ICD-10: Targeting reporting and reimbursement

Telemedicine: Finding untapped revenue
BYOD security strategies
Do health apps work?

Thought Leaders
Four steps to a winning accountable care strategy
Reed Liggin, VP
Client Development,
Clinicals Enterprise,
athenahealth
THE DIFFERENCE IS INFORMATION GOVERNANCE

Leveraging Information as a Strategic Asset

Reliable and Trusted Information for
- Improving Patient Outcomes
- Better Informed Decision Making
- Compliance and Security Risk Mitigation
- Leveraging Clinical, Financial and Administrative Information
- Streamlining Business Processes

IGAdvisors™ is leading the healthcare industry in expert information governance (IG) strategy and implementation by providing consulting services to help organizations understand and improve the trustworthiness of their information.

IGAdvisors™ uses IGHealthRate™, the industry standard tool for assessing IG maturity.

(844) 554-IGIQ | IGAdvisors@ahima.org | IGAdvisors.com
CONTENTS

::: HEALTH APPS
14 | Do health apps work?
By Steven Willey, M.D., Founder and Chief Scientist, YouPlus Health

::: TELEMEDICINE
16 | The beginning of a new era
By Samir Qamar, CEO, MedLion
18 | Phone it in: A perfect storm takes telemedicine to new heights
By Michael Sherling, M.D., MBA, Chief Medical Officer and Co-Founder, Modernizing Medicine

::: BYOD SECURITY
19 | VMI: The no-data-foot print path to mobile security
By Sinan Eren, Vice President and General Manager, Avast Mobile Enterprise

::: THINK TANK: ICD-10
8 | ICD-10: Targeting reporting and reimbursement
A panel of experts fields questions on how the industry is adapting
11 | 2016: A year of change for healthcare finance
By Karen England, Revenue Cycle Consultant, Ingenious Med
12 | Five steps to promote accuracy in the wake of ICD-10
By Ken Bradley, Vice President of Strategic Planning and Regulatory Compliance, Navicure
13 | CMS: Assess your ICD-10 KPIs, RelayHealth
Financial reports claim denial trends

DEPARTMENTS

Industry Watch
6 | A patient's perspective on ransomware
- Accenture: Hospitals missing out on millions
- Hidden costs of pager use revealed
- Doctors and patients at disconnect over health-tracking app data
- War on germs takes flight

COLUMNS

Viewpoint
4 | Replacing the wall with a fence
By Chad Michael Van Alstin, Features Editor

Thought Leaders
28 | Four steps to a winning accountable care strategy
By Reed Liggin, Vice President, Client Development, Clinicals Enterprise, athenahealth

::: SECURITY BREACHES
22 | Risking a breach
By Art Gross, President and CEO, HIPAA Secure Now!
23 | Holding data hostage
By James Savage, Founder and President, Concurrency

::: THINK TANK: ICD-10
8 | ICD-10: Targeting reporting and reimbursement
A panel of experts fields questions on how the industry is adapting
11 | 2016: A year of change for healthcare finance
By Karen England, Revenue Cycle Consultant, Ingenious Med
12 | Five steps to promote accuracy in the wake of ICD-10
By Ken Bradley, Vice President of Strategic Planning and Regulatory Compliance, Navicure
13 | CMS: Assess your ICD-10 KPIs, RelayHealth
Financial reports claim denial trends

DEPARTMENTS

Industry Watch
6 | A patient's perspective on ransomware
- Accenture: Hospitals missing out on millions
- Hidden costs of pager use revealed
- Doctors and patients at disconnect over health-tracking app data
- War on germs takes flight

COLUMNS

Viewpoint
4 | Replacing the wall with a fence
By Chad Michael Van Alstin, Features Editor

Thought Leaders
28 | Four steps to a winning accountable care strategy
By Reed Liggin, Vice President, Client Development, Clinicals Enterprise, athenahealth

::: SECURITY BREACHES
22 | Risking a breach
By Art Gross, President and CEO, HIPAA Secure Now!
23 | Holding data hostage
By James Savage, Founder and President, Concurrency
THE EHR THAT SOLVES HEALTH CARE’S BIGGEST PROBLEM: THE EHR
IT’S TIME TO LET DOCTORS BE DOCTORS

YOUR PHYSICIANS DIDN’T GO INTO MEDICINE TO DO DATA ENTRY. OUR REDESIGNED ELECTRONIC MEDICAL RECORDS SIMPLIFY THE WORKFLOW AND REDUCE NON-CLINICAL TASKS SO DOCTORS CAN FOCUS ON THE WORK THEY DO BEST: PROVIDE EXCELLENT PATIENT CARE.

IT’S PART OF OUR NETWORKED SUITE OF SERVICES THAT HELP YOUR ORGANIZATION GET PAID MORE, FASTER; REDUCE ADMINISTRATIVE COST; AND STAY CURRENT ON INDUSTRY CHANGE.

LEARN MORE AT ATHENAHEALTH.COM

athenahealth

NETWORK-ENABLED EHR, PRACTICE MANAGEMENT, PATIENT ENGAGEMENT, AND CARE COORDINATION SERVICES
VIEWPOINT

Replacing the wall with a fence

That Apple v. FBI court case will impact healthcare security.

I’M PERSONALLY VERY CONCERNED WITH PRIVACY AND SECURITY. It’s this facet of HIT that garners my attention the most, and as such I took every opportunity I could at HIMSS16 to pick the brain of security experts from across the space. How do we keep patient data private and secure from prying eyes? Do seized medical records give the bad guys a window into our lives? What can be done to halt data breaches and stop identity theft?

The answers I received during my chats seemed to converge into one overriding piece of advice: Security starts with you, and it’s the job of each and every consumer to protect their own privacy. With a heated battle wages in the courts between Apple and the FBI over unlocking iPhone data, I was happy to hear most security experts – or at least those I spoke with – seemed to look past emotions surrounding the issue and delved deep into the logistics of what weakened encryption means for everyone – not just the purported perpetrators, but for me, you, and every person who values their privacy.

The media narrative has been simplified to a story where the FBI wishes to access one shooter’s phone, and Apple refuses on the basis that doing so would open a “Pandora’s Box” of weak encryption, where soon every overreach of government agency, oppressive regime, and two-bit criminal on the planet will exploit the workaround for their own aims.

And while it may sound crazy, Apple isn’t wrong. And believe it or not, this issue of the San Bernardino shooter’s phone also may impact security at healthcare practices all over the globe.

With more and more institutions utilizing smartphones and tablets to deliver care, a mobile device with built-in backdoors – even those made to be used (theoretically) only by authorities – means these devices are, by definition, insecure. Encryption, often touted as the final effective line of defense to protect patient records, is meaningless if a device contains malware or a doorway that can be accessed by someone other than the user. In an era where no secret seems safe, to suggest that only the “good guys” would have this backdoor is to suggest that every single person who works for Apple and the FBI is a good, ethical person who will not overstep their bounds. Even if I could accept such a premise, secrets always find a way of being leaked, especially if those secrets can be leveraged to make a lot of money.

David Finn, Health IT Officer, Symantec, has said in JMT on more than one occasion that data security is a “people problem”. Users are careless with devices or may download malware unwittingly. It’s ultimately human error that is the cause of many security incidents. In my opinion, intentionally designing a device to have a security flaw will only amplify this problem. Training may fix the “people problem,” but teaching patients and clinicians to encrypt their devices means very little if the standard encryption methods aren’t actually able to keep invaders out.

With more and more data changing hands via health apps, telemedicine, and through BYOD at the point of care, the security of an iPhone is a whole lot bigger than one criminal case. As long as the devices doctors, nurses, and patients use are insecure, we’re inviting more identity theft and cyberattacks to happen, and the results could be catastrophic. It’s my hope that Apple wins this battle – and if they don’t, I hope many of you will join me in seeking third-party encryption alternatives.

As always, I want to thank you for reading our magazine, and I welcome your feedback at cvanalstin@npcomm.com.
BUILDING on the success of today for an EXCEPTIONAL tomorrow

ciox
HEALTH

Advancing the way health information is managed.

cioxhealth.com
800.737.2585

Previously known as HealthPort, IOD Incorporated, Care Communications, and ECS.
Security

A patient’s perspective on ransomware

By Sean Mason, Director of Threat Management, Cisco Security Advisory Services

In 2015, I had a crippling case of sciatica. This prompted me to undergo a series of tests, including an MRI and, ultimately, a very scary lumbar microdiscectomy surgery to fix a severely herniated disc. I mention this because, while I am an information security professional, I’m also a patient who requires medical care on occasion. I put my trust and confidence in both the hospitals and healthcare providers that help me.

This is why it’s very concerning and personal to me when I receive nearly weekly calls from hospitals and healthcare providers seeking assistance to respond to ransomware and other malware incidents taking place within their environment.

Upfront reality

By the time I receive those phone calls, considerable damage is usually already done. In a recent case, an entire wing was rendered inoperable, and the ability to service patients was severely impacted. When it comes to ransomware, there is no way to recover your data outside of taking the chance – and risk – of paying off the perpetrator and hoping they follow through with their end of the bargain.

While I usually advocate that prevention is not a panacea and can eventually be defeated, the reality is that the best way organizations can address ransomware is to be proactive and work to stay ahead of it.

The fundamentals

It is important to recognize that healthcare organizations are rather unique, given their mix of devices on the network. Many are running unsupported operating systems from a decade or more ago. As such, the cybersecurity fundamentals required to protect the network are slightly different. For example, many of the newer and more effective cybersecurity technologies that reside on the endpoint are incompatible with older operating systems, so network-based defensive approaches should be considered.

Additionally, all organizations should:
• Ensure a robust security program is in place;
• Incorporate continuous patching, monitoring, and tuning of security tools;
• Include a process to respond immediately to any issues to ensure that they don’t become exacerbated; and
• Consider consulting with a trusted security advisor to develop your security strategy before disaster strikes.

Final thoughts

According to the 2016 Cisco Annual Security Report, one ransomware campaign alone was targeting up to 90,000 victims per day, for an estimated $30 million total annually. With numbers like these, criminals will continue to operate these campaigns. Organizations will continue to see ransomware and other variations of it for quite some time.

Taking the time and effort to be proactive and implement approaches to combat this threat is required not just now, but will be needed for years to come. Additionally, while it can be very easy to have a hyper-focused level of concern with ransomware, these techniques will also help you stay ahead of other malware issues that can cause considerable impact to your healthcare organization.

Always remember: While it may appear simpler to just pay a ransom, you are dealing with criminals. There is no guarantee that paying them off will work.

Healthcare organizations must be vigilant in protecting patients, instilling trust and confidence, with the assurance that their solutions are safe to use. This is paramount to any patient, including this one.

Mobile Apps

Accenture: Hospitals missing out on millions

Only 2 percent of patients in the largest U.S. hospitals are using hospital-provided mobile health apps, according to new research from Accenture, and it’s a costly situation. Accenture estimates that failure to align mobile apps to the services consumers demand could cost each of these hospitals, on average, more than $100 million annually in lost revenue.

The research, which assessed mobile app use among the 100 largest U.S. hospitals, found that two-thirds (66 percent) of the 100 largest U.S. hospitals have mobile apps for consumers, and roughly two-fifths (38 percent) of that subset have developed proprietary apps for their patients. However, only 11 percent of health systems offer patients proprietary apps that operate with at least one of the three functions that consumers demand most: access to medical records; the ability to book, change, and cancel appointments; and the ability to request prescription refills electronically.

“Simply having a mobile app is not enough,” says Brian Kalis, Accenture’s Managing Director of Digital Health Strategy. “Hospital apps are failing to engage patients by not aligning their functionality and user experience with what consumers expect and need.” Those who become disillusioned with a provider’s mobile services (or a lack thereof) could go somewhere else.

