WELCOME TO A NEW DIMENSION
OF PATIENT CARE

PAGE 4
REFRESHING YOUR I.T. INFRASTRUCTURE WITH A PATIENT-CENTERED MINDSET

Patient care doesn’t just stop at the point of care. The continuum of care spans multiple dimensions that reach far beyond the medical facility’s walls.

The patient journey is not only about receiving quality care, but about ensuring that patients feel empowered, secure and connected at every juncture. In today’s changing healthcare environment, an individual’s first contact with a community healthcare provider might now be over social media instead of via a friendly postcard in the mail. Instead of grabbing a magazine in the office waiting room, a patient might be entertained through interactive digital displays that invite engagement. Following an initial visit, he or she will likely continue to connect with the physician through telemedicine video conferencing or a secure online portal.

How much impact does this multi-faceted patient experience have on a facility’s IT infrastructure?

This issue of Health Tech Report peels back the hood of the data center and shines a light on what it takes for true IT transformation amid the twists and turns of today’s environment. As always, your dedicated CDW Healthcare account team stands ready to help you make the right decisions.

BOB ROSSI
Vice President, CDW Healthcare
CONTENTS

THE SKY’S THE LIMIT
New trends that are propelling the patient experience to new heights

10 SOLUTION REVIEW
Software-Defined Data Centers (SDDC)
Is your data center robust, agile and scalable enough to protect yet provide access to vital patient data? It can be with SDDC.

12 TECH TIPS
How Healthcare IT Leaders Deal with Data: Simplify, Consolidate, Converge
Converged infrastructure and the cloud improve IT management.

14 EMERGING TRENDS SPOTLIGHT
The New Faces of the C-Suite
As different health initiatives become increasingly important, leading-edge providers are making changes to the C-suite.

16 INFOGRAPHIC
Off the Charts: Analytics in Healthcare
As an increasing amount of patient data becomes available, see how the healthcare industry is poised to benefit from investing in analytics.

18 MEANINGFUL INSIGHTS
Cyber (In)Security
Because they’re prime targets for hackers, healthcare providers need to reevaluate their cybersecurity measures.

20 KEY LEARNINGS
Implementing ICD-10
Take action today to avoid reimbursement and security problems down the road.

22 PARTNER CORNER
Managing Data and Analytics in Healthcare
Chris Gough from Intel shares his thoughts on why data management matters.

Data Center Cloud Extends Healthcare Innovation
Tom Foley from Lenovo talks about how leveraging cloud for data centers helps bring other innovations to life.
THE SKY’S THE LIMIT
PROPPELLING THE
PATIENT EXPERIENCE
TO NEW HEIGHTS

THE TOP 10 TECHNOLOGY
TRENDS RAISING QUALITY,
SECURITY AND SATISFACTION

Anyone who knows what’s up with healthcare today knows the focus is on improving the patient experience. Consumers and providers alike are setting the bar high in terms of expectations and performance. And, increasingly, they’re relying on technology to boost that ever-critical patient engagement, elevate the quality of care and secure sensitive data. Take a look at the technology trends on the rise right now.

THE SOCIAL SHAKEUP

Social media is becoming a must-have in healthcare. A new Health Data Management study reports that more than 99% of hospitals had a Facebook, Foursquare and Yelp account, and more than half had a Twitter account. Facebook was popular for attracting new patients, while Yelp was used to gauge a patient’s in-hospital experience. Medical professionals also find social media a valuable way to track a crisis in real time, helping them prepare for an onslaught of patients. Of course, hospitals need to actively and responsibly manage their social media presence to avoid invading patient privacy or exposing sensitive medical data.

45.6%
of U.S. adults search for health information when using social media.

