IN SEARCH OF THE EHR’S DESIGNATED RECORD SET
If there’s one thing our customers all have in common, it’s the look of confidence when they know they’re assigning the right code using the TruCode Encoder. And you can feel this confident, too.

Visit our booth at AHIMA to learn how TruCode presents critical information at the point of coding for a streamlined workflow that allows you to more quickly and accurately assign codes.

Plus, don’t miss our session presentation, Clinical Validation & Preventing/Managing Denials: What Is Your Process, at 2:20 p.m. on Tuesday, September 17, at the HIM Expert Theater, D1 Andersonville.

Win a Lunch & Learn built just for you! Stop by booth #2316 for your chance to win an accredited Lunch & Learn customized just for your team. You pick the topic. You pick the lunch. We’ll do the work and your team will get the credits. See you at AHIMA!

WWW.TRUCODE.COM
WHEN YOU PARTNER WITH CODING EXPERTS:
SUCCESS IS ONE STEP CLOSER

COMPLIANCE AUDITS
Designed to identify outliers that impact our partner's coding accuracy, revenue, and data quality, increasing reimbursement opportunities while mitigating risk.

OUTPATIENT, INPATIENT, PROFEE
Experienced coders with over 95% coding accuracy and effective turnaround. YES offers affordable programs to address backlogs, overflow coverage, staffing shortages & coding quality improvement plans.

CODING EDUCATION
Nationally recognized educators and executive team meet with clients on a periodic basis to deliver practical content and coding updates. Over 6000 HIM/Coding professionals have successfully completed our courses.

YES HIM CONSULTING, INC. | INFO@YES-HIMCONSULTING.COM | BOOTH #1923
# Contents September 2019

**Cover**

12  
*In Search of the EHR’s Designated Record Set*  
*By Mary Butler*

### Features

16  
*Data Analytics: The Straight-Lined Labyrinth that Entrapped the HIM Profession*  
*By Ryan Sandefur, PhD, and David Marc, PhD, CHDA*

20  
*Historic State AG HIPAA Filing: An Important Case to Understand*  
*By Iliana L. Peters, JD, LLM, CISSP, and Pasha Sternberg, JD*

24  
*PHI Hide and Seek*  
*By Ken Reiher, MBA*

28  
*AHIMA19: Health Data and Information Conference Guide*

32  
*Unveiling the Illusion of Digital Health Data Security [Sponsored]*  
*By Erin Benson, MA, MBA*

**Departments**

6  
*President’s Message*  
*Collaboration is Key to Leading Through Transformation*

8  
*Bulletin Board*

11  
*Inside Look*  
*New Starts and Transformation Wins*

52  
*Calendar*

53  
*Keep Informed*

56  
*Addendum*  
*New App Gives Patients a Chance to ‘Share This Appointment’ with Caregivers*
Working Smart

34 Lost Data and Its Implications for Litigation
By Ron Hedges, JD

36 Data and Analytics Drive Effort to Curb Opioid Abuse: A Holistic Approach for Health Systems
By Kapila Monga and Harpreet Singh

38 The Danger of Being Connected
By Ty Greenhalgh, HCISPP

40 Developing and Defining a Legal Health Record Policy
Cindy Zak, MS, RHIA, PMP, FAHIMA

Practice Brief

42 Recruitment, Selection, and Orientation for CDI Professionals

Coding Notes

46 Data Mapping of Clinical Terminologies, Classifications, and Ontologies
By James R. Campbell, MD, FACP, FACMI

48 Reporting Social Determinants of Health
By William C. Fiala, BS, MA, CCS-P, CPC, RMA

Quizzes

AHIMA members may earn continuing education credits by successfully completing the following quizzes at https://my.ahima.org/store

22 “Historic State AG HIPAA Filing: An Important Case to Understand”
Domain: External Forces

26 “PHI Hide and Seek”
Domain: Clinical Data Management

50 “Reporting Social Determinants of Health”
Domain: Clinical Data Management

Telling the Story of AHIMA19
Check in with the Journal website for updates from this year’s annual meeting, AHIMA19: Health Data and Information Conference, taking place September 14 – 18 in Chicago, IL.

Slideshow: The Day in Pictures
A look back at photo highlights of the day from AHIMA19: Health Data and Information Conference.

Code Cracker
Are there best practices for establishing coding productivity standards? A recent Code Cracker post poses this question in a discussion of emerging trends in productivity standards.
While Working Full Time - 100% Online

If you’re looking for career growth in the healthcare information management field, earning your master’s degree in health informatics can open the door for greater advancement and earning potential in a field where job satisfaction is extremely high.

The University of San Diego offers an innovative program that goes beyond the programmatic and technical skills associated with a typical informatics curriculum. At USD, you’ll develop leadership, planning and management competencies while addressing contemporary issues in informatics such as data analysis, cyber security and telehealth.

In just 2 years, you’ll be prepared to take on a leadership role in informatics within your organization.

Learn more and see if you qualify.  [HCInformatics.SanDiego.edu](http://HCInformatics.SanDiego.edu) | 877-927-2476

NEW

Customize your program with a specialization in health data analytics or health care leadership!

37 unit program can be completed in just 2 years

Accredited, top-ranked university

Take one class at a time, completely online

Start in January, May or September
I AM SO inspired by our leaders all across the country. At last year’s CSA Leadership Symposium it was agreed that AHIMA was in a state of decline and that change was needed. It was an amazing moment—one I will never forget and one that really inspired me as a leader of AHIMA.

At this year’s CSA Leadership Symposium, we spent two days discussing AHIMA’s transformation story and its new mission, vision, and strategy for 2020-2023.

The mission, which describes our purpose and reason for working in HIM, is, “Empowering People to Impact Health.”

The vision is, “A world where trusted information transforms health and healthcare by connecting people, systems, and ideas.”

AHIMA’s strategy represents the steps we intend to take to meet our new vision. Our new strategy should result in three outcomes:

1. Advance and advocate for the creation and use of trusted information across the evolving healthcare continuum.
2. Shape the health information profession by growing the influence and competitiveness of health information skillsets.
3. Drive strategic transformation and renewed growth to make AHIMA a great organization to partner with and a great place to work.

Each attendee received a coin inscribed with the mission statement. In a powerful moment, we each held our coin high as we pledged our commitment to move AHIMA forward to renewal and innovation.

Jan Bazow of FORTIS Leadership spoke at the symposium, emphasizing key characteristics of leaders working in 2020 and beyond. At the top of the list was the ability to collaborate. As Grace Whiting Myers said in her first president’s address in Chicago in 1929, “The group brings together all the excellence of many individuals, raises it to a high plane, and gives it a large outlook embracing great possibilities.”

Myers understood even then the importance of collaboration and that bringing a group together could harness unbelievable possibilities. We can still do that today by coming together as one voice, one group, and one profession working together to do the best for our organization.

Bazow asked each of us to come to the microphone and choose one word that reflected each person’s wholehearted commitment to leading. It was deeply moving to see the openness and undying support for our profession and AHIMA as each person stepped up and shared words such as “love,” “grace,” “excitement,” “calm,” and “energy.”

My word was “accountable,” which demonstrates my commitment to make sure that AHIMA continues on the path of renewal and innovation. With the support of our members and leaders, we can make our vision a reality.