According to Accenture, this is already happening: Approximately 7 percent of patients have switched healthcare providers due to a poor experience with online customer service channels, such as mobile apps or Web chat. Accenture estimates that this pattern could lead to a loss of tens of millions of dollars in annual revenue per hospital and suggests that as consumers bring their service expectations from other industries into healthcare, providers are likely to see higher switching rates on par with the mobile phone industry (9 percent), cable TV providers (11 percent), or even retail (30 percent).

The report suggests that one way for hospitals to improve the customer experience is to partner with digital disruptors such as Good Rx, ZocDoc, InstaMed Go, and WebMD to create mobile platforms tailored to their specific patient demands. For example, a large healthcare provider might partner with ZocDoc to improve appointment scheduling or with InstaMed Go to improve bill paying.

Source: Accenture
Secure Messaging
Hidden costs of pager use revealed

A new study commissioned by TigerText shows hospitals pay 45 percent more for antiquated paging technology than they would for secure messaging. The HIMSS Analytics study, which surveyed 200 U.S. hospitals, revealed that 90 percent of these organizations still use pagers and each spends, on average, $180,000 per year.

“The Hidden Cost of Pagers in Healthcare” study included research from HIMSS Analytics and other market research. The HIMSS Analytics research found that the average paging service cost per device was $9.19 per month, compared to industry research showing the cost of secure messaging app alternatives to be less than $5 per month.

The HIMSS Analytics research also revealed significant “soft” costs from the continued use of pagers:

• A lack of two-way communication was the most commonly cited disadvantage of using pagers among the executives interviewed;
• One-way paging does not give recipients full context nor the option to provide feedback or ask questions, costing care teams precious time to manage patient care;
• Pagers were seen in interviews as causing communication gaps by not allowing updates to contact directories and on-call schedules, which are critical to effectively reaching physicians;
• Survey respondents noted the inconvenience of carrying and managing more than one device; and
• The limitation of paging systems operating only on a single network was perceived as a significant disadvantage, unlike smartphones, which communicate across multiple networks (i.e., cellular, Wi-Fi).

The HIMSS Analytics research included a quantitative survey of more than 200 pager users at hospitals throughout the United States, with a bias toward large organizations with more than 100 patient beds, as larger hospitals tend to have a high correlation to pager use.

Source: TigerText

Mobile Tech
Doctors and patients at disconnect over health-tracking app data

So you’ve been using your fitness tracking band religiously for months, and you’re excited to show your doctor all the progress you’ve made logging extra steps and counting nearly every calorie. And look at that heart rate! But will your doctor even care, and is your data even usable on a professional level?

These are some of the main questions that University of Washington (UW) researchers tried to answer in a new study on healthcare activity trackers, apps, and self-reported data. The overall conclusion (brace yourself): Most healthcare providers don’t have the time or tools to review your data – and your data may not be scientifically valid anyway.

UW researchers surveyed 211 patients and interviewed 21 doctors, dietitians, and other healthcare providers about their expectations for how patients’ self-tracking data should be shared and used.

“We’ve heard doctors say more and more that people bring this data into the clinic, and they’re just overwhelmed by it,” says lead study author Christina Chung, a UW doctoral student in Human-Centered Design and Engineering.

“When you’re managing chronic disease or symptoms, day-to-day lifestyle tracking data can be useful, but doctors don’t have a way to use these data efficiently and effectively.”

What kind of data does get attention? Providers who asked patients to keep paper diaries or suggested specific tracking tools often found the resulting information helpful in collaboratively diagnosing triggers or arriving at effective treatments. That was largely because those providers had designed and refined those processes over time to elicit useful information and track the most relevant patient behavior.

But patient-initiated tracking efforts – apps that were suggested by a friend or activity trackers received as birthday gifts, for example – were a different story. The study concluded that, on a whole, the ways that some activity trackers or calorie-counting apps present data are more suited to supporting healthy lifestyles than helping providers make clinical decisions.

“As a provider, you feel pressured because you want to help and interpret the data that people are bringing you, but every format is different and none of the data is validated,” says study paper co-author Jasmine Zia, an attending physician and Acting Assistant Professor in UW Medicine’s Division of Gastroenterology.

In ongoing work, the UW team is exploring ways to make self-tracking data more clinically useful and to help healthcare providers and patients collaborate and engage with it.

The study, “Boundary Negotiating Artifacts in Personal Informatics: Patient-Provider Collaboration with Patient-Generated Data,” won a best paper award and was presented in March at the Association for Computing Machinery’s conference on Computer-Supported Cooperative Work and Social Computing in San Francisco.

Source: UW

Infectious Agents
War on germs takes flight

Engineers at Boeing (Everett, WA) are casting a new light on airplane bathroom hygiene, and that light is deadly — for germs, that is.

The airline designers and builders have created a self-cleaning lavatory prototype that uses a special kind of ultraviolet (UV) light to kill 99.99 percent of germs when the bathroom is unoccupied. The Clean Lavatory system can disinfect all surfaces after every use in just three seconds, and can even help eliminate odors. When combined with touchless features such as a hands-free faucet, soap dispenser, trash flap, automatic lifting toilet lid and seat, and hand dryer, the whole system aims to minimize the growth and potential transmission of micro-organisms.

The patent-pending cleaning system, which will require further study before it can be offered to airlines, lifts and closes the toilet seat by itself so that all surfaces are exposed to a flood of Far UV light during the cleaning cycle. The light bath is activated only when the lavatory is unoccupied. Far UV is different from the UVA or UVB light in tanning beds, and is not harmful to people.

Source: Boeing
ICD-10: Targeting reporting and reimbursement

A panel of experts fields questions on how the industry is adapting to the new coding structure.

It’s official: The ICD-10 launch happened six months ago. It was then that the U.S. healthcare industry joined the rest of the Western world in updating the way patient records are coded for classification and reimbursement. While most in the United States had years to prepare, a grace period instituted by the Centers for Medicare & Medicaid Services allowing for the acceptance of older codes is evidence that many were still in a mad scramble to adopt the upgrade. With six months to go before that grace period permanently expires, HMT sits down with experts Marianne Slight, Senior Director, Clintegrity Product Management, Nuance; Susan E. Belley, M.Ed., RHIA, CPHQ Manager, Clinical Content Development and Outsource Services, 3M Health Information Systems; William Shrader, Sr. Field Client Executive, Allscripts; and Melanie Endicott, MBA/HCM, RHIA, CDIP, CCS, CCS-P, FAHIMA, Senior Director of HIM Practice Excellence, AHIMA, to get their takes on how the ICD-10 transition has been received and what we can expect to see in the future.

Slight: Overall, yes. Most hospital provider clients made efforts to provide ICD-10 education to prep physicians for the increased specificity through clinical documentation improvement (CDI), which helped with the transition. Many Nuance hospital clients took full advantage of our ICD-10 coding boot camps prior to implementation to give coders a basic foundation to code in ICD-10, which definitely helped prepare for the transition and cushion the initial coding productivity loss. We also found that clients who took advantage of our data analytics were better prepared from a coding and clinical documentation perspective.

Since ICD-10 took effect, Nuance Clintegrity coding clients have indicated an increased number of provider clarifications – but over time. These types of coder clarifications will decline as long as coders continue advanced procedure coding system (PCS) education.

Non-acute care providers – clinics, offices, specialists, etc. – were also well prepared for the ICD-10 implementation in their office setting. We have heard reports of various types of failures such as EHR failure, outsourced vendor failure, billing software failure, and clearinghouse issues. While these failures have not been widespread, the impact has been significant for the affected parties.

Shrader: For the most part, providers and insurance companies were ready for ICD-10. While there have been denials related to the new diagnosis codes, the transition has been better than most would have expected.

Endicott: Yes. Implementation seems to have gone seamlessly. I have heard very positive feedback about the relative ease of transition. There should be ongoing provider education to ensure that the most complete documentation is being entered in the health record. This not only enables accurate code assignment, but also ensures quality care of the patient.
HMT: Do you expect claims denial rates will rise once CMS demands more specificity in terms of coding and stops accepting older codes? What can providers do to prepare themselves for the extra scrutiny? Or are we in for another delay?

Slight: There will likely be increased claims denial rates once the CMS ruling expires on Oct. 1. In advance of this, providers should continue to educate, audit, and reinforce the need for appropriate specificity in all appropriate codes. It’s important to get in the habit of documenting and coding in full specificity today – specificity is already a critical component of the revenue cycle for documenting, coding, and reporting outcomes.

We have not heard reports about a potential delay in the CMS enforcement of specified codes.

Shrader: Denial rates will rise for providers who are not keeping current with Medicare and insurance payer policies. Providers will need to review chargemasters for invalid CPT/HCPCS and revenue codes. Continuing education and identifying the denials early on is key to addressing the diagnosis and coding errors.

Endicott: It’s possible we will see an increase in denial rates, but providers have been and should continue to have complete documentation to ensure that the most accurate codes are assigned. The more specificity, the better! An ideal way to help capture more complete documentation is through focused education for professionals within the organization who view the documentation daily.

HMT: We’re seeing reports that some claims are being denied due to a simple error, such as a rogue parenthesis. Is there a way to process these claims with a reasonable level of flexibility?

Slight: While there doesn’t appear to be a significant increase in denials, we are starting to hear that denials are starting to creep up a bit. One Clinctegrity coding client reported about one denial per month, citing “invalid code” when they had submitted a correct and valid code. Initially, there were some reported issues with medical necessity determination and edits that affected certain provider specialties.

Facilities and providers should closely monitor and track all claims denials and determine appropriate action on a case-by-case – and timely – basis to ensure the denial rate does not significantly increase in the next six to 12 months, resulting in lost revenue.

Shrader: It will take a team effort to reduce denials. Healthcare organizations with strong scrubbers can help keep claims clean, including identifying and removing rogue characters. The payer community also bears some of the responsibility to make sure their computer systems remain flexible.

HMT: In general, is revenue increasing since the adoption of ICD-10? If so, can the new coding structure be credited for that?

Slight: Improved documentation will certainly have a positive impact on severity, outcomes, and, in some instances, case mix. This is especially true if these are impacting revenue, SOI, or ROM. Some CDI clients have already seen that better documentation – including specificity on billing codes – helps better reflect the care delivered, which leads to both clinical and financial benefits for organizations.

Shrader: Revenue is not and will not increase as a result of the specificity of the codes. With the increasing level of detail, procedures are grouped in a greater degree of acuity. But, as was the situation with ICD-9, diagnosis will not move to a higher level of reimbursement.

HMT: What steps can providers take to make sure they’re analyzing their claim denials and spotting trends and problem areas?

Slight: Track, track, track! It’s so important to track various key performance indicators (KPIs) pre- and post-ICD-10 implementation – such as days to payment, days to final bill, claims denial rates, and coder productivity – to find any differences, analyze them, and determine the root cause for negative findings. We always recommend using an external coding auditor to validate coding accuracy, claim submission, and clinical documentation improvement opportunities. Following any type of audit services, the organization should always receive a comprehensive report including coding accuracy rate, documentation completeness for ICD-10, and rate of unspecified code usage.

Shrader: First, providers need to ask: Does my procedure meet medical necessity? If not, then they should review for the appropriate diagnosis. Second, providers need to review their payer denials by denial code to identify trends to correct. Third, they should offer ongoing education for practitioners and hospital providers. Finally, providers should have a strong review team and processes to identify potential denials.

Endicott: Providers should have a dedicated professional review the claims denials to look for trends and to analyze whether the denials are due to documentation gaps or coding errors.

HMT: Is there any evidence that private insurers are denying patients coverage more often after the ICD-10 implementation?

Slight: The recent February Healthcare Billing and Management Association (HBMA) survey suggests an increase in the number of private payor denials.

Shrader: It is too soon to tell. However, private insurers have policies in place related to timeliness of filing – some companies require a clean claim to be filed in 30 days or less, whereas Medicare and Medicaid are normally 365 days for a clean claim to be filed.
This shorter timeframe, combined with the complexity of ICD-10, could lead to more denials.