60%
of doctors say social media improves the quality of care delivered to patients.
Protecting patient information requires a lot more than email encryption and password-secured laptops these days, with cyberthreats climbing and healthcare data breach costs soaring to $6 billion annually. Emerging technologies such as cloud access security brokers (CASBs) inspect and secure data, log activities in real time and alert IT staff to unusual behavior. Digital watermarks can be used to track sensitive information, and single sign-on (SSO) solutions remain good hacker deterrents. Low-tech employee security and privacy awareness training is essential for breach prevention. But given the high risk of breach, a breach response team and plan are also must-haves. For organizations seeking an extra layer of protection, it may be worth looking into one of the new cyber-insurance policies.

Healthcare organizations are eager to ramp up their use of analytics, cloud computing, telemedicine, mobility and other technologies to improve patient care, engagement and experience — and to cut costs. In fact, providers estimate that by 2016, Big Data can help them reduce their annual IT budgets by 21%, or $7.2 billion, and that the cloud can save them 20%. But first they need to bring their infrastructures up to speed. Only 4% say their IT infrastructure is ready to fully integrate these technologies into their clinical workflow.

65% of patients said data security was more important than convenient access for imaging and test results, doctors’ notes, diagnoses and prescriptions.


96% of providers say their infrastructure isn’t prepared for the evolution of their EMR.

2/3 of hospitals are running EMR applications in the cloud. 49% deploy a private cloud strategy, while 35% use hybrid or public clouds.

THINGS TO KNOW ABOUT THE INTERNET OF THINGS (IoT)

First of all, what’s the best way to define IoT, given how frequently the term is tossed around these days? In a recent report, the FDA describes it as “devices or sensors — other than computers, smartphones, or tablets — that connect, communicate or transmit information with or between each other through the Internet.” And the FDA singles out healthcare as a particularly promising area for reaping IoT benefits. Connected devices, including glucose monitors, blood-pressure cuffs, movement sensors and beyond, can provide a rich source of data for physicians, engage patients in their own care, reduce costs, and improve quality of life and patient safety. The flip side of the opportunity, so often the case when it comes to technology, is the challenge of protecting sensitive data and securing devices against unauthorized use.

BEWARE THE HAZARDS

Technology has powerful potential to save lives and improve care, but it also presents a host of hazards that can be life-threatening if left unaddressed. These range from incorrectly configured IT systems, incomplete data and ineffective malware protection to improper medical device maintenance, device design flaws and quality issues. The patient safety organization ECRI Institute lists inadequate alarm configuration policies and practices as the number one hazard, leading to alarm-related adverse events. Incorrect or missing data, insufficient medical device security, and overwhelmed recall and safety-alert management programs also rank in the top 10 hazards for 2015.

The annual number of medical device recalls and alerts increased tenfold between 2001 and 2011 and has remained at nearly 2,500 annually since then.

THE NEW ERA OF POPULATION HEALTH MANAGEMENT

Federal entities and private payers seeking to improve outcomes and reduce costs are putting intense pressure on health IT to support population health management goals. For example, Congress’s “21st Century Cures” initiative seeks to consolidate meaningful use, quality reporting and value-based payments into a single program. HHS recently released the Federal Health IT Strategic Plan to coordinate health data collection, sharing and use among 35 federal departments and agencies. And as CMS pushes Medicare toward a value-based system, a coalition of major providers and insurers has created the Health Care Transformation Task Force with the aim of operating 75% of their businesses under value-based payment arrangements by 2020.

By the end of 2016, at least 30% of Medicare payments will be tied to value through alternative payment models such as ACOs or bundled payment arrangements. By the end of 2018, this figure will rise to 50%.


CLINICAL INFORMATICISTS 2.0 HIT THE GROUND RUNNING

Chief health information officers (CHIOs) and chief health informatics officers (also CHIOs) are rapidly swelling the C-suite ranks along with the more traditional CIOs, CMIOs and CTOs, thanks to healthcare organizations’ growing reliance on IT and analytics for population health and value-based care. Although it’s clear this new generation of clinical informaticists has moved well beyond directing EHR implementation, their new responsibilities remain somewhat vague — yet highly demanding. They range from integrating the business and clinical sides of healthcare, to data visualization and presentation, to using technology as an enabler to achieve patient care and financial goals.