This year has not been easy. AHIMA has had to overcome internal challenges and external disruptors as we have moved through our transformation process. While some of these challenges have been difficult, they have made us stronger and given us more energy to achieve our vision for the future. I hope you will join us as we move forward in our transformation.

Valerie Watzlaf (Valerie.watzlaf@ahima.org) is vice chair of education and associate professor at University of Pittsburgh.
Health information management (HIM) solutions aren’t created equal. If your CAC and CDI technology doesn’t deliver what you expected, it’s time to consider a different approach.

Start with a truly integrated platform for CDI and coding teams. Power it with clinically intelligent, patented NLP. Let the technology automate documentation review and pinpoint the gaps that need improvement. Get documentation right upfront, so you can get coding right the first time, and make a positive impact across your organization.

Discover how much more you can achieve with the Optum® Enterprise CAC and CDI 3D Platform.

Learn more at [www.Optum360.com/enterprisecac](http://www.Optum360.com/enterprisecac)

Download a copy of our new NLP white paper. Natural language processing (NLP) is helping to transform the revenue cycle. But not all technologies are created equal. Learn the five attributes of a top-performing NLP engine.

- [optum360.com/nlpwhitepaper](http://optum360.com/nlpwhitepaper)
- 1-866-223-4730
- [optum360@optum.com](mailto:optum360@optum.com)
- Follow us @Optum360

© 2019 Optum, Inc. All rights reserved. WF1337231 07/19
WHO Group Discusses ICD-11 Transition Planning

By Sue Bowman, M.J., RHIA, CCS, FAHIMA

IN JUNE 2018, the World Health Organization (WHO) released a version of ICD-11 to allow countries to begin planning for implementation. This version came 18 years after WHO launched ICD-10. ICD-11 was adopted by the World Health Assembly on May 25, 2019 and will go into effect on January 1, 2022, which is the earliest date any country can implement ICD-11. While there may be a few countries that are early adopters that will implement ICD-11 soon after the effective date, many countries (including the United States) will not be ready to transition to ICD-11 until later.

WHO decided to move forward with development of an 11th revision of the International Classification of Diseases (ICD) for several reasons, including:

- ICD-10 is outdated both clinically and from a classification perspective
- Several chapters needed substantial structural changes
- Necessary changes could not be handled under the normal ICD-10 updating mechanisms
- An increasing need to operate in an electronic environment
- A recognized need to capture more information, especially for morbidity purposes

Historically, the ICD was intended for mortality data reporting, but has increasingly been used for morbidity data reporting applications. Previous revisions of the ICD have responded to these expanding needs in an ad hoc fashion, but ICD-11 was designed to support multiple use cases.

ICD-11 reflects critical advances in science and medicine. It is fully electronic and can be well integrated with electronic health applications and information systems.

Major differences in ICD-11 include the use of extension codes to capture information such as temporality, severity, and anatomic detail, and the introduction of code clustering—the combination of two or more codes in an explicit post-coordinated way to describe a diagnostic entity.

Some chapters and sections in ICD-11 have been restructured (i.e., infectious diseases, HIV, valve diseases) and some diseases have changed location (i.e., cerebrovascular diseases moved from the circulatory to the nervous system chapter).

There are six new chapters: Diseases of Blood and Blood-forming Organs, Disorders of the Immune System, Conditions Related to Sexual Health, Sleep-Wake Disorders, Extension Codes, and Traditional Medicine.

This is an excerpt from “Under the Dome,” an online column from AHIMA’s Policy and Government Affairs team published by Journal of AHIMA. Read the full article and get more legislative insights at journal.ahima.org.
Lawsuit: Google, University of Chicago Misuse Patient EHR Data

An information-sharing partnership between Google and the University of Chicago Medical Center is now the subject of a class action lawsuit alleging HIPAA violations.

As the *Journal of AHIMA* reported in 2017, Google and the University of Chicago Medical Center teamed up to use machine learning and artificial intelligence (AI) to extract predictive capabilities from electronic health records (EHRs) supplied by the medical center. The lawsuit alleges that even though Google and the University of Chicago Medical Center say they de-identified the patient information being shared, Google’s data mining tools can too easily reidentify the patients whose records are being used.

According to the lawsuit, “Google and the university claimed the medical records were de-identified. But that’s incredibly misleading. The records the University provided Google included detailed datestamps and copious free-text notes.”

The lawsuit itself provides no evidence that Google or the medical center has misused the collected data.

Jay Edelson, founder of Edelson PC, a law firm specializing in class action privacy violations against tech companies, however, remains alarmed.

“We believe that not only is this the most significant health care data breach case in our nation’s history, but it is the most egregious given our allegations that the data was voluntarily handed over,” Edelson told the *New York Times*.

The lawsuit also argues that DeepMind, Google’s AI initiative—which was subject to complaints by England’s National Health Service in 2016 for patient privacy violations—could further compromise Google’s promise to preserve patient identities.

**IN BRIEF**

US healthcare industry data breaches are more costly than those in other industries, costing organizations more than $6 million on average, according to an annual report from IBM Security and the Ponemon Institute.

Cybercrime group FIN8 is distributing new malware called Badhatch via phishing emails to penetrate networks.

A new report from the Department of Health and Human Services’ Office of Inspector General found deficiencies in Indian Health Service hospitals’ use of state-run prescription drug monitoring databases.

Eighty-eight percent of respondents to a Black Book Research survey of members of hospital and health system boards admitted to a lack of knowledge about healthcare cybersecurity risks.

**RESOURCES**

**HEALTHCARE CODE SETS, CLINICAL TERMINOLOGIES, AND CLASSIFICATION SYSTEMS, FOURTH EDITION**

https://my.ahima.org/store

This new text from AHIMA Press features up-to-date content to familiarize readers with healthcare’s vast and complex structure of vocabularies. With content that includes ICD-10-CM/PCS, CPT, HCPCS, CDT, SNOMED CT, LOINC, RxNorm, and ICD-11, this text provides students and practitioners in health information management and informatics with an overview of each system.

**SOFTWARE INFORMS NEONATAL INTENSIVE CARE UNIT DECISION-MAKING**

http://astartemedical.com

Developed to address the challenges of early infant nutrition, NICUtrition Analytics from Astarte Medical is an enteral feeding protocol audit and monitoring tool that measures adherence to hospital protocol and correlates it to preterm infant outcomes. The tool helps clinicians make care decisions based on real-time data.

**RESOURCES**

**READER POLL: WHO’S ON YOUR CDI TEAM?**

Which of these describes the CDI team where you work?

- 14% Coders Only
- 57% Coders and RNs
- 29% RNs Only

This reader poll, posted to AHIMA’s Twitter account (@AHIMAResources), was inspired by the cover story from the July-August 2019 issue of *Journal of AHIMA*, “Coders or Nurses for CDI Teams: Why Hiring Both to Collaborate Works Best.” Watch AHIMA’s social media accounts for the chance to weigh in on discussions and polls about articles in this and future issues of *Journal of AHIMA*.  

Journal of AHIMA  September 19/9
What is 2.0? It is a designation for improvement. It is the next level up.

And that’s exactly what we’ve done here with our completely renovated ICD-10 Trainer Academy.

AHIMA’s ICD-10 Trainer Academy 2.0 offers expanded content where coding experts learn to train others to collectively raise quality standards within an organization. Confidently walk colleagues through almost any coding scenario, whether that’s updated basic cases to advanced code-sets.