**HMT: Is there a discrepancy between what’s expected from a claim processed by Medicare and Medicaid, as opposed to a private insurer?**

**Slight:** Each state Medicaid program and private payer is able to set their own claims processing rules. These may or may not correlate to CMS requirements.

**Shrader:** It all depends on the contract with the private insurance company, which can affect authorizations, limits on treatment options, requests for additional inpatient treatment days, additional clinical documentation, or review by the provider and the insurance company. For example, some insurance companies require that an insurance authorization be obtained within 24 hours of the private insurance patient being seen in the emergency department, but that is not the case with Medicare and Medicaid.

**HMT: Are small practices showing the same level of success as larger healthcare systems?**

**Slight:** We have not heard of discrepancies based on healthcare system size, although there are reported differences based on specialties. Anesthesia, primary care, and radiology experienced more problems than emergency medicine, pathology, or oncology – which reported no problems. These differences appear to be more related to medical necessity issues for certain types of services rather than size of provider practices.

**Shrader:** Smaller practices, which may deal in fewer diagnoses of illnesses, should have fewer items to focus on, but accuracy is extremely important for them. Larger systems are going to face some issues with providing the additional details to identify the diagnosis.

**HMT: Is the ICD-10 coding structure leading to physicians getting more information about their patients, and is this new information being used to reap any benefits?**

**Slight:** Providers are already able to reap the benefits of the additional documentation available when providing follow-up care to their patients. Some CDI clients have already seen that better documentation helps better reflect the care delivered, which leads to both clinical and financial benefits for organizations.

Once we have a full year of ICD-10 data, we’ll be able to have a better understanding of the benefits. However, it may be a year or longer before we see benefits from additional claims specificity, such as a reduction in requests for medical records from payors.

**Shrader:** Yes, it will as we make progress toward population health and clinical predictive analytics. Identifying the best treatment options for a patient, or similar group of patients, should lead to improved clinical care.

**Endicott:** Anecdotally, I would say the ICD-10 coding structure is helping physicians to get more information about their patients. I haven’t seen any reports on this yet, but with the increased specificity of ICD-10, one of the benefits is improved patient care.

**Shrader:** If physicians take advantage of ICD-10’s specificity when documenting their patients’ diagnoses and conditions, there is no question the more precise documentation will reap benefits. One example is documenting for hierarchical condition categories (HCCs). HCCs are used by CMS to determine reimbursement of Medicare Advantage Plans for their costs in treating patients within a population. We’re also seeing increasing adoption of HCCs by commercial payers; so they are becoming a key focus for many healthcare organizations. HCCs identify diagnoses present in the patient that complicate their care and require more resources to treat. The sicker the patient, as indicated by an HCC, the more expenses that might be incurred – so reporting of HCCs impacts the per-member per-month payment from CMS or a commercial payer.

**Belly:** No, all those “crazy codes” did not muddy the waters for physician providers. Codes such as being “pecked by a turkey” were often bandied about in news articles, but what got lost in the media coverage is that physicians are not required to report these codes. While some states may require that hospitals report “external-cause codes” as they are called, there is no national reporting requirement, and either way, it doesn’t impact physicians. External-cause codes describe injuries caused by an external force and include motor vehicle accidents, accidental injuries, and violent injuries.

**HMT:** In the end, did all of those crazy ICD-10 codes we kept hearing about really muddy the waters for providers?

**Slight:** The so-called “crazy” codes fall under Chapter 20, External Causes of Morbidity (CM), which have little impact to providers outside of emergency department settings. Unless a provider is subject to a state-based external-cause code reporting mandate, or these codes are required by a particular payer, reporting of ICD-10-CM codes in Chapter 20 is not required of the patient at the time of the event, and the person’s status.

**Shrader:** The waters are muddied because reimbursement is attached to the ICD codes. The United States is the only country to correlate ICD codes with reimbursement. The original purpose of ICD was to group specific diseases or ailments. In ICD-9, diseases could be more general with less specificity.

**Belly:** No, all those “crazy codes” did not muddy the waters for physician providers. Codes such as being “pecked by a turkey” were often bandied about in news articles, but what got lost in the media coverage is that physicians are not required to report these codes. While some states may require that hospitals report “external-cause codes” as they are called, there is no national reporting requirement, and either way, it doesn’t impact physicians. External-cause codes describe injuries caused by an external force and include motor vehicle accidents, accidental injuries, and violent injuries.

**HMT:** Is the disease burdens of their patients. One example is hepatitis C. Many physicians simply document “hepatitis C” in the patient’s medical record when their patients actually may have chronic hepatitis C. Chronic hepatitis C is considered an HCC, whereas hepatitis C with no further description is not. In failing to document this additional specificity, neither the disease burden of the patient nor the extra dollars needed to treat this patient are recognized. This will impact reimbursement. ICD-10’s coding structure makes it possible to document disease burden and be paid appropriately under HCCs. This is just one example of the benefits to be gained from ICD-10.
External-cause codes may seem amusing and unnecessary, but they can be very important for public health initiatives. For example, a lot of turkeys died or had to be destroyed in 2015 due to avian flu. Although very rare, turkey-to-human transmission of avian flu is possible. Thanks to the new ICD-10 codes, the CDC can quickly identify, track, and monitor potential disease outbreaks as a result of coming into contact with a turkey.

**Slight:** ICD-11 is now being developed through a continuous revision process through the World Health Organization (WHO) and is scheduled to be finalized in 2018. The U.S. will then need to develop the clinical modification version to meet U.S. specific reimbursement and reporting needs; therefore, ICD-11-CM for the U.S. is still several years – if not many years – away from release.

**Shrader:** ICD-11 will have to wait until we fully understand ICD-10, which has taken our focus for the last five years.

**Endicott:** The WHO website says ICD-11 is due by 2018. Keep in mind that this is the WHO version, and the U.S. must modify it for our particular needs, which will take at least 10 years.

**Belley:** Keep in mind that, after the WHO released ICD-10 in the mid-90s, it took the United States nearly 20 years to adopt it as the national coding standard. Before ICD-10 could be implemented, the diagnosis codes had to be modified and procedure codes had to be created for use in this country. Then there were lengthy industry comment periods before and after CMS initiated the rule-making process. Once the final ICD-10 rule was published in 2009, it took six years for Congress to legislate ICD-10 adoption and establish an official start date – after three delays! I think we can expect a good long time before the U.S. is ready to move to ICD-11, especially if we follow a similar path to what we did with ICD-10.

**HMT:** When do you think we’ll start hearing rumblings of ICD-11?

---

**2016: A year of change for healthcare finance**


It’s safe to say the ICD-10 transition occupied the minds of many throughout 2015, dominating the conversation among healthcare finance professionals. While the buzz around ICD-10 has begun to settle down, other topics in healthcare finance are on the rise. Medicare is enforcing payment revisions and shifting its reimbursement model, and some of the largest commercial payers are questioning their participation in Affordable Care Act exchanges. And analyzing data has become increasingly necessary as many healthcare organizations struggle to improve revenues. While the impact of ICD-10 is still playing out, more changes are on the way, and health organizations will begin to uncover new areas to improve overall efficiencies and quality of care in 2016.

**Medicare gets ‘hip’**

One area of significant change involves Medicare making mandatory payment revisions for hip and knee replacements, moving toward a bundled payments model. Since knee and hip replacements are among the most common – and costly – procedures Medicare pays for, the service is starting with these and planning to expand to other operations in the future. This impacts the facility, the surgeon, and any person responsible for the patient’s care within a 90-day period after the surgery. Providers and facilities must start advancing the way they coordinate to improve patient care in order to operate in this new healthcare arena, and these mandatory bundled payments are a big step closer to a pay-for-performance reimbursement model.

**The ACA: Will it be OK?**

Additionally, as UnitedHealthcare, the largest commercial payer in the country, talks about plans to pull back on its offerings through the public Affordable Care Act exchanges, it opens up several questions for the rest of the industry. To which providers will the hundreds of thousands of affected UnitedHealthcare customers move? What if they don’t seek coverage elsewhere? How will the volume of other vendors be affected? These types of inquiries led to an initial drop in stock prices. Should other payers follow United’s lead, there may be negative, long-term financial impacts to providers, patients, and stockholders of insurance exchange companies.

**Data = Reduced costs and improved quality**

Also in 2016, healthcare professionals will become more data driven as a direct result of the ICD-10 transition. It’s never been more important for healthcare professionals to keep their sights set on data to optimize financial performance by reducing care costs and improving care quality. Looking further ahead into 2016, healthcare professionals should compare patterns and volumes before ICD-10 with current analytics. Healthcare providers must leverage this information to make data actionable and increase revenue. They need to compare the length of time it takes to process charges and get claims out the door to get reimbursements back into the system.

Additionally, improving physician documentation will help greatly with improving the financial performance and care quality of the organization by reducing readmissions, length of stay, and other facets of the patient encounter. If all continues to go smoothly, the remainder of 2016 will give way to improvements in revenue and patient care due to changes in the healthcare landscape.

**HMT**
Five steps to promote accuracy in the wake of ICD-10

Every one of us has come face to face with the conundrum of speed versus accuracy. Do you tend to work quickly, thus ensuring completion of the task at hand, or do you maintain a more cautious pace that pays off with greater accuracy? In the typical environment where providers treat more patients and more complex cases, either choice can feel like a tradeoff.

Since Oct. 1, the ICD-10 transition has put even more pressure on healthcare teams, from clinicians to front-office and revenue cycle staff. Especially during these initial months following the ICD-10 launch, providers must strive to avoid two types of ICD-10 errors. First, they must pay careful attention to coding, ensuring it matches clinical documentation and meets specificity requirements. Second, they must do their best to avoid any coding errors, such as selecting inaccurate codes or not meeting medical necessity requirements. These errors can impede cash flow for weeks or even months. As the healthcare industry adapts to ICD-10, five steps can help providers achieve greater accuracy:

1. Foster the right environment. The stress and anxiety that naturally accompany change will already have teams on edge, which can lead to errors. By establishing the expectations that ICD-10 isn’t a race, and staff won’t be expected to keep the same pace as they did with ICD-9, leadership can foster an environment where accuracy trumps speed. Encourage team members to take time as needed to ask questions, check each other’s work, and simply focus on getting things done the right way the first time. Tell coders and physicians you know queries will increase; you’d rather have them spend the extra time to ensure clinical documentation is not only accurate but also meets specificity requirements. Allowing for minor delays now can safeguard against serious payment delays later. As everyone becomes more comfortable with ICD-10, speed will follow.

2. Ask your clearinghouse for support. Clearinghouses have a better vantage point for spotting common problems that can impact cashflow. Ask whether your clearinghouse has aggregated rejections over its entire client base to pinpoint typical problems. If your clearinghouse sends regular and as-needed reports to update clients regarding payer issues, make sure team members are on those distribution lists.

3. Pay close attention to front-end processes. During a period when claims-related productivity is slower, patient collections can generate much-needed revenue. If you haven’t done so already, adopting a proactive strategy for reviewing patient estimates and accounts receivable can help ensure your organization’s financial health. Involve front-end staff in reducing rejections and denials by creating a team that reviews reasons for rejections and denials, and implements ways to potentially eliminate these caused by office staff.

4. Have a financial safety net. As the United States continues to recover from one of its worst economic recessions, providers are under great pressure to sustain their financial health and, in some cases, simply make payroll. Having a line of credit or other financial safety net can give you peace of mind during the initial weeks of the transition. Even if your organization has implemented a thorough ICD-10 transition plan, certain factors are out of your control. For instance, if a large percentage of your claims comes from a certain payer that has problems, your cashflow may suffer.