National Coordinator Karen DeSalvo, MD, appointed the ONC’s first chief health information officer in January to “expand and enrich the federal government’s focus on health information management, data analytics and interoperability.”

SOURCE: healthitanalytics.com, “ONC Appoints Its First Chief Health Information Officer,” January 2015
Despite substantial investment in patient portals, they have yet to truly transform patient engagement and communication. In fact, nearly 40% of patients are unsure if their primary care physician even has a patient portal, and less than half report being shown a portal either during or outside their office visit. The key to better engagement may be to use portals as one of several tools in a holistic patient engagement strategy. For example, some physicians are projecting visual displays of EHR data onto flat screen TVs during appointments. Other providers are starting to embrace “smart” solutions such as stand-alone mobile tools and interactive patient platforms, separate from EHRs. And then there’s always email and texting – as long as the messaging is secure, of course.

WEARABLE TECHNOLOGY: MOVING BEYOND FASHION FAD

Consumers appear increasingly willing to wear health and fitness trackers, especially if encouraged to do so by their employers, physicians or insurers. A survey by Cornerstone OnDemand found 8 out of 10 full-time employees would use a company-provided wearable device in exchange for benefits such as a year-end bonus, reduced health insurance premium or exercise program discount. And while another study by Technology Advice Research found that only 11% of those surveyed used a fitness tracker, 48% say they would do so if prompted by their physician, and 57% would if it lowered their insurance premiums. However, many clinicians are still waiting for wearables to prove their practical value in improving health. A new lab at Stanford University may provide some answers with research focused on how to make all the biometric data the devices collect medically meaningful.

THE MILLENNIAL MINDSET

Millennials matter, since their preferences will drive healthcare consumption and delivery in the future. And given that they’re the generation that grew up with technology, they expect to use it in healthcare, just like they do in the rest of their lives. A Salesforce-sponsored Harris Poll reported that about 75% consider online reviews and the ability to book appointments and pay bills online important when selecting a physician. 71% want a mobile app to book appointments, share health data and manage preventive care, while 60% support telemedicine options in lieu of in-person visits. And 60% are interested in innovative technologies like swallowing pills to track internal vitals or 3D printing for prosthetics, hearing aids and other health-related items.

HEALTHCARECOMMUNIT

CDW Healthcare’s CommuniT is a great tool to connect to the latest IT trends and technologies. Visit CDW.com/communiT and see how we’ve redesigned the site to bring you the best in healthcare IT!
Server virtualization is only the beginning. By extending virtualization concepts to storage resources, healthcare organizations are beginning to transform their data centers from deeply siloed operations defined by hardware to highly automated resources designed around software.
As virtualization, cloud and mobility create more complex environments, healthcare data center managers are challenged to handle new data streams, add layers of security, and connect with more applications and users while trying to minimize routine, labor-intensive activities or the need to add costly, specialized systems.

It’s the increasingly common situation of having to do more with less. Your infrastructure needs to be robust, agile and scalable enough to protect vital patient data while, at the same time, ensuring immediate access to that data anywhere, anytime. Quality patient care depends on it.

Enter the SDDC, or software-defined data center. With an SDDC, the core infrastructure elements—networking, server, storage, security—are integrated and virtualized. Intelligent software systems control the entire center, and this software is used to automate application deployment and management, provisioning, configuration and operation.

Instead of manually coordinating virtualized and non-virtualized elements, configuring load balancers or applying security profiles, IT staff can support initiatives (ICD-10, anyone?). Plus, SDDCs offer the flexibility, computing power and unified platform to deploy the latest applications without the need for an expensive and time-consuming physical overhaul of the data center.

**SDDC BENEFITS**

Upgrading existing data centers to SDDCs can reduce capital equipment costs by 58% and reduce infrastructure operating expenses by 56%. A more responsive, agile, secure and high-performing data center that takes full advantage of the underlying hardware offers a number of benefits:

**Impressive cost-effectiveness.**

Virtual IT services, automated operations, and centralized monitoring and management boost resource utilization and staff productivity, reduce costs and increase efficiency.