Our 2.0 curriculum also treats you to new content:

- Computer-Assisted Coding (CAC)
- Mapping
- Clinical Document Integrity (CDI)
- Auditing
- ICD-11

Candidates further learn how to apply proven adult learning principles, which includes an opportunity for a teaching demonstration with valuable feedback.

ICD-10-CM/PCS Trainer Academy attendees receive:

- 3 days of interactive, face-to-face instruction with expert AHIMA trainers
- Pre-Academy online course material to test your current knowledge
- Recently updated ICD-10-CM and ICD-10-PCS codebooks and a student workbook
- Online assessment to validate ICD-10-CM/PCS competency
- 24 CEUS
- AHIMA-Approved Trainer Badge to display in emails, on digital resumes and via social media

Build a team you can trust. Get trained and get going!

AHIMA.org/Education/TrainTrainer
SEPTEMBER IS A time of new starts. At AHIMA, it’s our busiest time of year as we prepare for our annual conference and a host of other fall and winter activities. It’s also a time to look back on the year: two-thirds done, one-third to go!

As you know, this year AHIMA has embarked on a process of transformation, which has meant an intense period of work. We’ve done the daily work of the association while addressing the things that we need to do better and envisioning and building the path forward to the future. While we’re not done yet, I can say there have been some definite wins:

• We’ve unveiled our new mission and vision statements and have embarked on a series of conversations internally and with members about our long-term strategic plan, which will guide AHIMA through renewal and into growth over the next four years. We are having conversations with volunteer groups and leaders to ask them to join us in making the strategy happen. Watch for ways you can get involved to help transform AHIMA.

• We’ve convened thought leaders to help us determine our future direction in key areas of growth such as clinical documentation improvement and data analytics. These groups have been engaging in debates and discussions this year and have sought feedback from the larger membership as they prepare to make recommendations to the Board of Directors. We are grateful to these participants and to everyone who commented. Watch for information on a thought leader group related to consumer engagement this fall.

• We’ve celebrated numerous industry alliances and collaborations that allow us to interact with the healthcare industry in new ways, such as Artifact Health, the American Health Care Association, Area9, and Smart-Brief. We continue to build additional collaborations that will further position AHIMA and our members front and center for transforming health and healthcare.

This month’s Journal explores a variety of policy and practice issues. In our cover story, Mary Butler takes a look at whether the “legal health record” even exists in this digital world—or if this very concept is outdated. Ililana Peters, JD, LLM, CISSP, and Pasha Sternberg, JD, explain why the recent suit filed by 12 State Attorneys General against a company for HIPAA violations is noteworthy in “Historic State AG HIPAA Filing: An Important Case to Understand.” Ken Reiher, MBA, reports on how a panel of privacy experts have worked to mitigate risks associated with hidden protected health information (PHI) in “PHI Hide and Seek.” And Ryan Sandefer, PhD, and David Marc, PhD, CHDA, put the recent discussions about the role of data analytics in HIM practice into perspective and argue that HIM professionals have a critical role to play in leveraging analytics to create better healthcare in “Data Analytics: The Straight-Lined Labyrinth that Entrapped the HIM Profession.”

This month we welcome the industry to Chicago, IL, at a revamped and refreshed annual conference: AHIMA19: Health Data and Information Conference. This issue features an overview of some of the exciting things we have in store. You can follow our conference coverage online at journal.ahima.org and via social media (hashtag #AHIMA19). I hope to see you here in Chicago!
IN SEARCH OF THE EHR’S DESIGNATED RECORD SET

By Mary Butler
WHEN RITA BOWEN, MA, RHIA, CHPS, CHPC, SSGB, broke her elbow while attending an AHIMA event in Baltimore three years ago, she soldiered on through the event but summoned her primary care physician for a telemedicine encounter to determine her treatment. Later, when collecting paperwork for her worker’s compensation claim, she went back to her physician, who had not started or maintained a note documenting the video conference.

“The doctor said, ‘That was a video,’ and I said, ‘You responded, so you’ve got to provide a record of the encounter,’” Bowen says, adding that the physician had to go back and write an account of the video appointment after the fact so that she had something to submit with her claim.

For as long as telemedicine has been a viable and reimbursable avenue of providing healthcare, health information management (HIM) professionals and others have been trying to figure out where documentation of telemedicine encounters belongs. Bowen, who is vice president, privacy, compliance, and HIM policy at MRO, says there’s still more regulations needed to ensure telemedicine is properly coded, classified, and reimbursed.

However, telemedicine’s entry into the medical record, and the electronic health record (EHR) in particular, helps illustrate the way technology is challenging long-held notions about what types of health data constitute the legal health record (LHR) and the designated record set (DRS) in the age of EHRs.

Though it has been years since most providers implemented an EHR system, there is still confusion and a lack of consensus on what constitutes the DRS as required by the HIPAA Privacy Rule, as well as what records should make up a LHR. The LHR is a term that was developed by AHIMA to help providers identify what information constitutes the official business record of an organization for evidentiary purposes. It is also used to document services provided as legal testimony regarding a patient’s illness or injury, response to treatment, and caregiver decisions.1 However, even among HIM professionals, confusion exists about the difference between the DRS and LHR. There is even a debate as to whether the LHR is an outdated term.

“I just think that, historically, the issue has been that some people use the terms designated record set and legal health record interchangeably—and sometimes some people are very distinct about which one they mean. Often, I hear people swap around the definition,” says Lori Richter, MA, RHIA, CHPS, CPHIT, CPEHR, OneCare EHR compliance director at Catholic Health Initiatives.

Further complicating the matter, the US Department of Health and Human Services (HHS) has rightfully been expanding patient rights to their information, including the DRS, putting more pressure on healthcare organizations to respond to release of information (ROI) requests compliantly. Additionally, the recent information blocking proposed rule, issued by the HHS Office of the National Coordinator for Health IT (ONC), which was required by the 21st Century Cures Act, provides a new, nebulous definition for “electronic health information” (EHI) that dictates health data that must be accessible to patients. The scope of EHI defined by the proposed rule is much larger than that defined for providers by HIPAA.

As regulation and technology shift the legal terminology around the DRS and LHR, HIM professionals still must make decisions in the best interest of their patients and their organizations based on these terms.

Designating the Designated Record Set

The best place to start when differentiating between the DRS and the LHR is to look at how they are used. Under the HIPAA Privacy Rule, the DRS designation 45 C.F.R. § 164.524 refers to an individual’s request for access. “The covered entity must permit an individual to request access to inspect or to obtain a copy of the protected health information about the individual that is maintained in a designated record set,” the regulation states.

Functionally, this includes data that includes patient medical and billing records; the enrollment, payment, claims, adjudication, and cases or medical management record systems maintained by or for a health plan; or information used in whole or in part to make care-related decisions.

The existence of EHRs makes it harder for facilities to determine what goes in their DRS for several reasons. For example, content used for decision-making and care of the patient may be external to the organization, such as outside records, diagnostic reports, and patient email exchanges. Organizations also frequently struggle with metadata, since in some provider organizations, it’s the responsibility of the information systems department to retrieve metadata when requested to do so, according to Judy Hoffman, BCRT, CHPS, CHP, CHSS, Regional Privacy Officer - Northwest, Catholic Health Initiatives.
Pending Regulations and the Designated Record Set

The HHS Office of the National Coordinator (ONC)’s much-anticipated information blocking rule, which was required by the 21st Century Cures Act, has drawn concern from AHIMA and other health IT stakeholders due to its lack of clarity and predictability around the definition of “electronic health information” (EHI) as currently proposed.