5. Measure your way to success. If payers identify errors and issue denials during their first adjudication, they can shorten providers’ payment delays. In this scenario, however, providers aren’t told about recurring problems and won’t be aware of trends in inaccuracies. Such systemic issues can lead to greater, long-term revenue problems that occur when mistakes are repeated and should be circumvented as quickly as possible. If you don’t regularly track revenue cycle key performance indicators (KPIs) such as denials, rejections, and A/R by payer, it’s a great time to start. You’ll be in a much better position to know exactly how the transition is impacting your practice’s financial health, and you’ll identify problem areas much more quickly.

It may be tempting to push your team to submit claims at a pace close to the one they maintained with ICD-9. During the initial months of ICD-10, however, this goal may be unrealistic and can create a stressful environment where accuracy suffers. In the overall scheme of your organization’s tenure, it’s a relatively short length of time to allow for adjustment to the new coding system. As our industry learns to speak this complex new language, teamwork and patience can help providers weather the pressures and reap ICD-10’s benefits. HMT
ICD-10 :::::::::

RelayHealth Financial, one of the industry’s largest clearinghouses, recently disclosed denial-rate data for more than 262 million claims processed between Oct. 1, 2015, and February 15, 2016. Of the $810 billion in claims processed using RelayHealth Financial revenue cycle management solutions, just 1.6 percent have been denied. This denial rate is expressed as a percentage of claim dollars that were initially denied for ICD-10 impacted denial categories in relation to dollars billed on remitted claims. This rate reflects only the denial categories of Authorization/Pre-Certification, Medical Coding, Medical Necessity, and Untimely Filing. This denial rate has remained unchanged since November and represents approximately $12.9 billion in denied claims since Oct. 1.

“The good news is that we’re not seeing a marked increase in claim denial rates when it comes to ICD-10, and there is heightened interest in denial management and prevention,” said Marcy Tatsch, Vice President and General Manager, Reimbursement Solutions for RelayHealth Financial, in a company statement. “The bad news is that as many as one in five claims is still denied or delayed within the normal hospital and provider revenue cycle world, which can mean a dip of as much as 3 percent in a hospital or health system’s revenue stream. While it’s important to keep monitoring those KPIs that are monitored on RelayHealth Financial’s Denials Dashboard, healthcare providers should now ramp up their broader denial prevention and management efforts.”

To help providers understand and navigate the challenges surrounding strategic denial prevention and management, RelayHealth Financial now offers ReduceMyDenials.com, an online resource that features best practices and operational considerations, with links to case studies, white papers, and a webinar focused on helping providers reduce and manage denials.

Checklist

**CMS: Assess your ICD-10 KPIs**

Now that you’ve made the switch to ICD-10, you can look for opportunities to analyze your progress. By tracking and comparing key performance indicators (KPIs), you can identify and address issues with productivity, reimbursement, claims submission, and other processes.

First, establish a baseline for each KPI. You’ll want to compare KPIs from before the Oct. 1, 2015, transition date with KPIs from after the transition date. Ideally, you either already have pre-ICD-10 baseline data for some KPIs from your clearinghouse, or you can generate baseline data from your practice management system, EHR, or other health IT system.

If you’re a provider in a small practice, you might not have routinely used or tracked KPIs in the past, so you may need to start by developing a new baseline with current data. Work with your billing and coding staff to see what data are already available in your systems, reports, and records. Check for data available from outside sources such as clearinghouses, third-party billers, and system vendors.

Once you’ve established baselines for your KPIs, compare the data pre- and post-Oct. 1, 2015, to put your current KPIs in context. Tracking KPIs can help you detect problems and identify opportunities for improvement.

**CMS KPI checklist for ICD-10**

- Days to final bill
- Days to payment
- Claims acceptance/rejection rates
- Claims denial rate
- Payment amounts
- Reimbursement rate
- Coder productivity
- Volume of coder questions
- Requests for additional information
- Daily charges/claims
- Clearinghouse edits
- Payer edits
- Use of ICD-10 codes on prior authorizations and referrals
- Incomplete or missing charges
- Incomplete or missing diagnosis codes
- Use of unspecified codes
- Return to Provider (RTP)/ Fiscal Intermediary Shared System (FISS) Volumes
- Medical necessity pass rate

**TIP:** Tracking KPIs separately for each payer will assist in isolating the root cause of issues.

In the United States, half of all adults have one or more chronic conditions. Obesity rates are at an all-time high, and chronic disease continues to be one of the most costly burdens on the healthcare system. As a practicing physician for over 20 years, it did not take long for me to realize how many preventable deaths happened on a daily basis in our country. Seeing a 40-year-old father being rushed into the emergency room due to a heart attack is a painful experience to be part of; however, these types of situations have always pushed me to research, examine, and innovate solutions to keep people healthier.

In more recent years, I have started to turn to health apps to help me guide my patients toward a healthier lifestyle. As I’ve investigated this space from a physician’s perspective, I’ve found that health applications have a tremendous amount of potential and the ability to transform one’s health. Unfortunately, they cannot all be trusted.

With 165,000 health apps available to consumers today, there is an overwhelming amount of options for consumers and physicians to test. From years of experience researching this market, I’ve realized there are ways to cut through the crowded space. According to an IMS Institute for Healthcare Informatics report, over 50 percent of health apps have narrow functionality, which limits their ability to help people make sustainable health behavior changes.

This report discusses the seven main dimensions of app functionality. These include:

1. Inform: Provide users with educational health information through text, photos, and videos.
2. Instruct: Provide clear instructions so the user can easily navigate and utilize the app.
3. Record: Capture data that the user enters, as well as data that is pulled in through wearables.
4. Display: Display users’ data through aesthetically pleasing and easy-to-read graphs and charts.
5. Guide: Provide context and guidance around users’ data to help them understand how to make sense of the information.
6. Remind/Alert: Provide reminders to the user to help them remember to stick to their goals.
7. Communicate: Allow the app to be a form of communication between a user and their physician.

Do health apps work?
This physician says, “Only some.”
Each of these dimensions is fundamental to a health app created for more than gathering user data. True success stems from educating users with health information, providing guidance and context to their data, and helping them more accurately communicate about their health and wellness with their physicians. No single dimension is more important than the others, which drives the need for consumers and physicians to utilize multifunctional apps.

Throughout the last couple of years, I have started to integrate health apps into my practice. I find that they help my patients become more aware of their decisions and actions, and it helps me to better understand them as individuals. A health app paints a picture for me of their everyday lives, helps me understand what motivates them, and allows me to identify patterns in their behaviors.

I am an advocate for treating each patient based on their specific needs and refraining from a one-size-fits-all treatment approach. For instance, when I see a patient who eats extremely unhealthy and does not work out at all, my recommendation may be to simply cut a single soda a day from their diet and walk for 5 minutes a day. Those may be small recommendations, but they are realistic and will work for that individual. In this case, a health app has the ability to provide constant reminders to my patient, as well as offer other lifestyle and health tips for them to test.

On the other hand, if I see a patient who diligently walks 10,000 steps a day and eats a balanced meal, but continues to struggle with weight gain, I may recommend more strenuous tactics. Adding strength training to their routine, for example, would help them build and maintain the lean skeletal muscle that leads to a loss of fat. There are health apps that are able to create personalized strength-training workouts that include video demonstrations of each exercise. I find the videos to be especially beneficial, since people often do not know the proper strength-training exercises and form to maximize their workout.

A study in the Journal of Medical Internet Research found that users of a multifunctionality health app were able to:

- Reduce their body weight by an average of 13.5 lbs;
- Reduce their waist circumference by 7.2 cm;
- Lower their systolic and diastolic blood pressure; and
- Attain significant increases in HDL and VO2 max.

These kinds of significant results prove that health apps have the ability and potential to truly transform people’s lives and guide them to a healthier lifestyle. Many of my patients have seen tremendous success by engaging with health apps. Of course, I am very particular about the health apps I trust enough to recommend. They must be multifunctional, but also based on extensive scientific evidence and medical research to truly reach this kind of success.

REFERENCE
1. http://www.cdc.gov/chronicdisease/overview/
The beginning of a new era

Telemedicine is growing with no signs of slowing down. The advent of smartphones, private video capability, and the growth of the Internet have all contributed to a rise in telemedicine. The global telemedicine technologies market, including hardware, software, and services, was valued at $17.8 billion in 2014, and is predicted to grow at a compound annual growth rate of 18.4 percent from 2014 to 2020. Why is telemedicine growing? Though reasons are multifactorial, three factors play a large part: cost, convenience, and access.

1. Cost
Telemedicine consultations cost less than clinic visits. Whereas a visit to an urgent care clinic can cost upward of $200 for an upper respiratory infection, a telemedicine consultation can cost many times less. It has been estimated that employers in the United States could save up to $6 billion per year by providing telemedicine technologies to their employees. Money drives markets, and the telemedicine industry is not exempt.

2. Convenience
The market gave us the drive-through, pizza delivery, and Uber. Consumers love convenience, and hate long waits. Telemedicine offers a convenient way to reach providers without having to go to the dreaded doctor’s office. Experts estimate that almost 75 percent of all doctor, urgent care, and ER visits are either unnecessary or can be handled safely and effectively over a phone or video.

3. Access
In the current broken healthcare system, fee-for-service incentivizes providers incorrectly. Patients are seen every 10 minutes, and schedules have to be fully booked (even double-booked) to ensure practice viability. With little access to same-day visits (one of the reasons for the rise in retail clinics), patients are unable to get timely care. Telemedicine, with its on-demand capabilities, disrupts the cumbersome status quo.

TIP OF THE ICEBERG
Despite hundreds of millions of dollars invested in telemedicine companies like Teladoc, Doctor on Demand, MDLive, and SnapMD, telemedicine is merely the tip of the iceberg. The iceberg represents an entirely different industry – a true moonshot that lurks beneath, waiting to be mined. The ability to receive the full spectrum of medical services instantaneously, regardless of location, is the real opportunity. Today’s telemedicine is just the beginning.

Currently, telemedicine primarily consists of phone or video, giving providers the ability to see and hear patients from anywhere. The future involves a great deal more – an entire virtual medical ecosystem designed to deliver healthcare in completely new ways. We are headed toward a new medical practice era that won’t just allow us to communicate with providers from anywhere, but also get physical exams, lab studies, imaging, and medication delivery. A new type of virtual medical practice is emerging, and will eventually be integrated with current models of healthcare.

OVERCOMING TELEMEDICINE LIMITATIONS
Telemedicine today has several limitations, including a general lack of examination capability, conflicting state laws, and challenging reimbursements. These obstacles, however, are already being negotiated.

MEDICAL EXAMINATIONS
No doctor’s visit is ever complete without an...
Until recently, telemedicine examinations were limited to expensive kiosks (like the failed HealthSpot) and large telemedicine carts. MedWand, a Nevada tech startup, recently introduced the world’s first portable medical device that allows patients to be remotely examined and vitalized, turning any computer into a virtual clinic. Another startup, AliveCor, can turn a smartphone into an EKG and upload results directly to clinicians. Adding such diagnostic devices to existing telemedicine platforms multiplies the power and reach of telemedicine far beyond today’s capabilities.

STATE LAWS
When it comes to the practice of medicine, technology always outpaces tradition. Tradition, however, is deeply rooted in society. Unlike most countries where clinicians are licensed nationally, medical licensure and laws in the United States are compartmentalized state by state. Telemedicine presents an interesting dilemma with its ability to erase geographic boundaries when providing medical services. Much of the issue is due to an inability to examine patients, fear that out-of-state providers will converge on in-state patient panels, and possible reluctance to embrace a new digital era in medical practice. As telemedicine technology, familiarity, and market adoption improve, it is predicted that state laws will eventually catch up to telehealth practices.

TELEMEDICINE REIMBURSEMENTS
In most cases, reimbursements for telemedicine visits are less than those of office visits. This is beginning to change. In New Mexico, for example, both visit types are reimbursed similarly for the same medical condition. As healthcare moves toward value-based systems (direct primary care, accountable care organizations) over existing fee-for-service systems, the enhanced access afforded by telemedicine gains attraction. Introducing medical examinations into telemedicine will correspondingly increase reimbursements. Tomorrow, a remote telemedicine provider will be able to “see” a patient, listen to lungs, and obtain vitals via a device like the MedWand. If a provider were to perform the same examination during an office visit, it would be logical that reimbursements would be similar.

