and transparency of healthcare to individuals, families and communities by relying on the patient plan of care for care coordination and transitions.

This article discussed the current healthcare environment of rewarding patient care quality in organizations that devote attention to outcomes measures and improvement and described a replicable method to examine EMR nomenclatures and lexicons using the structured nursing concepts of the CCC system. The examination of EMR nomenclatures and lexicons using the methodology described in ISO report provides the replicable method to examine nursing concept consistency between EMR templates for nursing documentation. The EMR, with data centered on the patient, is a communication process that involves coordinated physician and nurse activities. The importance of outcomes measures is increasingly supported by all health professions with patient plans of care the first step for nursing in evidence-based practice to accelerate the attainment of healthcare value and quality transparency.

**REFERENCES**

ABOUT JHIM
The Journal of Healthcare Information Management (JHIM) is the quarterly peer-reviewed digital journal published by HIMSS, and is devoted to healthcare information and management systems.

READERSHIP AND CIRCULATION
Our circulation is about 30,000. Our primary audience includes healthcare professionals in hospitals, corporate healthcare systems, clinical practice groups, vendor organizations, healthcare consulting firms and government settings. JHIM is indexed by the American Hospital Association’s Hospital Literature Index and the National Library of Medicine’s online bibliographic database, Health.

ABSTRACT SUBMISSION GUIDELINES
Abstract proposals must include a single-spaced abstract (no more than 250 words) and a complete list of authors and contact information. Send abstracts to Matt Schlossberg, Manager (mschlossberg@himss.org).

ACCEPTABLE MANUSCRIPTS
JHIM seeks articles in the following formats:
- **Market analysis:** Articles defining the state of the field, or its various components, and identifying information and management system needs.
- **Technology overview:** Articles surveying and defining the key enabling technologies and/or business methodologies for the industry or its components, formulas for budgeting and/or needs assessment.
- **Case studies:** Articles explaining who, what, when, how and why of a problem or challenge, and how it was solved or solution proposal. These include consumer-focused case studies. “Marketing” articles are unacceptable. Products names are allotted a single mention. We strongly suggest that articles be co-authored by the provider and vendor.
- **Pilot studies and university studies:** Articles should follow the general format for a scientific article: Introduction, methods, results and comments.
- **Reviews:** In-depth reviews or surveys of a book or resource to further readers’ understanding of the field.

Send articles to Matt Schlossberg, Manager (mschlossberg@himss.org).

MANUSCRIPT SUBMISSION GUIDELINES

**Length:**
- **Articles:** 3,000-5,000 words
- **Columns:** 1,000-1,500 words

**Format:**
- Single-spaced, single-column format, with ragged right body text.

**Layout:**
- Opening page will include title and bylines. Articles MUST include the abstract and six to 10 keywords.
- DO NOT include headers or footers in article. Do not include page breaks or numbering.
- Footnotes and references should NOT be formatted. To indicate a footnote within the body of text use a standard unformatted number inside brackets. (Exp. [1]). Use AMA style for references.
- Major headings should be in CAPITAL LETTERS, flush left within the column.
- DO NOT include any graphics, illustrations, figures or tables in the body of the article. All graphics must be submitted in separate documents.
- Author biographies are limited to 30 words and should appear at the end of text.
- Caption text for each figure and graph MUST appear at the end of the article.

**Figures/Graphs/Charts:**
- Articles are limited to three figures, graphs and charts.
- Do not create graphics (tables, figures, charts, graphs, illustrations) in a word processing program.
- Graphics MAY NOT be included within the text of an article. They must be submitted in native file formats.
- Graphical files must be a minimum resolution of 300 dpi and submitted in native file formats. Vector-EPS extensions are strongly preferred. Tables should be as Microsoft Excel documents. PowerPoint presentations, PDF and Web-based (.gif) extensions are UNACCEPTABLE.
- Assign a title and/or figure number to each graphic in the extension. DO NOT include title within body of graphic.
- Label x and y axis of every graph.
- Distinguish bars or pie chart sections by pattern, not color.

**Style and Presentation:**
- Use standard spelling, style, reference, and grammar guides such as Webster’s New Collegiate Dictionary, the American Medical Association Manual of Style and The Elements of Style.
- Use active sentences and be specific. Back up generalities with examples. Avoid jargon.
- All articles will be copy edited and, where necessary, rewritten. The process by which authors may review and approve changes is defined in the letter of agreement.