In comments submitted by AHIMA to ONC, AHIMA stated that “…EHI as currently defined adds an additional layer of complexity in complying with existing definitions in current law, including individually identifiable health information (IIHI), protected health information (PHI), and electronic protected health information (ePHI) as well as state laws that define medical information.”

Lauren Riplinger, JD, vice president of policy and government affairs for AHIMA, says that the new EHI definition dramatically expands the scope of what providers could need to include as part of their DRS.

“Here’s the problem with the DRS. Institutions themselves define what is and what is not considered part of DRS,” Riplinger says. “When you have institutions defining it on an individual basis, that creates variability in terms of patient expectation of what should be there when they request their records. And so as part of our comments, we said, not only should you constrain it [the EHI definition] to the US Core Data Set for Interoperability (USCDI), but create a crosswalk from EHI to the DRS.”

AHIMA is saying, essentially, that the information blocking rule’s definition of EHI is somewhat in conflict with how HIPAA currently defines what a patient has access to.

“It affects it in the sense of the definition of EHI as it currently stands. I think that’s where the challenge is going to be. Are HIM professionals going to be so focused on compliance with DRS that they don’t send everything to the patient [required under the EHI definition]? If we assume that DRS is smaller than EHI and I’m an HIM professional, [what if] someone comes in and requests their record? I do what’s legally required by HIPAA and send them what they requested. Then that patient could go to ONC and say, ‘They didn’t provide me with everything that’s my legal health information—ONC, you need to investigate [instances of information blocking].’ That creates a crazy enforcement challenge, right?” Riplinger says.

The good news for providers is that the regulatory process will take a couple months since ONC will need to consider thousands of comments from AHIMA and other organizations that were unhappy with the rule as it was written. In the meantime, AHIMA is working with the American Medical Informatics Association to encourage policymakers to create a universal definition of a designated record set so there’s predictability for providers, systems, and vendors about what elements should be included.

Her organization chooses to produce and disclose relevant information and records in compliance with applicable laws, court procedures, and agreements made during the litigation process.

“The IT department will provide assistance to HIM and data owners in the search and retrieval process for various systems and data sources. IT representatives will decide the format in which the information will be disclosed, such as paper, ASCII, PDF, TIF, screen shot, mirror copy of data file, or review of material online,” Hoffman says.

Wes Morris, CHPS, CIPM, HCISPP, managing principal consultant for Clearwater Compliance, takes a similar tack.

“I, and many others I have consulted with, take the position that if you’ve included external documents in your record and they are used as part of the clinical decision-making, then they are now a part of your DRS, regardless of the provenance of the original documents,” Morris says.

According to the experts, facilities need to resist the simpler and somewhat blanket approach “that everything housed in the EHR now is part of the DRS,” which some organizations opt to do for simplicity’s sake.

“We have certain communications that are stored in our EHR that do not meet the definition of a DRS,” says Dana De-Masters, MN, RN, CHPS, privacy and security officer at Liberty Hospital, in Liberty, MO. “We do not collect and store a separate formal DRS, for example, we pull information from the EHR based on our DRS policy.

HIPAA requires that the DRS be organized and defined, so healthcare facilities need to create a formal policy around what is included. But determining just what gets included in the DRS can be a challenge—especially in the digital world, where there is more information than ever.

Lorraine Fernandes, RHIA, principal and founder of Fernandes Healthcare Insights, sees this as a major concern for providers—data is created and stored in many different places for data analytics purposes and population health.

“I hear people talking about, we need common data dictionaries and business glossaries and common definitions, and common definitions deserves a designated record set to ensure that as data is more broadly used, it is used and interpreted in the right context. So that we’re all singing from the same sheet of music, in so many words,” Fernandes says.

One way to do this is to create a matrix where all these DRS documents live—what the names of the documents are, and retention and disposition limits. Catholic Health Initiatives’ Richter says it’s not unheard of to get a records request and to
have to go to four or five different EHRs or systems to retrieve all the requested data. Having a matrix that can serve as a table of contents to where records live can be a key to unlocking the data siloes, Richter says.

**Legal Health Record Revisited**

As the term itself suggests, the LHR’s job is to serve as a health-care organization’s business and legal record, and as noted previously, document the services provided as legal testimony regarding the patient’s illness or injury, response to treatment, and caregiver decisions. Several of the organizations queried for this article define their own LHRs based on AHIMA Practice Briefs and guidance on the topic, including DeMasters.

“I think there needs to be a basic definition so there is an understanding of the DRS versus the legal health record and examples of each—I would refer to AHIMA documents [including Practice Briefs],” DeMasters says. “To write a policy to capture all things pertaining to the legal health record is daunting.”

It is also crucial.

At MRO, a release-of-information vendor, Bowen works closely with providers to make sure they know the difference between the DRS and the LHR because of the massive file size and volume of data that must be released.

“I’m just surprised at the number of facilities who don’t understand the difference between what the DRS should be and contain—some simply say they [DRS and LHR] are one and the same—and they are not one and the same,” Bowen says.

She adds that the only time information should be released from the DRS is if it’s to the patient or a patient-directed request. For any other general ROI purpose, it’s going to come from the LHR, in Bowen’s view. If an organization decides that everything in a patient’s EHR is part of the LHR, they may have to release a radiology image to a patient who doesn’t know how to read an X-ray or an MRI image.

If a facility’s LHR policy has too much overlap with the DRS, they may be stuck releasing all sorts of images the average patient is unable to interpret.

---

**Note**

1. AHIMA. “Fundamentals of the Legal Health Record and Designated Record Set.” *Journal of AHIMA* 82, no.2 (February 2011): expanded online version.

Mary Butler (mary.butler@ahima.org) is associate editor at the *Journal of AHIMA*. 

---

**HEALTHCARE COST SOLUTIONS**

- Hospital Coding Compliance Audits
  - MS-DRG, APR-DRG, APC
  - HCC, LTAC, CVIR/IR
- Professional Fee Coding Compliance
  - E&M, Specialty Surgical
  - Non-Physician Practitioner
- CDI Audits and Assessments
- Remote Coding Support
- HIM Interim Management
- Online ICD-10 Tutorials - **FREE to all Clients**

**Focus On Missed Revenue**

**Optimizing Your Rightful Reimbursements**

1.866.427.7828
WWW.HCSSTAT.COM
DATA ANALYTICS:
The Straight-Lined Labyrinth that Entrapped the HIM Profession

By Ryan Sandefor, PhD, and David Marc, PhD, CHDA
SKILLS IN DATA analytics are critical to the future of health information management (HIM), yet there has been considerable confusion regarding how to articulate what data analytics means for the profession. In a survey of more than 3,300 HIM professionals, skills in data analysis were ranked among the top five most important skills for future HIM practice. Similarly, the 2014 AHIMA Workforce Study reported that a “skill in analyzing big data” was among the 10 most important skills for future HIM professionals. Data analytics has become more prodigious across the HIM profession as more professionals move into roles to evaluate data related to financial, operational, and clinical performance. HIM professionals are becoming more involved in developing solutions for healthcare organizations to better manage and use data. For instance, HIM professionals are developing the policies, procedures, and best practices to ensure organizations are maximizing the integrity and ethical use of data. Because of the clear need in the industry to support the analysis and use of healthcare data, AHIMA placed analytics as a top priority domain in 2018. Despite these notable trends, data analytics remains an elusive term that has yet to be fully understood by many in the profession.