WHAT THE FUTURE HOLDS
Any consumer service that evaporates physical barriers tends to not only become popular, but adopted into mainstream culture. Television allows us to see cities beyond our homes. Telephones allow us to speak with others around the world. With telescopes we can look at galaxies beyond our own. With telemedicine, we can now eliminate vast distances when providing medical services. Telemedicine will eventually become a part of regular medical practice. The future of telemedicine isn’t just coming; it’s already here.

REFERENCES
1. www.researchandmarkets.com/research/qn3csn/global

The MedWand portable telemedicine device allows doctors to examine a patient remotely.
Phone it in: A perfect storm takes telemedicine to new heights

Telemedicine is by no means a new concept, but several forces currently at play stand to make 2016 the year adoption of this model of remote care hits its tipping point. Advances in mobile technology, such as cutting-edge photo capabilities and secure messaging, make smart devices viable tools for telemedicine. These advances are resulting in a more accessible and user-friendly experience, thereby helping to make the use of telemedicine more attractive to both the patient and the physician. The massive wave of adoption of these technologies has also made smart mobile devices all but ubiquitous in the average household and provider organization. Couple technological advancements with increasing reimbursement options for telemedicine, and we have the perfect storm in place to take telemedicine from an obscure practice to the mainstream of healthcare in the United States.

Growing adoption of modern electronic health record (EHR) systems is helping to bridge the data gap challenge previously presented with telemedicine. The ability to tightly integrate a modern telemedicine system with a data-driven EHR system makes for the easy capture of patient data – whether that capture occurs in-person or remotely. New and innovative ways to efficiently capture patient data in a structured manner during a telemedicine visit ensure that nothing is lost along the way and that the data can be tracked and utilized in the same manner, as though the visit occurred in-office. This will also allow physicians to effectively monitor outcomes over time and ensure that telemedicine aligns well with the growing shift toward value-based care and quality reporting.

Improved camera technology on smartphones and tablets also helps make telemedicine a more attractive option for patients and physicians. This is particularly true for highly visual specialties, such as dermatology. The ability to effectively bring a physician into the living room of a patient through the sharing of high-quality photos further mimics the benefits and efficiency of an in-person visit. It is very likely that the convenience of being able to virtually check with a physician on a condition like a recurring rash will lead many people to manage their care in a more effective manner, rather than waiting until it’s too late or bearing the inconvenience of geographic constraints.

Whether it is blood pressure or sugar monitors, we are also seeing significant advances in mobile medical devices that have the potential to easily interface with consumer smart devices. These technologies will only further serve to bridge the gap between in-office and telemedicine patient visits.

These technological advancements come at an ideal time, as some providers continue to see decreasing reimbursements and experience increased regulatory pressure to provide more cost-effective care. Physicians whose patient base may not be covered for telemedicine can immediately accept cash payments for virtual visits, changing in the $30 to $100 range for virtual visits that are simply paid out of pocket. Many patients could be willing to pay a premium for the convenience of a telemedicine visit.

Reimbursement issues have traditionally been one of the top barriers for telemedicine adoption. Over the last year, we have seen more private plans, as well as the Centers for Medicare & Medicaid Services (CMS), begin to get a better handle on telemedicine. Aetna, Cigna, UnitedHealthcare, and Medicare are just some of the important players that are beginning to support different forms of telemedicine coverage for select members. The majority of current plans have focused primarily on the lowest hanging fruit, in terms of patient populations covered, such as those in rural populations. There are several indications from a number of other payers, both private and federal, that point to a strong desire to provide wider coverage for telemedicine in the coming years. Private physicians who adopt telemedicine services with a built-in revenue stream can expect to retain more of their patients who may otherwise seek telemedicine treatments from alternative providers. This continuity of care is better for the patient’s health – and the practice’s bottom line.

Innovative healthcare professionals will increasingly turn to telemedicine as an added way to serve patients more effectively and expediently – and to ensure they have more in-person time to dedicate to patients with orphan diseases or more complex diagnoses.

While physicians have to observe, understand, and evaluate new technologies before adopting them into their practices, there is a major opportunity at hand for key players in the healthcare industry. From a payor perspective, telemedicine visits may result in reduced healthcare spending, with fewer more expensive in-person visits for conditions that can be handled virtually. From a provider perspective, telemedicine visits can grant more timely access to patients and an additional revenue stream. We have finally hit a point where telemedicine is not only viable, but also very attractive. That is why I expect that 2016 will be the year that we see adoption rates rise and the practice become more widely used than ever before. HMT

By Michael Sherling, M.D., MBA, Chief Medical Officer and Co-Founder, Modernizing Medicine
VMI: The no-data-footprint path to mobile security

Healthcare data is under assault. Criminal attacks on healthcare organizations jumped 125 percent between 2010 and 2014. And this was before several leading insurers, including Anthem, reported staggering breaches last year.

This surge in criminal hacking has coincided with an explosion of mobile devices in healthcare – a trend spurred by bring-your-own-device (BYOD) policies in hospitals. BYOD makes good sense. Mobile devices enable medical practitioners to forward patient records, share test results, and communicate with each other in real time, improving the speed and quality of healthcare delivery.

But these devices are notoriously vulnerable to remote attackers and physical hackers, leaving patients and healthcare organizations at the mercy of bad actors bent on exploiting protected healthcare information (PHI) for financial gain. In a study last year by the Ponemon Institute, 96 percent of respondents reported at least one security incident involving a lost or stolen device. It is clear that old attitudes and strategies have failed; it’s time for a new approach.

The stakes are undeniably high. Stolen PHI, which includes medical records, claims, and billing information, is already being monetized on the “Deep Web’s” shady black market. According to Bankrate, identity thieves who compile full dossiers of personal information that include healthcare data, known colloquially as “kitz,” can sell them for more than $1,000. Of even greater concern, medical records are far more sensitive than any other type of data; they cannot be reissued like credit cards, reimbursed like bank accounts, or adjusted like credit scores.

Despite the enormous consequences, the healthcare industry has been slow to recognize and step up to the challenge – in no small measure because mobile security vendors have struggled to find solutions. First-generation approaches involved wrapping in-house mobile apps in a security layer that would ostensibly keep hackers at bay. This might have gained more traction if not for a critical shortcoming: The technology does not protect third-party apps commonly used within the healthcare industry, such as electronic medical record software.

The security industry then gravitated to containerization, in which a series of custom-made healthcare applications is encapsulated within a container with its own runtime environment. But like wrapping, this technology did not enable users to move beyond a limited menu of predetermined apps. Of greater concern, neither wrapping nor containerization could safeguard data if a lost or stolen device were to be physically hacked or remotely compromised through exploitation of vulnerabilities. Physical attacks on mobile devices have been largely left unaddressed by vendors. Biometric sensors, such as fingerprint readers, made these attacks even more successful by enabling hackers using image-capture applications and 3D-printing technologies. It is quite an irony that the airplane mode usually accessible from the locked screen of a smartphone or tablet is all an attacker needs to prevent remote wiping of the device or locating it using iCloud. Essentially, airplane mode, paired with the fingerprint sensor attack vector, yields all device-based security solutions ineffective.

It’s time to recognize that these prevailing mobile app security models simply haven’t worked. Instead, we must focus on securing data rather than devices – an approach that taps into (and borrows from) one of the most powerful software trends of the last decade: virtualization. We commonly think of virtualization as a cost-effective way to boost efficiency and agility. But virtualization, which makes it possible to run multiple operating systems and applications on the same server at the same time, provides powerful built-in security advantages.

This is the premise behind virtual mobile infrastructure (VMI), a technology that provides mobile device users secure access to all their business mobile environment applications. VMI creates a mobile environment (operating system, apps, and corresponding data) that runs on a remote server. Because VMI enables ephemeral sessions, all apps and data remain on the remote server rather than on the device, so criminals or state-level actors cannot harvest any data from a lost or stolen phone, tablet, or laptop.

There are other advantages to VMI. Users can access corporate mobile apps regardless of the device they are using, and they can still use their phones or tablets for personal use without having to deal with restrictions imposed by their employer. VMI is the only way to manage mobile business applications with any certainty, without giving away the keys to the kingdom.

A number of security vendors are moving in this direction. Citrix, the on-demand software maker, has re-rendered Microsoft Windows and corresponding apps for mobile. Others such as Nubo, Hypori, and Avast have taken a different approach by virtualizing mobile apps for mobile platforms, resulting in a more elegant and streamlined user experience.

Critics correctly note that virtual mobile infrastructure is not a panacea when users are offline. That’s because enabling offline access would require caching data on smartphones, tablets, and laptops – a solution that would defeat the key security advantage of VMI. But this is a non-existent issue in all but the most remote locations. We cannot afford to let isolated instances keep us from adopting technology that is a major step forward in safeguarding hundreds of millions of people’s healthcare data. Let there be no mistake: Cyberattacks that yield healthcare data will only increase in the years to come unless we move quickly to adopt VMI.
BYOD done the smarter way
Three BYOD strategies health organizations should adopt to protect sensitive health records.

With medical records worth 10 times more than a credit card number on the black market, health organizations need to develop a secure bring-your-own-device (BYOD) strategy to keep cybercriminals at bay. According to the latest account from the Identity Theft Resource Center, 40 healthcare breaches have taken place so far this year, exposing over 1 million records.\(^1\) To help put these breaches into context, consider this: Health organizations have suffered more breaches this year than banking, education, and government organizations combined. This is due to the increase in patient monitoring systems and wearable/smart devices, which create more data but also more opportunities for hackers to steal sensitive information.

With the increase in data generation and data leaks, the industry has to adapt and evolve. For example, the Department of Health and Human Services is building a healthcare industry cybersecurity task force in an effort to improve preparedness for cybersecurity threats affecting the healthcare industry. In addition, HIPAA compliance standards are becoming stricter, with enforcement and penalties coming more swiftly.

In response, health organizations need to create and enforce secure BYOD policies for protected health information (PHI) and avoid hefty fines. Healthcare organizations, namely their executive teams and IT departments, need to be proactive about cybersecurity. With the emergence of smartphones, tablets, and wearables in healthcare, organizations need to think like a hacker when it comes to establishing a secure BYOD initiative. Below are three considerations health organizations and providers should prepare for when adopting a BYOD program.

1. **Provide employee training for cybersecurity awareness**

According to a recent PwC report, three-quarters of large organizations experienced an employee-related data breach in 2015.\(^2\) Sadly, half of the most damaging breaches were the result of human error. Unintentional data breaches can be largely mitigated through consistent and comprehensive employee training. There are a number of benefits inherent for employee cybersecurity training. Obviously, it helps decrease the likelihood of careless errors when handling sensitive data. Second, it reinforces for employees that management lists data security as a top priority, and therefore employees should as well. Third, it instills in employees the value of protecting patient and employee information, namely, better training means fewer breaches and safer, happier customers. Lastly, employee training sends the message to staff that management values their staff and is willing to provide them with the tools they need to be successful.

To start, training should specifically highlight cybersecurity awareness, as hackers are continuously developing new methods of stealing sensitive data. The training should include topics such as email security best practices, as well as the importance of strong passwords and secure methods of handling sensitive information. In addition to periodic training sessions, an ongoing support system from IT that has the full support of management ensures that employees have the resources and education required to make smart decisions when handling PHI.

2. **Develop and enforce policies for using dated applications**

Dead or stale apps – apps that are no longer supported by developers but still sit on your personal device – present an open door for hackers. Thankfully, there are precautions organizations can take to protect the increasing amount of sensitive data that resides on a mobile device. For starters, employees should regularly update apps when newer versions are made available. Alternatively, if employees no longer need or use a particular app, encourage them to delete it from their device.