JHIM 2013 EDITORIAL CALENDAR

**WINTER 2013**
Preparing for ICD-10
Abstract Due: CLOSED
Manuscripts Due: August 23, 2012

**SPRING 2013**
Integration and Interoperability
Abstract Due: October 17, 2012
Manuscripts Due: November 26, 2012

**SUMMER 2013**
Clinical and Business Intelligence
Abstract Due: January 4, 2013
Manuscripts Due: February 18, 2013

**FALL 2013**
Mobile Health Technology
Abstract Due: March 28, 2013
Manuscripts Due: April 19, 2013
Congratulations to the following individuals who have recently achieved the Certified Professional in Healthcare Information and Management Systems (CPHIMS) credential from November 1, 2011 through May 31, 2012. CPHIMS is dedicated to enhancing and promoting the healthcare information and management systems profession by providing the premier credential in the industry. CPHIMS accomplishes this mission by establishing standards for professional practice; creating a fair, valid, and reliable examination process by which professionals can demonstrate their knowledge and skill; granting certification to those who meet the program’s standards; and communicating the value of the credential to consumers and other key constituencies.

- Ramana Adibhatla, MSc, MBA, PMP, CPHIMS – Horshoeheads, N.Y.
- John Marc Alban, CPHIMS – Advocate Health Care – Chicago, Ill.
- Sarah Almadchin, MS, CPHIMS – University of Pittsburgh – Pittsburgh, Pa.
- Manoj V. Alsi, CPHIMS – Saint Francis Hospital & Medical Center – Hartford, Conn.
- Jeanne Anderson, CPHIMS – Blessing Health System – Quincy, Ill.
- Susan T. Anderson, CPHIMS – Government of Alberta – Edmonton, Alberta, Canada
- Davis R. Austria, RN-BC, MS, PMP, CPHIMS – New York University – New York, N.Y.
- William John Bailey II, CPHIMS – Columbus, N.J.
- Seth Baker, CPHIMS – Hartford Hospital – Hartford, Conn.
- Kevin Malcolm Baldwin, CPHIMS – UCLA – Los Angeles, Calif.
- Rao Bandla, PMP, CPHIMS – Bandia Project Consultants – Delta, British Columbia, Canada
- Ellen Batch, BSN, CPHIMS – Texas Health Resources – Plano, Texas
- Christopher L. Becker, CPHIMS – WHTEC – Elbe, Wis.
- Gary Bellamy, RHA, CPHIMS – CareTech Solutions – Mount Pleasant, S.C.
- Anne Margaret Bobb, RPh, CPHIMS – Children’s Memorial Hospital – Chicago, Ill.
- Collin Boetger, CPHIMS – Fujitsu – Rocky River, Ohio
- Barbara A. Borrowman, CPHIMS – VMware – Inver Grove Heights, Minn.
- Cheryl Bowman, CPHIMS – UW Health – Madison, Wis.
- Cyril Braude, CPHIMS – Toronto, Ontario, Canada
- Dwight Brown, MA, CPHIMS – Mayo Clinic – Rochester, Minn.
- Sepideh Browning, ILT, MHA, PMP, CPHIMS – Grayson, Ga.
- Christine Bullerick, MS, CPHIMS – SSM Health Care – Saint Louis, Mo.
- Robert C. Campbell, RN, MSN, CPHIMS – US Army – San Antonio, Texas
- Jerome Canete, MD, CPHIMS – Burnaby, British Columbia, Canada
- Jennifer Carpenter, RN, CPHIMS – University Hospitals – Shaker Heights, Ohio
- Jim Casselt, CPHIMS – HSM – Saint Paul, Minn.
- Kathleen Grace Charters, CPHIMS – Columbia, Md.
- Muhammad Chebi, CPHIMS – Somerset, N.J.
- Melissa Cherry, CPHIMS – Navy Medicine – Schertz, Texas
- Poo Ling ‘Pauline’ Chua, CPHIMS – Vancouver, B.C., Canada
- Karen Clark, MBA, CPHIMS – OrthoTennessee – Knoxville, Tenn.
- Patrick Correia, CPHIMS – NYSTEC – Albany, N.Y.
- Catherine Cosby, CPHIMS – Adventist Health System – Lake Mary, Fla.
- Claudio Costa, MD, MSc, CPHIMS – Sao Paulo, Brazil
- Todd B. Cutick, MS, CPHIMS – Cutick Analytics – Silver Spring, Md.
- Mara Lynn Daiker, CPHIMS – CPHIMS – Columbia St. Mary’s – Wauwatosa, Wis.
- William John Bailey II, CPHIMS – Columbus, N.J.
- Davis R. Austria, RN-BC, MS, PMP, CPHIMS – New York University – New York, N.Y.
- Tony Aufenkamp, CPHIMS – Florida Hospital – Orlando, Fla.
- Tarek Emara, CPHIMS – IBM Canada – Markham, Ontario, Canada
- Colleen Ennett, CPHIMS – Philips – White Plains, N.Y.
- Kevin Estoff, CPHIMS – Lakeland Regional Medical Center – Lakeland, Fla.
- Benjamin D. Exley, MBA, MHA, CPHIMS – Evansville, Wis.