There is considerable research and evaluation that is being completed by AHIMA’s Council for Excellence in Education (CEE) and by members of the AHIMA Foundation Research Network (AFRN) to evaluate workforce trends related to the HIM profession. In 2019, the CEE released an updated HIM Curricula Competencies, including an entire domain for associate, baccalaureate, and graduate program curricula focused on informatics, analytics, and data use. The revised set of curricula demonstrate a commitment by educational institutions to address the shortage of HIM professionals with the necessary skills and abilities to meet industry demand as evidenced by the numerous workforce studies cited above. While there is obviously work needed to design and implement updated curricula and train faculty, this is another step in adapting and re-tooling academic programs to ensure relevance in a rapidly changing healthcare environment where leveraging data as an asset is critical.

Healthcare organizations have recognized the need for data analytics to support strategic and operational goals. Studies have found that investing in data analytics can prevent unnecessary information technology costs, improve the quality and accuracy of clinical decisions, improve the communication between clinical and administrative teams, support interoperability, gain insights into healthcare trends, and optimize business growth by supporting the development of services in a highly competitive healthcare market. For example, organizations that have invested in infrastructure to support the distributed and adaptive storage of unstructured data have accelerated the use of this data—largely through natural language processing—to generate insights into the patients they serve and identify revenue-generating opportunities. Additionally, investing in technology to enhance decision-support capabilities for reporting purposes through smart dashboards have supported real-time evaluation of data, supported long-term strategic decisions, and identified emerging healthcare issues that can impact the care of patients.

Prioritizing Data Analytics in the HIM Profession

HIM professionals are perfectly suited to enhance healthcare organizations’ use of data by leveraging data analytics. The HIM profession as a whole acknowledges its current and future identity as a primary steward of data integrity for enterprise-wide health information. Data analytics is integral to the stewardship of data integrity. The current definition used by AHIMA to define the profession of HIM emphasizes data analysis. According to AHIMA, “Health information management (HIM) is the practice of acquiring, analyzing, and protecting digital and traditional medical information vital to providing quality patient care. It is a combination of business, science,
AHIMA has previously stated the importance of people in the healthcare industry, in particular that “people will always be central in harnessing the power of information to tear down barriers to better health.”

This very idea is critical to understanding the relationship between analytics and HIM. Data analytics is simply a skill that can be used to transform data into information, which can be used to improve decision-making. This is central to the work of HIM professionals.

HIM professionals are the aforementioned “people” who should be “harnessing the power” of data to transform health. There is no other profession that owns analytics. Health information professionals have a responsibility to leverage what we consider the “most powerful currency” in our industry. It is our job to transform ourselves in order to transform healthcare and the overall health of the populations we serve.

Clarifying Data Analytics for HIM Professionals
A question that continues to arise in the field of HIM is “What is the difference between analytics and informatics?” Let us be very clear on this topic: data analytics and informatics are not two separate disciplines. Similarly, data analytics and health information management are not two separate disciplines. Data analytics refers to a set of skills used by individuals to drive meaning from data—typically, raw data. Healthcare data analytics has been defined as “the practice of using data to make business decisions in healthcare.” Data analytics cuts across all professions and disciplines. It is not unique to HIM, informatics, computer science, or, for that matter, banking, aviation, or cartography. The techniques and procedures used to carry out different analyses are drawn from statistics, mathematics, computer science, sociology, and philosophy, among other entities. So in this way, data analytics and informatics are not two separate disciplines. The two are interrelated. HIM professionals (and informatics professionals) rely on data analysis to carry out the basic functions of their various roles and responsibilities. However, health informatics professionals are often required to have more advanced skills in data analytics. Some of these functions use complex analytical procedures like machine learning and other data mining techniques. Others use inferential statistical analyses to demonstrate statistical differences while others use more basic descriptive statistics and visualization methods to summarize information. These techniques are not contingent on credentials in one professional association or another.

The CEE’s work to promote higher levels of competence in analytics among those graduating from accredited academic programs is exciting. Domain III of the 2018 curricular competencies includes multiple standards related to analytics at the undergraduate and graduate levels. Additionally, the data management track at the associate level supports the enhancement of data analytics skills. Managing health information in an electronic era requires foundational skills in data acquisition, extraction, preparation, and use in multiple electronic formats. The new curricular competencies provide flexibility for academic programs to leverage the skills of their faculty and the relative needs of their primary industry partners to create curricula that has the most impact.

Analytics is Part of HIM
The ultimate takeaway is that analytics is not somehow removed from core HIM skills. Instead, it is a core HIM competency. There is not “analytics for the HIM profession,” but rather analytics for “harnessing the power of information to tear down barriers to better health.” Because analytics and HIM practice are inseparable in today’s environment, the skill of analysis needs to be seen as a priority. Individuals need to

---

**InstantText**

**makes a few letters worth a thousand words**

Make your clinical documentation and data entry **timely - accurate - reliable** and give doctors more time for patient care.

**SPEED UP YOUR TEXT INPUT**

- Create customized glossaries in an instant.
- Type a few letters and Instant Text suggests.
- Continue phrases without typing.

Call 1 800 355 5251  |  www.instanttext.com  |  Instant Text 7 Pro
---

The Best Productivity Software
develop that skill through enhanced training and professional development. Further resources that assist individuals and organizations to better meet their outcomes need to be developed. Analyses of leading indicators clearly demonstrate data analytics as a priority for the profession. Are health information management professionals committed to interpreting these findings and responding accordingly?

Notes
7. Ibid.

Ryan Sandefer (rsandefer@css.edu) is associate professor and assistant vice president of academic affairs, department of health informatics and information management, at the College of St. Scholastica. David Marc (dmarc@css.edu) is associate professor and department chair, department of health informatics and information management, at the College of St. Scholastica.
Historic State AG HIPAA Filing: An Important Case to Understand

By Ilana L. Peters, JD, LL.M, CISSP, and Pasha Sternberg, JD

ON MAY 30, 2019, Medical Informatics Engineering, Inc. and its subsidiaries (collectively referred to in this article as “MIE”), agreed to pay $900,000 to 16 states that had jointly filed suit for violating the Health Insurance Portability and Accountability Act of 1996 (HIPAA). Also, in late May, MIE settled for $100,000 with the US Department of Health and Human Services’ (HHS’) Office for Civil Rights (OCR) and agreed to begin a two-year plan to correct potential HIPAA violations. MIE’s settlement with the 16 states marked the first time a significant number of State AGs banded together to file suit against a company for violating HIPAA. Although the suit was settled, the case is worth a close look as this collective state effort could have short- and long-term effects on health information management.

MIE provides a web-based electronic health record system to healthcare providers. Because the providers are covered entities (CEs) under HIPAA, MIE is a business associate (BA) and therefore subject to applicable HIPAA requirements and enforcement not only by HHS, but also by the State AGs, with regard to the individual patients who reside in their states, pursuant to the HITECH Act’s expanded enforcement of HIPAA.