IT departments can also establish and enforce a mobile app whitelist to manage which apps are...
safe and approved for employees to download. The intention of the app whitelist is to help control how healthcare workers access PHI on mobile devices and desktops. If properly followed by healthcare employees and enforced by IT, the whitelist will ensure that users never jeopardize PHI by using questionable, insecure, or infected apps to access patient records – regardless of whether they are stored on the device or within the organization’s network.

“Rather than focusing on the strength of an encryption algorithm, organizations may be better served focusing on where encryption keys are held and managed.”

3. Ensure secure storage and transfer with ownership of encryption keys

Whether information is being stored on and accessed via smartphones, laptops, tablets, or wearables, organizations should be aware of the risks of inadequate encryption. Managing and maintaining encryption keys is necessary for ensuring data housed on these devices remains out of the hands of cyber criminals. Rather than focusing on the strength of an encryption algorithm, organizations may be better served focusing on where encryption keys are held and managed. Should a healthcare organization entrust their encryption keys with a third-party, public cloud storage provider who is obligated to decrypt and share PHI should intelligence or law enforcement agencies ask for it? As you would never share your house key with a stranger, the same concept should be applied with encryption keys.

A private cloud storage solution is the best way to guarantee exclusive ownership of encryption keys and therefore the best option for maximum protection and control over a healthcare organization’s data. Private cloud solutions also enable IT departments to establish their own security parameters rather than having to adhere to those established by the cloud storage provider.

With a costly data breach occurring almost every day, it’s imperative that health organizations invest considerable effort in developing adequate policies, training, and solutions to ensure PHI is properly and safely stored, accessed, and shared. It only takes one attack for an organization to incur heavy costs and damage to their reputation. Health organizations need to develop, monitor, and continually enhance BYOD policies and internal systems to safeguard PHI so that they can stay a step ahead of the next cyberattack. HMT

REFERENCES

BYOD adoption is hampered by lax security

By Michael Keoni DeFranco, CEO, Lua

As a growing number of medical providers use their smartphones and tablets to improve the speed and quality of healthcare delivery, this explosion of portable and largely unsecured devices is leaving patients and healthcare organizations vulnerable to hackers and cyber criminals bent on exploiting patient data for personal gain.

The reason they’re targeted is because the vast majority of healthcare providers haven’t taken the necessary steps to ensure patient data is encrypted. This turns what should be a win-win situation into a lose-lose one; patients could have their data exploited, healthcare organizations face massive fines, and everyone loses if security concerns prevent healthcare providers from taking advantage of the latest technologies to improve the delivery of care.

The threat to healthcare data is real. Some 112 million medical records were compromised in 253 incidents last year – an astounding toll that highlights the vulnerability of our personal healthcare information (PHI), which can be used for insurance fraud, identity theft, or to make money through extortion.

Healthcare providers across the country have struggled to strike the right balance between innovation and security. The upside to portable devices is obvious, and a growing number of providers allow and encourage staff members to use mobile devices, often of the BYOD variety, to share critical test results, consult with colleagues, respond to code blues, and provide emergency notification.

But a recent Sophos white paper reports that only 29 percent of tablets and smartphones used in a healthcare setting are encrypted, and just 22 percent of wearable devices are encrypted. That compares with an encryption rate of 66 percent for healthcare PCs and 70 percent for servers.

These numbers should concern all of us because they highlight the degree to which patient data is vulnerable. But equally alarming is evidence that concerns over data security are turning some providers away from the use of mobile messaging. According to a recent study by secure mobile messaging provider Spok, BYOD usage among healthcare providers actually fell from 88 percent of respondents in 2014 to 73 percent in 2015 in large part due to concerns surrounding data security.

The challenge is made all the more difficult because many legacy technology providers often do not support secure communications via staff members’ personal devices. And finally, healthcare providers have not moved on this issue because they have been required to, until now.

This is because according to HIPAA, encrypting health data is “addressable” rather than “required.” This means healthcare groups must assess whether encryption is “reasonable and appropriate” given an organization’s systems, policies, and practices. But given the rapid growth in use of portable devices and the growing number of thefts of those devices, the Department of Health and Human Services Office for Civil Rights is now signaling that it expects to see healthcare organizations adopt secure mobile messaging platforms to protect PHI. Failure to do so could now result in penalties of as much as $50,000 per violation.

The OCR is expected to soon show its enforcement teeth once again as it implements its next round of HIPAA compliance audits during the next several months.

But the risk of fines pales in comparison to the other forms of damage that a data breach could cause. Not only would patient privacy be compromised, a severe breach could tarnish a healthcare organization’s reputation. Most importantly, failure to overcome this issue could have a long-term impact on the healthcare system’s ability to innovate and improve the speed and quality of life-saving care. HMT
Risking a breach

Risk assessments protect practices against breaches – and OCR fines.

A

ssessing risk factors – such as high blood pressure or cholesterol – alerts physicians to potential heart health problems in their patients. Similarly, conducting a security risk assessment (SRA) enables small and medium-size medical practices to identify where they are vulnerable to a major threat to their own wellbeing: data breaches. A data breach can be catastrophic for both a practice and patients, as medical identity theft can cause tremendous harm.

Imagine this: A patient walks into a medical office, and there is a sign that says, “We do not protect patient information.” What do you think most patients would do? They would walk out. Patients are very concerned about the privacy and security of their information these days. They expect and assume that their providers are taking care of this.

The SRA is not only an essential first step in protecting a practice from damaging breaches. It also remains a requirement for complying with the Security Rule under HIPAA.

Yet many physicians’ offices with 20 or less employees still do not fulfill HIPAA requirements for preventing electronic protected health information (ePHI) from falling into the hands of identity thieves. These medical practices have resisted the idea that their small operations could be worthwhile targets for data thieves. But now that hackers have become more sophisticated, and patient information is a hot commodity on the black market, hackers are hitting doctors’ offices of all sizes.

Medical practices may also be fined if they do not report a breach properly – as can happen when a laptop is stolen. While doctors may contend their laptops contain no information that identifies patients, the OCR (Office of Civil Rights) takes a different view, which can be summed up as “guilty until proven innocent.” The OCR assumes that laptops used in medical settings have ePHI on them, and if the device cannot be recovered, it is difficult to prove otherwise. The OCR’s position can be bolstered by statistics showing that six out of 10 HIPAA data breach violations can be traced to lost or stolen laptops.

Fortunately, the twin challenges of fending off data thieves along with potential OCR audits can be met by taking a proactive approach to securing sensitive patient information, starting with an SRA.

Here are the main elements of a comprehensive risk assessment designed to show an organization how it is protecting its data, and what gaps it needs to fill:

1. Identify and document all the ePHI repositories

Medical practices often operate under the assumption that sensitive patient data is stored in electronic health records (EHRs). But that assumption leaves them wide open to thieves who can pick that information off emails, Excel spreadsheets, Word documents, letters sent to patients, PDFs with scanned explanations of benefits, or even ultrasounds and MRIs. That is why the risk assessment must begin with efforts to determine exactly where all ePHI is stored.

2. Identify and document potential threats and vulnerabilities for each repository

Once the repositories of patient information are identified, the next question naturally follows: How is it being protected? The risk of fire or flood that could destroy servers must be taken into account. And the theft or loss of laptops, thumb drives, cell phones, and other mobile devices cannot be overemphasized as a threat to data security.

3. Assess current security measures

Existing security measures could include encrypting data and backing up computers. It is also necessary to question employee policies in this section of the risk assessment. For instance, are termination procedures in place to stop terminated employees from accessing patient information?

4. Determine the likelihood of threat occurrence

Once the location of patient information is determined and potential vulnerabilities are identified, the likelihood of an actual breach needs to be ranked as high, medium, or low. It may be more likely, for instance, that an unprotected ground-floor office could be broken into than one located in a high-rise with around-the-clock security. Then again, it could be easy for employees to lose cell phones or other devices containing patient information, so that threat might be ranked as “highly likely.”

5. Determine the potential impact of threat occurrence

If a physician loses a laptop with 1,000 patient records on it, the impact on a practice could be huge. Look for devices that can store large amounts of patient data. Those have the highest potential impact if they are compromised.

By Art Gross, President and CEO, HIPAA Secure Now!
6. Determine the level of risk
The combination of the likelihood of a threat and its impact determines the level of risk. Devices that can easily be lost or hacked and also contain lots of ePHI have the highest level of risk.

7. Develop a work plan
Current security measures must be increased if they are not adequate to lower the level of risk revealed in the assessment. Practices need to develop a work plan – the document that accompanies the SRA to identify gaps and remediations. For example, the practice may be missing signed agreements with business associates. The work plan should note the issue and assign the task.

8. Document the findings of the SRA
This step may be the most crucial because HIPAA compliance demands documentation. In the event of an audit, examiners are going to want to see documented proof that the medical practice is actually doing what it claims to be doing.

9. Train employees
Employees are the first line of defense against hackers and cybercriminals. They also pose a large security threat. Employee medical identity theft is one of the largest causes of HIPAA violations. You need to “trust” but “verify” that your employees are not taking data. They must be aware that you are checking on them. You also must train them to recognize phishing attempts, phone scams, and rules for accessing public Wi-Fi, social media posting, etc. in order to avoid inadvertent breaches.

To develop a proper SRA takes someone who has an understanding of HIPAA, IT, and cybersecurity, and can manage the process. Often, the practice will settle for a staffer who lacks the qualifications, or forgo the SRA altogether and simply answer security questions on a checklist that has been found on the Internet. That is not a proper SRA, and HHS/OCR has said so in writing.

If the practice lacks an experienced employee who can perform the SRA, it should follow the advice of CMS and outsource the project to a qualified HIPAA compliance expert.

Taking the time and devoting the resources needed for a comprehensive risk assessment is the best strategy for defeating data thieves and satisfying auditors. Outsourcing your SRA or your HIPAA compliance needs does not have to be expensive. Nor does it have to be time consuming. External resources are available to help organizations through the confusing maze of HIPAA compliance and regulations. Small practices can achieve HIPAA benchmarks in a cost-effective and time-effective manner, allowing them to concentrate on what matters most: their patients.

---

Holding data hostage
Protection against ransomware requires up-to date operating systems.

By James Savage, Founder and President, Concurrency

Hollywood Presbyterian Medical Center recently went public with news of a so-called ransomware attack that had paralyzed its computer systems for 10 days. The episode affected patient care, including some emergency patients being sent to other hospitals. Ransomware is a form of malware in which rogue software code effectively holds a user’s computer hostage until a “ransom” fee is paid.

“It’s no different than if they took all the patients and held them in one room at gunpoint,” said California State Senator Robert Hertzberg, who has introduced legislation to make a ransomware attack equivalent to extortion and punishable by up to four years in prison.

What’s unusual here is not the event – but rather that the hospital went public. Usually, organizations try to cover over such attacks. In this case, the hospital paid $17,000 to the hackers in order to get its systems up and running again.

What are the most common vulnerabilities that enable hackers to pull off something like this? How can healthcare organizations such as hospitals, nursing homes, and clinics protect their systems – and patients?

A little-recognized fact of information technology security is the significant role that operating system software plays in keeping attackers at bay. Modern operating systems incorporate sophisticated identity and access management (IAM) technologies that – when properly implemented – greatly reduce the threat of unwanted access.

Without modern IAM tools in place at the operating system level, organizations must cobble together access restrictions for each individual software application. That approach almost universally leaves security holes. If you were to ask a skilled information technology consultant how long it would take him or her to break into a computer system running an outdated operating system and create a new, unauthorized network administrator account, you’d probably hear “less than a week.”

Unfortunately, this is the normal state of affairs. Healthcare organizations in particular have had to focus heavily on patient records and updated coding, often at the expense of the basic “blocking and tackling” needed for effective technology management. They are not alone. The dirty little secret in the IT world: Organizations leave themselves open to threats – and potentially to extreme peril, as in the case of Hollywood Presbyterian – by delaying updates to their operating systems.