**Streamlined provisioning.**

Deploy and manage applications across your entire health system in minutes with automated, agile provisioning.

**No-nonsense security.**

Policy-based management protocols and advanced security services integrated directly into the network platform ensure compliance, and unified monitoring provides insight into potential threats.

**Major mobility support.**

Secure, speedy delivery of mobile apps ensures clinicians on-demand access to critical patient data on any application on any device, whenever and wherever they need it.

**Valued responsiveness.**

Automatically apply pooled network resources to unplug bottlenecks and ensure application responsiveness, even with increased network traffic.

**READY TO OPTIMIZE YOUR DATA CENTER?**

Here are some best practices to keep in mind:

**GO VIRTUAL.**

Virtualizing computing power, networking, and storage creates a highly flexible, efficient and integrated infrastructure that speeds access to critical data, enhances security and compliance, and centralizes and streamlines management. Plus, fewer devices means fewer setup, management, power, cooling and cabling costs.

**HA VE A STRATEG Y.**

Transitioning to an SDDC requires adoption of automation and orchestration at a strategic, organizational level. Ensure that mission-critical policy and compliance issues, including those affecting information security, are fully accounted for in the plan.

**STAY FAST AND FLEXIBLE.**

Unified management tools help detect and resolve problems quickly, and make it easy to add storage and bandwidth.

**KEEP DATA ACCESSIBLE.**

Make sure your data protection strategies don’t prevent clinicians from quickly and easily accessing patient data. Keep critical data readily available with smart, tiered storage management and robust networking.

**TO LEARN MORE:**

- Download our new “Transform Your Data Center for Healthy Outcomes” eBook, at CDW.com/infrastructureebook
- Read the white paper, “Defining Moment: The Software-Defined Data Center,” at CDW.com/wpdatacenter

**SOURCES:**

- tanejagroup.com, “Transforming the Datacenter with VMware’s Software-defined Data Center vCloud Suite,” June 2014
- blogs.vmware.com, “Tribal Knowledge,” September 2014
- healthcareitnews.com, “Infrastructure unready for new EMR tools,” October 2014
How Healthcare IT Leaders Deal with Data: Simplify, Consolidate, Converge

Converged infrastructure, virtualization and the cloud. That’s where healthcare environments are headed, driven by compliance and data storage requirements and an increasing need to streamline operations.

Healthcare IT managers must wrangle a crushing amount of data — often on siloed, disparate systems — to ensure that clinicians and patients have safe, secure, yet on-demand access to it. “There’s a great need in healthcare to simplify, to consolidate the management of the infrastructure,” says Robert Forster, a solution architect at CDW specializing in servers and storage for larger healthcare organizations. “Many of my conversations are about virtualization, converged infrastructure and the cloud — forward-looking approaches that help bring about improved resource utilization, centralized management and lower overall costs.”
In converged infrastructure, compute, storage, virtualization and networking are combined into one node or appliance. “From an initial cost standpoint, you don’t have to overspend to buy something you’ll eventually grow into,” says Robert. “As you grow, you just add more appliances. It’s a ‘buy as you need’ format.” This elasticity allows companies to expand easily, quickly and with less management.

Converged infrastructure can fast-track IT’s ability to improve the patient experience without overtaxing the team. That’s because it’s:

**More flexible.** Adapts quickly to new demands and cost-effectively scales to keep up with growth.

**More manageable.** Provides greater visibility, automation and resource utilization to boost efficiencies.

**More secure.** Reduces the number of access points vulnerable to data breach, and takes advantage of better backup and recovery tools to further protect data.

**Cloud-ready.** Virtualization helps build a solid foundation for transitioning to cloud computing and SDDS.

A new CDW survey, “Cloud 401: Navigating Advanced Topics in Cloud Computing,” revealed that cloud services migration and integration was a top challenge for most IT professionals. Healthcare industry leaders have identified storage and email as the easiest services to transition to the cloud, and report their top uses of the cloud are to deliver, either partially or totally, storage (58.7%), email (46%) and productivity (42.7%) services.