On December 3, 2018 twelve State Attorneys General (State AGs) jointly filed suit against MIE. Within weeks, four more states joined the suit, bringing the total to 16. In their complaint, the State AGs claim that a data breach impacting 3.9 million individuals, which MIE reported in 2015, was the result of MIE’s failure to comply with multiple HIPAA and state law requirements, that MIE’s response to the breach was deficient, and that by allowing a breach to occur after previously stating that it secures patient data, MIE had acted in a deceitful manner.

This case is noteworthy not only because of important lessons learned but also as an indicator of future regulatory actions by State AGs potentially affecting HIPAA-covered entities and BAs.

Brief Summary of the Data Breach
MIE’s breach was the result of basic security failings that made its systems susceptible to a fairly straightforward and common attack. According to the complaint, in May 2015, threat actors identified two publicly accessible user accounts that were used by MIE to test its system. These accounts had very simple and common usernames—“tester” and “testing”—and passwords that matched the username. These weak credentials offered very little protection and, after either guessing or programmatically cracking these account credentials, the threat actor was easily able to gain access to the accounts.

In addition to having weak credentials, at least one of the accounts was susceptible to a SQL injection attack, a well-known and unsophisticated type of infringement that’s been perpetrated for at least a decade. This attack allowed the threat actor to repeatedly query the account and obtain credentials to two other accounts. These subsequent accounts had administrator privileges, which gave the threat actor access to the system and the ability to exfiltrate unencrypted data that MIE held in its databases.

MIE was not aware of the breach until the volume of data that the threat actors exfiltrated grew to a size large enough to trigger an alert after slowing down network traffic. After the alert, it took MIE three days to investigate the issue, identify what the
attacker had done, and stop the data from being stolen.

MIE failures were not limited to pure technical issues; they also existed at an administrative level. The breach investigation revealed that MIE was aware of these weaknesses and the risks they posed well before the breach but had not taken steps to remediate the issues. In the time leading up to the breach, MIE had conducted at least two penetration tests that flagged the issues—one that flagged the two accounts’ credentials and another that had identified the SQL susceptibility. Both penetration tests not only flagged the issues but also identified them as high risks.

Legal Framework and MIE’s Compliance Failures
In their complaint, the AGs allege that MIE failed to comply with a number of legal requirements. They point specifically to violations of HIPAA Privacy and Security Rules and state law requirements that require companies to maintain reasonable security measures, notify individuals of a breach in a timely manner, and accurately state the level of security that a company has for the data it maintains.

HIPAA Technical Security Requirements
Also, in the complaint the AGs claim that MIE’s security protections do not meet the standards of multiple HIPAA Security Rule standards. In their Complaint, the AGs allege that MIE failed to comply with numerous HIPAA Security Rule violations, including:

- Failing to review and modify security measures needed to maintain a reasonable and appropriate level of protection over ePHI
- Maintaining insufficient security measures to reduce risks and vulnerabilities to a reasonable and appropriate level
- Failing to regularly review records of information system activity
- Lacking mechanisms that record and examine activity in information systems
- Failing to identify and track users’ access as well as authenticating users and not managing their access
- Not adequately encrypting the data it stored

With the complaint, the State AGs highlight the absence of an active security monitoring and alert system. Per the complaint, not having these types of protections is significant because had they been in place they would have alerted MIE to the presence of suspicious remote connections long before the network slowdown. The lack of this system would, therefore, be a potential violation of the Security Rule because MIE failed to review and modify security measures needed to maintain a reasonable and appropriate level of protection over electronic protected health information, implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level, implement procedures to regularly review records of information system activity, and implement mechanisms that record and examine activity in information systems, all of which are required by the regulations.

The complaint also faults MIE’s lack of controls around how users accessed the network, including not identifying and tracking users, not authenticating users, and not managing user’s access, all of which is also required by the Security Rule. Finally, the AGs identified the lack of encryption of the data that was exfiltrated as a final violation of the Security Rule’s technology requirements.

HIPAA Administrative Requirements
In addition to the technical safeguard issues, the AGs cited MIE with deficiencies in meeting required administrative safeguards. The complaint specifically makes note of MIE’s flawed incident response process and its non-finalized and incomplete incident response plan. The AGs deem this to be a violation of HIPAA’s requirement to have such a process in place and allude to the fact that the state of the incident response plan is representative of the quality of MIE’s other policies and procedures. Similarly, the fact that MIE conducted risk analyses but did not remediate the risks that those analyses revealed is yet another administrative violation. Finally, the AGs’ position is that the lack of controls on the amount of information that was accessible using the compromised accounts is an indication that MIE does
Historic State AG HIPAA Filing

not adhere to the Privacy Rule’s minimum necessary standard. Notably, the complaint does not allege that MIE impossibly disclosed information or any other Privacy Rule violation.

State Data Protection and Data Breach Notification Requirements

Separately from the HIPAA violations, the State AGs also argued that MIE violated various state laws. At the time of the breach, eight of the states—Arkansas, Florida, Iowa, Kansas, Louisiana, Minnesota, Nebraska, and North Carolina—had breach notification laws that required notification either within specific timelines or without unreasonable delay. The time between MIE’s discovery of the breach and the notification of impacted individuals ranged from 52 days to more than six months, a violation of numerous state statutes, according to the AGs.

Additionally, five of the states—Arkansas, Florida, Indiana, Kansas, and Wisconsin—have laws that require companies to implement reasonable procedures to protect personal information. According to the AGs, the same failings that trigger the HIPAA violations also create a violation of these statutes; in the complaint, the AGs are treating the lack of protections required by HIPAA as being unreasonable under the state laws, an important point regarding future potential enforcement of state laws applicable to data breaches.

Finally, the twelve states that originally filed the suit had statutes prohibiting unfair or deceptive trade practices. The AGs included allegations that MIE violated these statutes in their complaint, pointing to the fact that MIE had previously made public statutes in which they claimed that it would comply with HIPAA and would protect patient information.

The AGs argue in the complaint that MIE promoted its ability to comply with HIPAA when promoting its services so not following through on these promises is a deceptive act. This deception is separate and apart from the underlying security violations and the failure to notify people of the data breach in a timely manner.

Putting the Case into Perspective

As discussed, there are a number of important aspects of this case. First, this case is unusual because it marked the first time that numerous State AGs have acted together to enforce HIPAA. The change of strategy by state regulators could be because MIE mishandled information about patients in multiple states. It is also noteworthy that MIE is a BA rather than a CE. Although HIPAA enforcement actions were routinely brought against CEs in the previous decade, the HITECH Act in 2009, which expanded jurisdiction over BAs, has decreased the scrutiny on BAs. This lawsuit could be an indication that meeting the basics is likely a way to keep HIPAA CEs out of State AGs’ crosshairs—for now.

Third, other than the minimum necessary standard, the AGs did not discuss the Privacy Rule and curiously did not include any claims that MIE improperly disclosed PHI. The Privacy Rule requires that both CEs and BAs disclose PHI only as permitted by the Privacy Rule, and an impermissible disclosure is and of itself a HIPAA violation.

Furthermore, the fact that the state law violations were imposed separately, and not overlapping, the HIPAA claims is important because by separating the claims, the AGs settled regarding separate fines under each law.

Note that the AGs’ imposed state claims required different duties on the part of BAs when compared to HIPAA requirements. As both HIPAA and the various state laws have significant penalties, this duplication can quickly increase the financial costs for the MIE.