It’s odd that such a basic need is so often ignored, but not especially surprising. Since the dot.com crash in the early 2000s, there’s been a general malaise among IT departments concerning their perception of the significance of operating system maintenance for both client devices and servers. We estimate that a typical organization is two to three major operating system iterations behind.

In healthcare especially, there is almost nothing more important than security. Recent news reports indicate that a person’s credit card record might be worth about $20 on the black market, whereas his or her health record is worth $60. Security matters to patients during episodes of care as well as away from the hospital if records are compromised.

Events at Hollywood Presbyterian should serve as a wake-up call for business leaders to ensure system software and configurations stay up to date. While it’s also essential to train staff to recognize abnormal activity and threats, the single greatest impact on an organization’s security is an ongoing commitment to keep operating systems current and properly configured.
Interoperability

Future looks bright for connected health tech in U.S. hospitals

The 2016 HIMSS Connected Health Survey unveiled at the HIMSS Annual Conference and Exhibition in Las Vegas paints an optimistic picture surrounding the emerging trend of connectivity within the healthcare ecosystem. With more than 50 percent of respondents indicating their hospital currently uses three or more connected health technologies, the high adoption rates (and other supportive statistics in the report) underscore the growing importance these technologies play in the hospital setting.

Respondents found that the technologies implemented within hospital settings positively impacted capabilities to communicate with patients along with the ability to deliver a higher standard of care. In addition, 69 percent of respondents whose hospitals are utilizing mobile-optimized patient portals indicated that the attention to a mobile environment expands the capability to send and receive data securely. Given these positive impacts, it’s understandable why healthcare organizations are looking to increase their investment in these tools for the future.

The survey was conducted in partnership with the Personal Connected Health Alliance (PCHA). Insights are reflective of 227 IT, informatics, and clinical professionals in U.S. hospitals and health systems with regard to their organization’s current and future use of connected health technologies. Currently, 52 percent of hospitals indicated the use of three or more of these technologies, including:

- 58 percent mobile-optimized patient portals
- 48 percent apps for patient education/engagement
- 37 percent remote patient monitoring
- 34 percent telehealth – audio-visual fee for service
- 33 percent SMB texting
- 32 percent patient-generated health data
- 26 percent telehealth – concierge service

Nearly half (47 percent) of respondents indicated their hospitals are looking to expand the array of connected health technologies they use. Another 5 percent of respondents expect their hospitals to become first-time users of at least one of the connected health technologies outlined in this report. The commonly cited technologies they plan on adding involve telehealth (concierge service) and patient-generated health data solutions.

Download the complete 2016 HIMSS Connected Health Survey at www.himss.org/2016-connected-health-survey.

Policies and Procedures

AHIMA: Information governance is key to HIT

Information governance (IG) is a business and strategic imperative for healthcare and essential to successful health information technology (HIT) initiatives such as electronic medical record (EMR) implementation, data analytics, privacy and security, and data sharing, according to an American Health Information Management Association (AHIMA) presentation at the HIMSS16 Conference and Exhibition.

In their presentation, “Taking a Pulse on Information Governance in Healthcare,” AHIMA’s Deborah Green, RHIA, MBA, Executive Vice President, Chief Innovation and Global Services Officer, and Kathy Downing, Senior Director IG Advisors, said IG is central to the successful implementation of reliable electronic data and information as well as improved usability. Based on analysis of 500 organizations that participated in AHIMA’s IG Pulse Rate Web-based tool to assess IG maturity, the presenters shared insights on how IG can assure successful implementation of organizational initiatives such as EMR implementation.

“Information, rather than technology infrastructure, must be at the center of EMR implementation,” Green said. “Planning and implementation of EMRs under an information governance framework assures that the focus is the information and includes input from clinicians and clinical workflows, ensuring the user’s needs are met. We cannot lose sight of the fact that the information is the reason organizations invest in infrastructure and systems improvements.”

A commitment to IG must be organization-wide and requires the adoption of principles to guide decisions about how information is governed, said the presenters. Organizations should assess their competency levels and establish goals for competency levels needed given their strategy, mission, role, and resources.

In addition to IG Pulse Rate, AHIMA has developed two other offerings in a suite of IG products and services. IG Health Rate is its newest product to help organizations assess and score their maturity in adopting IG, and IG Advisors offers expert consultation with a variety of IG services including implementation services and gap assessment. AHIMA also offers a toolkit sharing best practices and resources for starting and implementing IG within an organization.
HIMSS16 Product Picks

ACO performance monitoring and operational management
Designed and built in consultation with Scottsdale Health Partners, a physician-led clinical integration network and accountable care organization in Arizona, the MSSP Management application helps ACOs gain the maximum savings available from the CMS MSSP program. This solution seamlessly integrates data into the reporting and monitoring workflows of all user types while preserving central oversight of quality measurements and scoring. Key features include real-time MSSP dashboards to track and improve clinical quality measures, a common interface for data capture and data sharing, customizable workflows, drag-and-drop file management, and advanced data integration. Orion Health

Eliminate tedious manual image transfer
Ricoh Electronic Data Exchange (Ricoh EDE) is a subscription-based service that helps improve the overall patient experience by transferring protected data, including clinical photography and images, to an intended destination. This workflow solution enables healthcare facilities to capture, store, and manage protected information, whether structured or unstructured, within an EHR or enterprise content management (ECM) system. Ricoh EDE helps providers eliminate tedious manual image transfers, image identification, and human error – ultimately boosting overall accuracy, efficiency, and productivity. At HIMSS, this solution was demonstrated leveraging Ricoh’s healthcare camera. Ricoh

On-demand marketplace for healthcare talent
With the need for qualified healthcare human resources spiraling upward, MyConsultQ allows healthcare employers to benefit from the skills of freelance consultants without compromising on financial and management efficiency, or on quality of service. Healthcare organizations of all types and sizes – from delivery systems to payers to vendors and many other support services – can rely on the on-demand online MyConsultQ marketplace to fill both temporary and permanent positions with the best executives, information technology professionals, project managers, and physicians. Instead of wading through traditional recruiting and hiring processes, which are notoriously time and labor intensive, healthcare employers can access resources that provide the same level of expertise as the top consulting firms at a fraction of the cost through MyConsultQ. Best of all, organizational leaders can rest easy, knowing that these resources are thoroughly vetted, having gone through a five-point screening process. MyConsultQ

Caradigm Intelligence Platform delivers actionable interoperability
Open Exchange is a set of interoperability capabilities available to healthcare providers that use the Caradigm Intelligence Platform (CIP). Open Exchange encompasses a range of interoperability solutions and standards (such as IHE.NET standards, DIRECT, and a REST architecture) to support provider population health initiatives. The big standout feature of this interface engine is that it is able to both ingest and codify data, and then deliver this information to anyone anywhere within the healthcare community. In making Open Exchange available to its CIP customers, Caradigm also announced that it has received certification from ConCert by HIMSS, a testing and certification program that assures secure and reliable transfer of data among EHRs, HIEs, and HIS services providers within and across organizational and state boundaries. Caradigm Open Exchange provides the ability to efficiently exchange information across the healthcare community by leveraging the Authentication, Authorization, Patient Consent, Auditing and Reporting, and Role-Based Access Control features of CIP. Caradigm

Make patient check-in a snap
Touchscreen terminal provider Posiflex is helping to bridge the gap between healthcare hardware and software through a partnership with Clearwave. Clearwave is the provider of a state-of-the-art patient self-check-in system, a cloud-based self-service technology that runs on the Posiflex XT-series of touchscreen terminals. The Clearwave self-serve medical check-in system improves workflow, streamlines the check-in process, and increases patient engagement. Additional benefits include improved patient satisfaction and overall experience. Clearwave

Enhance medication ordering in CPOE
FBD OrderSpace is a Web-based software tool that enables hospital informatics teams to customize the medication ordering content in CPOE systems to optimally reflect the characteristics of the institution’s patient population and preferred practices. The solution also tracks medication orders over time, so that customizations are recorded in an auditable change history record that all designated users at a hospital can view. Users can also review FBD updates to medication ordering content and compare these to their local customizations, ensuring all new clinical evidence is taken into account. Once customizations are made and published, they are stored in a custom file and incorporated into the HIS in a seamless fashion during a regular update process. The McKesson Paragon electronic health record is the first to deploy FBD OrderSpace, with the goal of making ordering medications easier and more satisfying for clinicians. FBD (First Databank)

Senior living redefined
As part of a five-month pilot, 60 residents at Ohio Masonic Home’s Springfield campus tested a new technology solution combining software from Reemo and smart connected devices. By combining the Samsung Gear S2 smartwatch and Samsung’s SmartThings connected home technology, Reemo’s software enables the older adults at the assisted living facility to perform everyday household tasks with a flick of the wrist. Using simple hand gestures, they can operate lights, locks, thermostats, and other appliances with SmartThings plugins. Meanwhile, the solution enables Ohio Masonic to remotely monitor residents’ health and well-being. Staff can view biometric and behavioral data in real time from an online dashboard, while Reemo also tracks data and alerts the organization to potential problems and troubling trends. Reemo, Samsung
Public Health
Medicaid data exchanged in real time

The Mississippi Division of Medicaid (DOM) has become the nation’s first Medicaid agency to send and receive clinical data in real time with a health system using the Epic electronic medical records system. The agency worked with MedeAnalytics and Epic to provide Medicaid data to the state’s largest provider of care to Medicaid patients, the University of Mississippi Medical Center (UMMC). The connection is powered by healthcare analytics specialist MedeAnalytics.

This accomplishment means that UMMC doctors can now review the electronic medical history of DOM patients, allowing them to make better-informed decisions quickly.

MedeAnalytics established and standardized DOM’s Medicaid Enterprise Master Patient Index (EMPI), a multi-year initiative that serves as the core identity management service to allow easy management of a patient’s longitudinal record.

MedeAnalytics first helped DOM lay the groundwork for the project by creating an EMPI and single patient identifier in 2014.

They analyzed and de-duped more than a decade of medical records from 2.3 million Medicaid beneficiaries. The process resulted in a unique longitudinal patient record for more than 750,000 Medicaid and Children’s Health Insurance Program (CHIP) beneficiaries.

MedeAnalytics also worked with DOM to make the data accessible through a Medicaid provider portal, then began the next phase of the project, which was standardization of the Medicaid clinical EMPI to support a clinical data interface with external stakeholders.

Today, DOM and UMMC can interact to share Consolidated-Clinical Document Architecture (C-CDA) patient summaries through UMMC’s Epic EHR. MedeAnalytics expects to receive approximately 3,500 clinical inquiries per day from UMMC and will send the corresponding clinical summaries for Medicaid beneficiaries in response.

Acute Care
UTMC speeds development of inpatient EHR

Cloud-based services provider athenahealth is expanding its relationship with the University of Toledo to develop athenahealth’s electronic health record with the University of Toledo Medical Center (UTMC) for providers who cross ambulatory and hospital care settings. The University of Toledo Physician Group has been an athenahealth client since 2014.

Development at UTMC will focus heavily on creating a seamless physician and nurse user experience for the academic medical center. Research will focus on identifying areas needing improvement for acute care workflows and then addressing them.

athenahealth announced the extension of its services into the acute care setting in early 2015 with the acquisitions of RazorInsights and webOMR. athenahealth will convert the technology acquired in these transactions into a comprehensive, cloud-based service within athenaNet for hospitals of all sizes and complexities.

The new service, athenaClinicals for Hospitals & Health Systems, will be an extension of the company’s existing EHR, athenaClinicals, ranked Best in KLAS for ambulatory care.

The effort will fully implement the cloud across all inpatient and outpatient environments.

Behavioral Health
New data sets get integrated

Minnesota Community Healthcare Network (MCHN), an alliance of five behavioral health organizations, is on its way to establishing interoperability among its member companies to enable care teams and clients to share healthcare information in real time.