According to the survey, the cloud helps healthcare organizations deliver about a third of their IT services. Interestingly, 52.8% were migrated from traditional delivery and 47.2% were newly introduced in the cloud.

“IT organizations that are ready to give up ownership and manageability of specific applications to cloud-based offerings gain additional advantages,” says Robert. “A hosted model reduces the need to buy hardware and software, and allows the application to be categorized as a recurring, month-to-month cost of business. Plus, someone else has the responsibility of storing, securing, replicating and protecting the data.”

What cloud services are healthcare leaders looking to next? “Better and improved disaster recovery,” says Robert. “Organizations want failover capability, ideally to another facility. If that doesn’t exist, a cloud-based solution makes a lot of sense.” With disaster recovery as a service (DRaaS), there’s no need for capital investments in new infrastructure, no worry about annual testing and failover, and — most important — it’s an active site that allows for continuity of patient care.

By taking advantage of converged infrastructures and cloud services, healthcare IT departments are taking great leaps forward in simplifying operations to focus on the critical: ensuring clinicians have access to patient data, and that patient data is both protected and preserved.

In converged infrastructure systems, reduce overall costs by 55% and time to deployment by 65%.

**SOURCE:** IDC, “Using Converged Infrastructure to Enable Cost-Effective Private Cloud Deployments,” June 2014

**TO READ MORE:**

“Cloud 401: Navigating Advanced Topics in Cloud Computing”

CDW.com/cloudreport
Growing priorities for data security, population health management and patient satisfaction are beginning to shape the next generation of healthcare leadership, as providers begin to see the value in adding some new talent and expertise to set them apart from the competition. Expect to see more of these new roles at the IT decision-making table.

Data, IT and Patient Experience Take Center Stage with New C-Suite Titles
Chief Data [Analytics] Officer (CDO),
Chief Health Information Officer (CHIO)

As data goes “Big” in every industry, including healthcare, its storage, accessibility and security have become vital. In fact, 57% of healthcare organizations have implemented or plan to implement clinical data analytics in the near future.1 Thus, CDOs — focused on managing data and leveraging analytics tools — have become a popular addition to the healthcare leadership team. The ideal CDO has both industry expertise and a decade or more of experience in data.

CHIO roles are serving similar functions, tackling the interoperability problem and lending strategic direction to better harness data that impacts patients. Because data is so dispersed across healthcare organizations, these roles centralize control to allow for better data management and ultimately the ability to leverage health information for population health and improved outcomes.2,3

Chief Medical Information Officer (CMIO),
Chief Nurse Information Officer (CNIO)

While the CMIO/CNIO role has existed in larger health systems for a while now, it’s starting to become more common across the board and move into a more strategic position in the overall leadership structure. CMIOs/CNIOs serve to bridge the gap between medicine and IT. Their strong IT backgrounds give them a solid technology foundation, but because they’re usually also physicians or nurses, they can easily interface with healthcare providers to help gain buy-in, implement new solutions and effectively drive improvements in outcomes.4

Chief Nursing Officer (CNO),
Chief Experience Officer (CXO),
Chief Transformation Officer (CTO)

Patient experience is closely linked to the quality and safety standards of a hospital, so it’s no surprise patient care and experience roles are taking center stage. Often reporting to the COO or CEO, these roles have responsibility for the service side of hospitals. Their end goal is to make patients feel good about their choice of provider by ensuring that a high standard of care and positive interactions are delivered at all levels of the organization.