While the AGs’ unique approach to this case is significant, it is unlikely that this type of action will become the norm. This particular action was the result of a large breach impacting many individuals in multiple states.

In situations without similar footprints, it is unlikely that multiple AGs would focus their attention on an entity, and even more unlikely that they would coordinate their efforts. Additionally, as mentioned above, given the nature of the alleged security failings, the AGs were likely confident that they could prevail or reach a worthwhile settlement for purposes of sending a message about good baseline security safeguards to other vendors.

Finally, coordination among states takes a significant amount of resources. Even with the $900,000 settlement for the State AGs (and the $100,000 settlement with HHS), the State AGs likely invested much more in this case. Taken altogether, the handling of this case has significance, but multistate lawsuits are unlikely to become the norm.

Disclaimer: Polsinelli, LLP provides this material for informational purposes only. The choice of a lawyer is an important decision and should not be based solely upon publications.

Iliana L. Peters (ipeters@polsinelli.com) is shareholder and Pasha Sternberg (psternberg@polsinelli.com) is an associate at Polsinelli, LLP.
YOUR PARTNER IN CODING EDUCATION AND RESOURCES

- Online access for AHA Coding Clinic® for ICD-10-CM and ICD-10-PCS and AHA Coding Clinic® for HCPCS – www.CodingClinicAdvisor.com
- ICD-10-CM and ICD-10-PCS Coding Handbook 2020
- Free coding advice service through AHA Coding Clinic® Advisor – www.CodingClinicAdvisor.com
- ICD-10-CM, ICD-10-PCS and HCPCS reference materials, webinars and more...

AHA Coding Clinic®
ICD-10-CM
ICD-10-PCS
AHA Coding Clinic®
HCPCS
AHA Coding Clinic®
Advisor
AHA Central Office™
An American Hospital Association Service

www.ahacentraloffice.org
PHI Hide and Seek

HIDDEN PHI CARRIES HIGH FINANCIAL RISK

By Ken Reiher, MBA
BEFORE ELECTRONIC HEALTH records (EHRs) and digital technologies, patient information was stored on mainframe computers located in secure rooms or recorded on paper charts and kept in file folders. Shared access was limited. The monetary value of personal information was low, and so the risk of breach was low.

The technology storm of the past three decades has made access to electronic protected health information (ePHI) easier, which benefits patient care in an ever-fragmented delivery system, but is bad for information security. Protected health information (PHI) can be found in virtually every corner of a healthcare system, concealed in unlikely places. With each new technology, acquisition, or merger comes new vulnerabilities that may remain unseen until the right assessments are performed to uncover them.

I recently sat down with a panel of information and privacy experts from three healthcare organizations to understand their unique experiences with hidden PHI and how they’ve worked to mitigate the associated risks.

Reiher: In your experience, what are some areas where PHI can be hidden?

Rich Temple, vice president, chief information officer, and HIPAA security officer at Deborah Heart and Lung Center in Browns Mills, NJ, focused on cardiac, pulmonary, and vascular care: There are many subtle places that can contain ePHI in a healthcare organization. Without proper monitoring, this poses a serious risk that could cause a breach with devastating consequences. For example, consider mobile phones still in use after a provider has left the organization. Though the provider has been disconnected from the hospital network, there may be circumstances where data that was downloaded up until the time of the disconnection could still be accessible. Even with the mandate that all emails containing PHI must be encrypted, there is still potential exposure here for PHI or, at the very least, sensitive business information being accessible on the device.

I also recommend paying close attention to a hospital’s business associates (BAs). Though all BAs are required to sign a HIPAA business associate agreement (BAA), it is often very challenging for a hospital to ensure the BA maintains the highest security possible for its data. There have been many documented cases of BAs inadvertently publishing PHI. Often, it is just a simple misconfiguration on the part of the BA, but the hospital is ultimately liable for the mistakes of its BAs.

Yet another area that needs to be monitored is PHI downloaded by individuals or physicians via remote connection to the hospital’s system from a home computer. Strict policies should be employed to ensure this cannot happen. Once PHI is on a personal home computer, it is highly probable that strong security safeguards, including encryption, are not present to protect that sensitive PHI from unauthorized access.

Sarah Hodson Grady, CPHI, HCISPP, RYT-200, conversion project manager/HIPAA security at Logansport Memorial Hospital, a not-for-profit medical center serving north central Indiana: Some EHR systems use Microsoft products that allow physicians to compose letters to, or on behalf of, patients. Though the EHR may launch, store, and save the file appropriately, this does not prevent a provider from storing that file elsewhere, such as on a local device. No EHR demo would reveal this behavior, but it does happen, and it’s a great example of hidden PHI. Physician devices need to be audited frequently to discover such issues.

Medical devices are another place where patient identifiers could be readily available. It is important to ensure that patient identifiers are removed from the device. I recommend a standard process to promptly transfer the information from the record to the patient’s chart and remove it from the device. This eliminates the possibility of filing a breach on anyone who might have been on that machine.

Jamie Pesci, director of health information management (HIM) and privacy officer for Christian Health Care Center, a nonprofit, healthcare organization offering senior living, short-
Top 10 PHI Vulnerability Assessment Questions

TO HELP UNCOVER hidden PHI, the following questions are recommended:

Does your organization:
1. Have a policy and process to lock down user workstations based on an analysis of risk and operational need?
2. Encrypt ePHI on portable devices such as laptops, tablets, USB/flash drives, external hard drives, and other electronic equipment?
3. Know which controls are in place to protect ePHI that is stored in remotely hosted databases?
4. Secure/encrypt the wireless transmission of ePHI within your facility?
5. Encrypt remote access transmission of ePHI?
6. Have policies and procedures in place for secure, complete destruction of any hard drive that contains ePHI?
7. Receive a certificate of destruction if using an external resource for disposal?
8. Have physical and technical safeguards in place for the patient portal?
9. Have a BAA in place with any telehealth vendors?
10. Have cybersecurity technology and processes in place to secure your internal network from intrusion?

term rehabilitation, and mental health services: ePHI can lurk in a variety of places, including hard drives and mobile devices of employees who work from home, and with business associates or their downstream third-party vendors. Pay attention as well to disgruntled employees who could be a source of breach if they have access to ePHI and a motive to share it inappropriately.

Reiher: Describe the potential risks—financial, operational, and reputational—of not uncovering these types of PHI locations.

Temple: In 2018, the Ponemon Institute reported⁴ that the average cost of a data breach in a healthcare organization is $408 per record, with an aggregate total estimate of breach costs at $3.6 million. So there is a devastating out-of-pocket expense for a healthcare institution in the form of fines, credit monitoring, and other expenses. That doesn’t even include the loss of goodwill and trust in the community where the hospital operates. The reputational loss is incalculable in dollars and cents. Trust, once lost, is very hard to regain.

Grady: Failure to turn over every rock is like agreeing to babysit without knowing how many kids are in the house. A large breach could mean a loss of independence or autonomy, even if it does not take a healthcare organization completely under.

In a recent case, Hancock Health in Indiana⁵ managed to protect its branding following a ransomware attack by hackers who accessed the hospital’s data via a third-party vendor’s remote connection. Hancock paid the $47,000 ransom and was able to uncover hidden PHI and mitigate risk.

Reiher: What role does HIM play in data privacy at your organization? Are they part of a broader governance and advisory group?