Through the Minnesota Accountable Health eHealth Initiative, and in partnership with Hennepin County Medical Center and Hennepin Health, MCHN created the “Mission Hennepin Community Collaborative” with the goal of using health information exchange to support communication and care coordination between MCHN members and the Hennepin Health System, an accountable care organization (ACO) consisting of four partners: Metropolitan Health Plan, Hennepin County Medical Center, the Hennepin County Human Services and Public Health Department, and North Point Health and Wellness Center.

MCHN received State Innovation Model (SIM) grant funds through the Minnesota Department of Health for this project. Beyond funding, MCHN needed to address the complexity inherent in bringing together clinical data at scale, including the ability to manage consent, security, and establishing interoperability across its members’ different IT environments.

MCHN enlisted RelayHealth, experienced in interoperability and the service provider for CommonWell Health Alliance, to help it establish connectivity throughout its complex environment. This new connectivity, powered by the RelayHealth vendor-neutral and SaaS-based solution, will acquire and normalize critical information from across care settings and provide access to aggregated information about an individual at the point of care. Establishing interoperability within the whole community using a solution that can scale across the entire health system will help MCHN build a foundation for more coordinated care.

Decision Support
Evidence-based treatment drives down sepsis rates

Sepsis is the deadliest condition treated in hospital critical care units, claiming approximately 258,000 lives in U.S. hospitals every year. At an estimated $20 billion annually, it is also the country’s most expensive condition to treat. Because the risk of death increases every hour the condition goes untreated, early identification is crucial to improving outcomes. That’s where solutions like Wolters Kluwer’s POC Advisor, a cloud-based decision support platform for the diagnosis and treatment of sepsis, can truly prove lifesaving.

POC Advisor, which can handle patient data from disparate clinical systems, leverages patient data within the EHR using real-time analytics and automated surveillance to deliver early sepsis alerts and treatment advice to clinicians via mobile devices and clinical portals. The solution reduced sepsis mortality by 53 percent in a pilot study at 941-bed Huntsville Hospital in Alabama in 2015.

In December 2015, Halifax Health, East Central Florida’s largest healthcare provider, decided to partner with Wolters Kluwer to adopt POC Advisor into its clinical workflow. Halifax, home to Florida’s largest emergency department (ED) with more than 116,000 emergency visits annually, will be the first to adopt POC Advisor for use in the ED.
Solutions

Foster provider, payer, consumer collaboration

Cognizant Health TranZform is a new digital healthcare platform developed with technology from Orion Health that aims to help consumers make more informed decisions about the cost and quality of their care, while enabling healthcare providers and payers to drive greater levels of consumer engagement and operational efficiency. This secure, cloud-based utility enables different industry healthcare stakeholders to easily interact with each other and consumers across the care continuum. Data from multiple systems, including payer data from Cognizant’s TriZetto payer core administration platforms, data from physician practice management systems, and other healthcare ecosystem platforms, can be integrated with EHRs to provide an improved customer experience and drive new solutions. Cognizant, Orion Health

Three in a row for long-term-care market leader

PointClickCare, a cloud-based software platform used by more than 10,000 facilities for the senior care continuum, was recognized in January by KLAS Research as the definitive Best in KLAS segment winner in Long-Term Care for 2015/2016, marking the solution’s third consecutive win in the category. This suite of fully integrated applications is powered by an interoperable, mobile-friendly, and regulatory-compliant EHR and revenue cycle management platform, helping customers connect and collaborate within their care network, achieve and demonstrate higher quality outcomes, optimize financial performance, and simplify their regulatory burden. PointClickCare

Bridge the gap between EHR systems and big data

AndonCare, a first-of-its-kind cloud-based care management analytics solution created by SSERACT and Quammen Health Care Consultants, proactively guides clinicians and other staff members to navigate all aspects of care as it unfolds. With this solution, important data is not just housed in an EHR but is fully utilized to move care in the right direction, leveraging just-in-time intelligence to help meet compliance requirements, identify and use best practice standards, improve patient safety by proactively addressing potential hazards, reduce length of stay, and significantly enhance overall patient care delivery. AndonCare will be piloted in late spring 2016 by a variety of healthcare organizations and will be generally available in fall 2016. Quammen Health Care Consultants, SSERACT

Get real-time analytics at the point of care

Based on one of healthcare’s largest datasets and integrated with nearly 600 EHR platforms, Data Diagnostics offers patient-specific data analyses that can be ordered individually on demand by clinicians at the point of care, within their existing workflow prior to or during a patient consult. Each report identifies specific actions the physician may take to improve the patient’s care according to quality, risk, utilization, and other metrics, including criteria that can affect financial payment for health services under value-based reimbursement models. Data Diagnostics is part of the new Quanum brand of Quest Diagnostics healthcare information technology solutions. Quest Diagnostics

Ranked tops for oncologists and hematologists

iKnowMed has been named the top-ranked EHR platform for oncologists and hematologists for the fifth year in a row by Black Book Rankings. iKnowMed was recognized for its superior focus on meeting the unique needs of community-based oncology practices. Implemented in more than 620 sites of care nationwide and used by more than 1,600 providers, iKnowMed EHR and iKnowMed Generation 2 received top rankings in 12 key performance areas, including support and customer care, best-of-breed technology and process improvement, and strategic alignment with client goals. Integrated modules include a patient portal and solutions that address patient engagement, data analytics, inventory and purchasing management, and revenue cycle reporting. McKesson Specialty Health

Clinical researchers offered ‘patient registry in a box’

InterSystems has partnered with Pulse Infoframe to facilitate clinical research and population health studies. Leveraging the InterSystems HealthShare health informatics platform for interoperability between clinical research systems and EHRs, physicians and researchers can easily capture, organize, model, store, and share clinical research data through a secure, Web-based application. Healthie, the Pulse platform, is a cloud-based clinical business intelligence solution that connects specialists from around the world in self-configuring networks and aggregates data from both mobile and stationary devices. Together, the technologies provide up-to-date tracking on how patients are doing. InterSystems, Pulse Infoframe

INDEX OF ADVERTISERS

<table>
<thead>
<tr>
<th>Advertiser</th>
<th>Web Site</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>AHIMA</td>
<td>IGAdvisors.com</td>
<td>IFC</td>
</tr>
<tr>
<td>athenahealth</td>
<td><a href="http://www.athenahealth.com">www.athenahealth.com</a></td>
<td>2-3</td>
</tr>
<tr>
<td>CIOX Health</td>
<td>cioxhealth.com</td>
<td>5</td>
</tr>
<tr>
<td>McKesson</td>
<td><a href="http://www.mckesson.com">www.mckesson.com</a></td>
<td>BC</td>
</tr>
<tr>
<td>PDI Communication Systems Inc</td>
<td><a href="http://www.pdiarm.com">www.pdiarm.com</a></td>
<td>15</td>
</tr>
</tbody>
</table>

This index is provided as a service. The publisher does not assume liability for errors or omissions.
Four steps to a winning accountable care strategy

Population health management in our communities can reap big rewards.

By Reed Liggin, Vice President, Client Development, Clinicals Enterprise, athenahealth

It’s an historic moment for population health. As the baby boomers become Medicare beneficiaries and chronic disease skyrockets, the Centers for Medicare & Medicaid Services (CMS) has announced a monumental shift toward value-based care by 2018. Hospitals and health systems are being asked to manage patients’ comprehensive (and often complicated) care needs, as well as take on accountability for the associated cost.

Major health systems have been recognized for their commitment to value as part of the Healthcare Transformation Task Force. But I believe that community hospitals have a large role to play in this transition, for the same reason that regional hospitals and healthcare institutions have always been known for their quality and affordability.

Many community hospitals are successfully navigating the transition to accountable care, despite the perceived cost and complexity that have discouraged others. No organization can afford to invest in the system modifications that a transition to value-based care requires without a strong strategy. Managing the care of a population with coordination and purpose is no small task. It’s important to have a solid plan in place to meet quality thresholds, maximize revenue, and reduce costs in order to ultimately realize profit. With the right technology and visibility into operations, community health systems can improve the care experience.

Here are four scalable population health management strategies for community hospitals that can help them thrive as they transform their care.

1. Get to know your data

The right technology tools are critical weapons for helping providers under accountable care engage more meaningfully with their data. Cloud-based services that integrate clinical and financial data can put network-wide insight at one’s fingertips and make it actionable. This data must include claims, administrative, and clinical data in a single view. The right business intelligence tool can reveal where patients in an accountable care organization (ACO) receive care, how much it costs, and how high quality it is. Select a tool that not only lets you monitor performance across your network but also identifies areas for intervention – for individual patients and across the system – and handles reporting.

2. Manage referrals to stem out-migration

Referrals directed internally help maintain retention rates, support coordinated care, and streamline data collection for payers. Keep your providers aware of in-network options and make network-wide scheduling tools available to all staff to directly schedule appointments while the patient is still in the care setting. Educate patients about why local treatment options are effective, convenient, and cost effective – particularly compared to the larger (and more prestigious) academic medical centers in the area – and make access to that care easy via two-way communication tools like a patient portal. Managing your referrals will build patients’ familiarity with the high-quality care your institution offers in network and will build patient loyalty – a virtuous cycle. Of course, very few ACOs can provide absolutely all the care its patients need. This is especially true for community-based hospitals, which often need to refer out of network for acute and specialty care. Always refer to high-quality, competitively priced institutions. To do this, providers must have convenient access to data about location, quality, and cost of providers out of network. Consider partnering with care sites that can give favorable terms.

3. Grow your panel

Grow your panel by bringing in new patients, engaging inactive patients, and attributing all existing ones correctly. Providers must understand that they, like the health system, are financially accountable for their panel and are responsible for bringing inactive patients in for treatment. Your providers should know precisely who in their panel needs what care and what chronic diseases they live with. Engage patients who need office visits, screenings, or chronic disease management via targeted outreach. Ensure that existing patients are accurately attributed to your contract and, for the Medicare Shared Savings Program (MSSP), included in CMS data. This is especially important for patients who may have recently aged into Medicare.

4. Implement care plans to close gaps

Care management programs are expensive but essential to any population health strategy. Find out where gaps in care exist amongst your quality measures. Cloud-based services should be able to keep the latest quality management rules up to date, without a software update or additional cost, and align patient data to the specific quality measure an ACO is responsible for. Stratify your population and identify opportunities for intervention. You need an accurate representation of disease burden in a population to do this. Clinical documentation must be comprehensive and capture the full complexity of a patient. Smart coding features ensure that historical coding for each patient won’t fall off the diagnosis in the most recent encounter. Create care plans to address gaps, and take appropriate action. Patients with more than one chronic condition account for most costs and offer the best opportunity to reduce utilization. Properly segment your patients to focus resources effectively – not just by condition, but by whether their condition is under control.

Healthcare is hungry for value. Population health management holds many of the answers. No matter what a community health system’s motivation for participation, accountable care requires a fundamental shift in thinking.
TO BE CONTINUED...

JUNE
- Cloud Computing: broadband backbone
- Top C-suite innovators
- Getting to know your patient populations
- Reducing claims errors and increasing reimbursements
- The Internet of Things and the care cycle

Health Management
TECHNOLOGY
The Source for Healthcare Information Systems Solutions

subscribe or renew your subscription now:
www.HealthMgtTech.com/subscribe
Congratulations on being named a CIO Superstar, Pam.

Health Management Technology made it official, but we’ve known it all along.

We are proud to be partnering with Western Reserve to elevate the role of IT and help deliver on their vision of improving the delivery of safe, high quality health care with improved patient satisfaction.

“We have a strong, collaborative relationship with McKesson. They share our vision for clinical excellence.”

Pam Banchy
R.N.-BC, PMP, CHCIO, CIO and Vice President
Clinical Informatics and Transformation
Western Reserve Hospital and Health System