CNOs often have an MBA, PhD or DNP and bring business and financial expertise to the patient care experience. CXOs come from a wide range of backgrounds — many providers prefer the credibility of having a doctor or nurse in the role; other systems look outside the walls of healthcare to employ individuals from service industries like hospitality and marketing. Similar to CXOs, CTOs aim to think outside the box and take organizations to a new level of value-based care.2 Individuals who fill this role need both a strong understanding of healthcare and an innovative, future–state mindset.4

Initiatives developed by these roles vary and can include training on patient interactions, recommendations for technology solutions and improvements to access.5,6 With both reimbursements and new business on the line, providers that establish an executive-level position dedicated to the delivery of care initiatives send a message to employees and consumers that they take this responsibility seriously.7

Sources:
Off the Charts: Analytics in Healthcare

With so much information at their fingertips, healthcare providers are investing in IT to harness the potential of analytics to improve care. A new CDW Healthcare report explored this topic further.

More than **TWO-THIRDS** of healthcare decision makers say analytics is one of their organization’s top three priorities.

65% of organizations say their analytics spending will increase in 2015.

ORGANIZATIONS PLAN TO INVEST IN A NUMBER OF AREAS:

- **36%** Enhanced data security
- **34%** Data warehouse/data models
- **35%** Real-time data analytics applications
- **39%** IT systems/solutions to improve data capture
- **41%** IT systems/solutions to optimize data processing
- **41%** IT infrastructure to optimize data storage

SOURCE: Analytics in Healthcare Report, CDW Healthcare, August 2014; 150 healthcare decision makers surveyed; total sample equates to a margin of error of ±7.97% at a 95% confidence level.
Implementing analytics has resulted in both clinical and operational enhancements.

**TOP CLINICAL BENEFITS:**

- 63% Reduced readmission rates
- 62% Improved overall health outcomes
- 82% Improved care

**TOP OPERATIONAL BENEFITS:**

- 49% Improved management decision making
- 54% Improved financial reporting capabilities
- 50% Improved hospital operational performance

63%

**TOP OPERATIONAL BENEFITS:**

62%

**TOP CLINICAL BENEFITS:**

82%

How could you benefit from greater use of analytics? Learn more about the latest in analytics at [CDW.com/communIT](http://CDW.com/communIT).

For the latest on Health IT topics and trends, get social with us! 🌐 @CDW_Healthcare  🍀 CDW–Healthcare  📳 CDW.com/communIT
A glaring spotlight has recently been shone on the vulnerability of electronic patient data as an increasing number of healthcare organizations have disclosed data breaches. These incidents serve to remind the healthcare industry of the need for strong cybersecurity measures and a skilled IT staff to support them.
Last year, the FBI warned the healthcare industry that it was the least prepared sector in regard to cybersecurity, and the FDA issued new guidelines for medical device manufacturers that encourage them to improve the security of their devices. Research also shows that healthcare organizations spend less than any other industry on cybersecurity.

If that weren’t alarming enough, the threat landscape continues to evolve. Attacks are more social, sophisticated and stealthy than ever. The typical hacker spends $400 on tools to create attacks, which can range from traditional and advanced malware to vulnerability exploits to targeted attacks.

### Protecting your data

Providers developing a security strategy for their electronic health records and patient portals need to take a holistic and multi-layered approach, considering the security needs of both their end users and the entire data center. A comprehensive review of its IT infrastructure and current security measures can help an organization determine how vulnerable it is to cyberattack. The assessment helps identify gaps in its systems, and providers can investigate ways to reduce or eliminate those issues.

Providers should ask themselves questions such as, “Are we running legacy environments that need an interim solution for security protection? Do we have cloud and data center environments and, if so, how are they secured? Are we offering the best technology for mobile patient care? How are we securing that data?” The answers to those questions guide an organization toward the security measures it should take.

Ultimately, the best solution takes a two-pronged approach: the right technology and the appropriate corresponding policies and procedures for users. Organizations should consider how data is accessed and shared, including devices, applications and networking, and storage and backup. The appropriate technology solutions may include anti-viral software, internal and external firewalls, phishing filters and access control measures. Additionally, organizations must train employees on how to recognize and respond to system breaches or phishing attempts, and set policies for traveling with work computers or mobile devices.