(continued on next page)
Congratulations CPHIMs!

- Marshall Ferguson, MBA, CPHIMs – Avanade – Austin, Texas
- Donna Ann Fitzpatrick, RN, BSN, CPHIMs – Pawtucket, R.I.
- Marc Flower, BSME, CPHIMs – Atlanta, Ga.
- Pamela Foyster, MBA, BSN, CPHIMs – Quality Health Network – Grand Junction, Colo.
- Andrew W. Fraser, Jr., CPHIMs – Knoxville, Tenn.
- Casie Frazier, CPHIMs-CA – Whitby, Ontario, Canada
- Dan Galles, MBA, CPA, CPHIMs, FACHE – Prime Healthcare Services – Reno, Nev.
- Ross John Gardiner, PMP, CPHIMs – Abu Dhabi, United Arab Emirates
- Kathleen Ann Geier, CPHIMs – Mendota Heights, Minn.
- Bobby Geohegan, CPHIMs-CA – Toronto East General Hospital – Toronto, Ontario, Canada
- Larry Gilbert, CPHIMs – Vermont Information Technology Leaders – Montpelier, Vt.
- Jennifer Gillett, CPHIMs – Ottawa, Ontario, Canada
- Cynthia Gingrich, MSIS, CPHIMs – Arcadia, Mich.
- Charles G. Groux, CPHIMs – Advocate Health Care – Oak Brook, Ill.
- Gregory E. Gomer, Capt, MA, MBA, CPHIMs – Chicago City, Minn.
- Andrew R. Goodwin, CPHIMs – Georgia Hospital Association – Marietta, Ga.
- Gilroy G. Gottiango, CPHIMs – US Army – Carlswolm, Md.
- Amin Goyal, CPHIMs – Zenser Technologies – San Jose, Calif.
- Andrea Gray, CPHIMs – Dalera Consulting – Kansas City, Mo.
- Alan Haakenson, CPHIMs – Oakville, Ontario, Canada
- Nona Hall, CPHIMs – Roswell, Va.
- Simon Hall, CPHIMs – Victoria, British Columbia, Canada
- Jeffrey M. Hammen, PMP, CPHIMs – Roswell, Ga.
- William Charles Hammond, CPHIMs – Memorial Sloan-Kettering Cancer Center – New York, N.Y.
- David Harvey, MBA, PMP, CPHIMs – Pembrooke Pines, Fla.
- Craig Harrington, CPHIMs – Dallas, Texas
- Arthur W. Harvey II, MS, CPHIMs – Boston Medical Center – Boston, Mass.
- Jenny Hatlen, MS, CPHIMs – Mercy Health Systems – Janesville, Wis.
- Carolyn Morgan Hayden, MBA, CPHIMs – AmeHealth Mercy – Swarthmore, Pa.
- Erica He, CPHIMs – Toronto, Ontario, Canada
- Donna M. Heathcock, CPHIMs – WellStar Health System – Atlanta, Ga.
- Martin Hodges, CPHIMs-CA – Toronto, Ontario, Canada
- Janine Hofmeister, PMP, CPHIMs – Harris Corporation – Melbourne, Fla.
- Joanna Mary Holt, CPHIMs – Abu Dhabi, United Arab Emirates
- Jennifer Hope, CPHIMs – Etoibike, Ontario, Canada
- Kent Hopkins, MBA, PMP, CPHIMs – Catholic Health Initiatives – Cedar Hills, Utah
- Robert Horst, MBA, CPHIMs – Audacious Inquiry – Caronsville, Md.
- Terry Huu, CPHIMs – Toronto, Ontario, Canada
- Trip E. Humphrey III, CPHIMs – Bon Secours Health System – Richmond, Va.
- Charles Hampton Huntley, CPHIMs – Appalachian Regional Healthcare System – Boone, N.C.
- Sarah Hutchison, CPHIMs-CA – Toronto, Ontario, Canada
- Junjie Javier Inocencio, Capt, CISP, CPHIMs – Army Medicine – San Antonio, Texas
- Andrew Insellmann, MSS, CPHIMs – Andrews Air Force Base – Washington D.C.
- Henry L. Jenkins, MS, MBA, CPHIMs – Huntington Hospital – Pasadena, Calif.
- Alex Jones, MBA, CPHIMs – US Department of Veterans Affairs – Silver Spring, Md.
- Valayia Jones-Smith, CPHIMs – Olivehurst, Calif.
- Paul J. Jutrasapong, CPHIMs – Henry Mayo Hospital – Valencia, Calif.
- Serena A. Judge, CPHIMs – Lawrence & Memorial Hospital – New London, Conn.
- Pallavi Kanitkar, MS, CPHIMs – Manalapan, N.J.
- Ajithkumar Kantrapati, CPHIMs – Ontario, Canada
- Ken Kaufman, CPHIMs – ICA – Nashville, Tenn.
- Scott Kaufman, CPHIMs – Waltham, Mass.
- Janine Kaya, CPHIMs – Ottawa, Ontario, Canada
- Yin Kean, CPHIMs – Chicago, Ill.
- David E. Keim, CPHIMs – Kaiser Permanente – Pleasanton, Calif.
- Patricia Caroline Kelsey, CPHIMs – Hudson, Ohio
- Margie Kennedy, CPHIMs-CA – Merigomish, Nova Scotia, Canada
- Rich Kerman, CPHIMs – Delouite – Alpharetta, Ga.
- Kasem Kharbat, PMP, CPHIMs – Saudi Aramco – Dhahran, Saudi Arabia
- Bassam Khawaja, CPHIMs – Rehabilitation Institute of Chicago – Naperville, Ill.
- Kimberly Anne King-Guinn, CPHIMs – Driscoll Children’s Hospital – Corpus Christi, Texas
- Donald E. Kinser, MBA, PE, CPHIMs – EDI – Atlanta, Ga.
- Suma Kiruthapradasad, CPHIMs – Flower Mound, Texas
- Bruce Kissel, PMP, CPHIMs – Orlando, Fla.
- Thomas E. Kniss, MBA, PMP, CPHIMs – Community Memorial Health System – Ventura, Calif.
- Ty Knox, CPHIMs – Wilmington, Del.
- Stephanie Koch, CPHIMs – Accenture – Milwaukee, Wis.
- Marc Koehn, CPHIMs – Gordon Point Informatics – Victoria, British Columbia, Canada
- Paul Koepeke, CPHIMs – Snaker Heights, Ohio
- Laura Marie Kroehsky, MBA, MHA, PMP, CPHIMs – Impact Advisors – Portland, Ore.
- Ian Krochak, CPHIMs – Niverville, Manitoba, Canada
- Manjik Kumar, CPHIMs – Medco – Towaco, N.J.
- Paul C. Kuo, CPHIMs – Loyola University Health System – Riverside, Ill.
- Charles Laker, MD, PhD, CPHIMs – Philips – Briarcliff Manor, N.Y.
- Dantes LaHens, PMP, CPHIMs – Lumi Consulting – Kirkland, Wash.
- Mary Lamb, CPHIMs – Telligent – West Des Moines, Iowa
- Shellie Lane, RHIA, CPHIMs – Mercy – Andromere, Okla.
- Chuck Lauflie, CPHIMs – CareTech Solutions – Troy, Mich.
- Edward J. Lavelle, CPHIMs – Columbus University in the City of New York – New York, N.Y.
- Po Jun ‘Francis’ Law, CPHIMs – Toronto, Ontario, Canada
- Christina Romero Lawrence, CPHIMs – Kaiser Permanente – Albany, Calif.
- Melanie Lawrence, CPHIMs – Oklahoma Health Care Authority – Mustang, Okla.
- Jon Le, PMP, CPHIMs – Dallas, Texas
- Pamela Linder Brown, MS, CPHIMs – MD Anderson Cancer Center – Houston, Texas
- Judith L. Lock, RN, MS, CPHIMs – UW Health – Oregon, Wis.
- Warren Longley, CPHIMs – Woods Cross, Utah
- Vanessa Ivette Lora, MD, MSHA, CPHIMs – Miami, Fla.
- Cinda Lott, RN, BSN, CPHIMs – West Georgia Health – Lanett, Ala.
- Mark Lott, CPHIMs – Qualexis – Naples, Fla.
- David Lovison, PMP, CPHIMs – Eugene, Ore.
- Patricia Soledad Lugtis, CPHIMs – MMS Group – Maple Grove, Minn.
- Collene M. Lyons, MBA, PMP, CPHIMs – Continuum Health Partners – New York, N.Y.
- Charlotte M. MacDonald, CPHIMs – Ottawa, Ontario, Canada
- Abid Malik, CPHIMs-CA – eHealth Ontario – Toronto, Ontario, Canada
- Shelagh Maloney, CPHIMs-CA – eHealth Ontario – Toronto, Ontario, Canada
- Warren Maloney, CPHIMs-CA – LifeHealth Ontario – Toronto, Ontario, Canada
- Erin Masinsin, BSME, CPHIMs – Lifesavers’ Home Health Services – Montebello, Calif.
- May Mathew, CPHIMs – Clarksville, Md.
- Marangeli Matos, CPHIMs – Caguas, P.R.
- Byron Mattingly, PhD, MPH, MBA, CPHIMs – Niverville, Manitoba, Canada
- Colleen M. McDonald, MS, CPHIMs – Continuum Health Partners – New York, N.Y.
- LuAnn K. Kimker, RN, MSN, CPHIMs – Arcadia Solutions – Burlington, Mass.

(continued on next page)