There’s no predicting what organization a hacker will hit next, but providers do have ways to protect their data from breaches — as long as they look at their systems holistically and proactively pursue solutions that are a fit for their needs.

According to a 2014 report from the nonprofit group Identity Theft Resource Center, the healthcare sector accounts for 42.5% of all security breaches.

Healthcare breaches are, unfortunately, nothing new. Yet with the impending deadline of ICD-10, conditions are ripe for a perfect storm that could throw the industry into chaos.

Security experts should play a major role in planning and testing prior to the October 1 deadline.
A recent article in *FierceHealth IT* reports that in many practices, data security and privacy have taken a back seat to the need for implementing electronic health records, administrative transactions and big changes like ICD-10. It’s not uncommon when organizations are racing to get high-priority projects implemented that, at the end of the implementation, they identify some security breaches and vulnerabilities.

A better approach is to involve staffers with a specific focus on cybersecurity at every stage of a project. In a related article, ICDmonitor.com suggests that providers who are testing the new coding system keep these security questions in mind:

**What types of data risks should we be thinking about and trying to mitigate as we roll out ICD-10?**

**Should we be concerned about connectivity issues with external trading partners?**

**Where does data security fit in as we execute ICD-10 testing internally and externally?**

With the increased amount of information that will be transferred to payers, and the confusion that is sure to ensue on October 1, providers should take steps now to beef up their data protection plans and reduce the likelihood of a major breach.

Take action today to avoid reimbursement and security problems down the road.

---

**Ready to get started on the road to a successful transition? Here are our key recommendations:**

Have a security team as part of your ICD-10 test team committee so they can guide the development of test environments and maintain the security oversight for ICD-10 projects. Include at least one person with a focus on cybersecurity.

Think carefully about who should have access to the codes. If you plan to outsource testing, it’s critical that your vendors fully understand the need for security and are able to maintain the privacy of the information they are handling on your behalf.

Conduct a thorough review of your cybersecurity policies and procedures before, not after, the ICD-10 deadline.

---

**CRACKING THE CODES**

The ICD-9 codes used by medical practitioners in the U.S. today date back to 1979 and are, in places, obsolete. Most of the world has already adopted the ICD-10 code set. After years of delay, America will make the switch on October 1, 2015.

**PLAY FOR PAY(MENT)**

The transition to ICD-10 is required for everyone covered by the Health Insurance Portability Accountability Act (HIPAA). Centers for Medicare & Medicaid Services (CMS) and other payers will accept, recognize and process only ICD-10 codes after October 1, 2015. Claims billed with ICD-9 codes after October 1 will be rejected and those providers won’t be paid.

**A SYSTEMS ISSUE**

CMS and many commercial health plans are unable to process claims for both ICD-9 and ICD-10 codes submitted for the same dates of service, so a “transition period” — in which providers could submit claims using either ICD-9 or ICD-10 — is not possible. It will be a clean cutover date.

**PLAN FOR SECURITY**

The American Health Information Management Association (AHIMA) recommends training on ICD-10 six to nine months before the compliance deadline. Don’t limit training to mapping the code set. ICD-10 is the perfect time to make sure your security is up to date.

**HELP IS AVAILABLE**

- AHIMA offers a Planning and Preparation Checklist as well as an Implementation Toolkit.
- The Road to Ten website has interactive tools to help practices build transition plans.
- Sign up for email updates or to follow CMS on Twitter at its dedicated site.

---

**Sources:**

- healthcareitnews.com, “CMS Touts End-to-End ICD-10 Test Success,” February 27, 2015
- Centers for Medicare & Medicaid Services’ eHealth University, Small and Medium Practices ICD-10 Transition Checklist, February 2014
- himss.org, “HIMSS ICD-10 Playbook,” March 2015
Managing Data and Analytics in Healthcare

The flood of data entering healthcare organizations will only grow as more information is shared between more healthcare entities in an effort to more accurately approach patient care, especially in regard to data analytics.

What’s behind this data push? Right now, I’m seeing two trends prompting a shift toward greater data analysis: 1) healthcare reform’s shift to value-based care; and 2) ever-growing concerns around patient safety. From growth in the number of ACOs to team-based reimbursement structures and rewards for healthy population outcomes, accurate review, sharing and measurement of data has never been more important. Likewise, to increase patient safety and quality care, accountability for both treatment successes and errors must be measurable and actionable.

The takeaway is that, going forward, all healthcare data will matter. And analytics will become crucial to forwarding all aspects of care.

But as organizations continue to struggle with data silos and disparate storage systems, it’s clear much infrastructure change is still needed.

In the end, to achieve greater data integration across structured data (lab reports), unstructured data (images, notes), EMR files and patient-generated data, visualization must be achieved. This entails optimizing the data architecture for the most effective analytics capabilities. At a high level, this solution boils down to balance — of the compute, storage, software and network aspects of a healthcare organization’s data infrastructure.

With balance comes the key to unlocking the true potential of data analytics for patient care.

Five-Step Checklist: Get Started with Your Big Data Analytics Project

- WORK WITH YOUR BUSINESS USERS TO ARTICULATE THE BIG OPPORTUNITIES.
- DO YOUR RESEARCH TO GET UP TO SPEED ON THE TECHNOLOGY.
- DEVELOP USE CASE(S) FOR YOUR PROJECT.
- IDENTIFY GAPS BETWEEN CURRENT AND FUTURE-STATE CAPABILITIES.
- DEVELOP A TEST ENVIRONMENT FOR A PRODUCTION VERSION.

ABOUT CHRIS GOUGH

As Lead Solutions Architect for Intel Health & Life Science, Chris meets with enterprise organizations around the world to advise them on Big Data and analytics, cloud computing, and healthcare security and privacy. Chris also works closely with industry partners and customers to design, develop and publish industry proof points that demonstrate the benefits of healthcare technologies based on standardized architectures.
DATA CENTER CLOUD EXTENDS HEALTHCARE INNOVATION

Q&A
with Tom Foley, Lenovo Global Health Solutions Strategy Manager, PCG Industry Solutions

Q: HOW ARE HEALTHCARE ORGANIZATIONS INNOVATING IN THE DATA CENTER?
A: They’re really starting to embrace cloud. In the past year I’ve seen a measurable increase in the adoption of cloud technologies, spurred by increased acceptance of the cloud as a secure option and underlying pressure to achieve greater efficiencies while freeing up budget to devote to other strategic initiatives.

Q: HOW DOES THIS UPTICK IN CLOUD ADOPTION MAKE THE ADOPTION OF OTHER INNOVATIVE TECHNOLOGIES POSSIBLE?
A: The cloud really provides the ability to better scale the infrastructure in a cost-effective and, in many cases, more secure manner. This, in turn, ensures performance and improves flexibility — allowing healthcare organizations to do more with less. This effort will permit greater focus on other strategic initiatives centered on care coordination, such as mobility, population health management, analytics, patient engagement and the medical home — all very important as the market shifts to an accountable care model inclusive of a new value-based reimbursement system.

Q: HOW DOES THIS SUPPORT PATIENT–CENTRIC CARE?
A: Meaningful use Stage 2 was a big driver behind getting patients and clinicians alike to share health information. mHealth and mobility in general have extended that to tie ancillary health data into the overall patient record, which supports population management.

At their heart, population health initiatives are about access to a broad base of information relative to the community of care servicing a particular patient. The data center/cloud securely stores this data in a central clinical data repository. The ability of the patient and the clinical care team to securely share this same information further facilitates the coordination of care across the different settings of care. This also facilitates a shift to a proactive versus reactive engagement model.

ABOUT TOM FOLEY
Tom has 25–plus years of information technology expertise, 15 of which have been in the healthcare market. He is well versed on meaningful use regulatory requirements, interoperability, patient engagement and population health initiatives — including health information exchanges.
Please remember to recycle.

MKT14F688