Temple: In our organization, HIM plays a leading role in data privacy. They spearhead our compliance with data retention requirements, and are closely involved with our committees that oversee privacy and security. HIM works with both our compliance department (privacy) and with our information systems (IS) department (security). HIM professionals are critical and knowledgeable partners in both realms.

Grady: Our privacy officer works directly with HIM to elevate data privacy issues to our governance committee.

Pesci: HIM plays a huge role in privacy for our organization. The director of HIM serves as the privacy officer who creates policies, monitors regulations, reviews subpoenas and court orders, controls access to records, and participates in performing risk assessments. We have implemented BA accountability, requiring the completion of a questionnaire regarding HIPAA compliance programs. We then assign risk.

The privacy officer, in coordination with the security officer, conducts HIPAA rounds. The privacy officer also serves on the corporate compliance team, monitors potential breaches, and educates employees, volunteers, and vendors using a variety of tools. In addition, the privacy officer maintains, updates, and posts the notice of privacy practices. HIM is the hub of the release of information.

Reiher: Describe a success story in which your organization was able to uncover hidden PHI and mitigate risk.

Temple: We have a strict policy in place with employees who are granted access to our email server through their mobile devices. When they terminate employment with our organization,
The American Health Information Management Association (AHIMA) is accredited as a provider of continuing nursing education by the American Nurses Credentialing Center's Commission on Accreditation.

The Inpatient and Outpatient CDI Academy offers best practices through real-life examples and exercises. Return to your organization with new insights and energy. At the Academy you will:

- Review key coding guidelines of principal/primary and secondary diagnoses
- Examine opportunities for CDI in the outpatient setting
- Realize the impact of coded data on secondary data uses such as meaningful use incentives, quality measures, and public health reporting

TAKE YOUR ORGANIZATION TO THE NEXT LEVEL!

[ahima.org/cdiacademy](http://ahima.org/cdiacademy)

*The American Health Information Management Association (AHIMA) is accredited as a provider of continuing nursing education by the American Nurses Credentialing Center's Commission on Accreditation.*

282.19
As the healthcare industry evolves, professional education should evolve with it. That is why AHIMA has revamped the AHIMA Convention and Exhibit, and given it a new name—AHIMA19: Health Data and Information Conference.

The conference will feature a number of new offerings this year to help healthcare leaders become more engaged in a dynamic industry. Here’s a peek at what attendees can expect.

**Transforming the Conference**

AHIMA19 has been specifically designed to give health information management (HIM) leaders—and all healthcare professionals with a stake in health data—the education and networking they need to be more strategic and innovative. By broadening the audience for the conference, AHIMA aims to promote greater collaboration and problem-solving across a diverse healthcare community.

“This year, AHIMA is in the process of transforming to achieve our mission of empowering people to impact health,” says AHIMA CEO Wylecia Wiggs Harris, PhD, CAE. “Likewise, we felt it was the perfect time to transform our annual conference. We look forward to highlighting the crucial issues and discussions taking place in the health data and information space and advancing the issues that affect healthcare organizations and patients.”

In fact, organizers designed the conference to appeal to a wide audience interested in health data and information—from HIM leaders to clinicians to IT, finance, and legal professionals. New educational pathways help guide attendees to the specific sessions that are the most relevant and connected to their specific goals. These pathways cover a broad array of topics, including clinical documentation improvement (CDI), the continuum of care, and innovation. All 60-plus sessions have been designed to help attendees at every experience level understand how they can thrive in the changing world of healthcare.

**Creating a Forum for New Ideas**

Another new addition to AHIMA19 that underscores the conference’s focus on innovation and change is the pitch competition, hosted in collaboration with MATTER, a health technology incubator based in Chicago, IL. According to the challenge statement, the competition is seeking “innovative solutions that improve the connections between people, systems, and ideas to transform health and healthcare.” Possible pitches might address interoperability, patient matching, or social determinants of health, although all ideas are welcome from HIM students and professionals as well as those outside of HIM.

Five entrants (selected by public voting and ranked based on judging criteria by AHIMA and MATTER) will be invited to pitch their creative idea in front of an expert panel of judges and a live audience of conference attendees on Monday, September 16, giving them invaluable exposure and feedback they can use to refine their concept. Winners also earn cash prizes to fund their ideas. First place wins $5,000, second place receives $2,500, and third place gets $1,500.

Joe Rizk, MATTER’s vice president of strategic partnerships, says the decision to collaborate on AHIMA’s inaugural pitch competition was easy because both organizations share the same drive to innovate to improve health outcomes. “We wanted to stimulate thinking within AHIMA’s audience as well as nurture startups and give them a stage to present their solutions,” Rizk says. “The startups benefit from getting feedback from individuals working in the field, but we also get to show people what is happening outside the walls of corporate America.”

Specifically, audience members at the pitch competition will gain insights on what is happening in the quick-moving and “scrappy” world of startups, Rizk says. “Sometimes, exposing a broader audience to that helps stimulate internal ideas on how they can think differently about solutions for imperatives in their own organizations,” he says.
The AHIMA19 Exhibit Hall is the place for conference attendees to explore new health information services, product offerings, and breakthrough technologies. This year’s floor offers expanded options for education including Monday and Tuesday’s Innovation Sessions, as well as the HIM Expert Theaters (formerly Product World.) Attendees earn 1 CEU by visiting the Exhibit Hall and may earn additional CEUs by attending HIM Expert Sessions and the Innovation Sessions on Monday and Tuesday. Attendees who join this year’s exhibitor Scavenger Hunt will be entered into a drawing to win a $1,000 gift card. Attendees who visit the hall on Monday and Tuesday also will be entered into drawings for additional prize packages. The following is a list of exhibitors as of July 31, 2019. Conference updates are available at www.ahima.org/conference.

Monday, September 16
Arie Crown Theater

Carey Lohrenz
USN 1st Female F14 Pilot, Aviator, Author, and Speaker

Tuesday, September 17
New this year: “Festival-style” sessions. Attendees choose their general session experience. Two sessions will be happening simultaneously, one in the Innovation Theater on the exhibit hall floor and one in the Arie Crown Theater.

Innovation Theater
(on the Exhibit Hall Floor)

“CMS Interoperability and Patient Access Initiative”
Alexandra Mugge
Centers for Medicare and Medicaid Services

“Patient Advocacy: How to Make Unlikely Things Happen”
Doug Lindsay
Inspirational speaker on leadership, innovation, and problem solving
Arie Crown Theater

“The Opioid Epidemic and the Burden of Chronic Diseases” and “Leadership in Today’s Healthcare System”
Patrice A. Harris, MD, MA, President of the American Medical Association (AMA)
David O. Barbe, MD, MHA, Past President of the AMA

“Arie Crown Theater

Wednesday, September 17

“Arie Crown Theater

“Leadership in Today’s Healthcare System”
Wyclea Wiggs Harris, PhD, CAE, Chief Executive Officer, AHIMA

John Quiñones, ABC News veteran, Creator, and Host of What Would You Do?
Unveiling the Illusion of Digital Health Data Security

Why ‘Perception’ May Be the No. 1 Enemy

By Erin Benson, MA, MBA

HIM PROFESSIONALS HAVE worked diligently to protect data privacy and security during a time of digital transformation in healthcare. The unfortunate reality? Hackers have worked even harder to access that data. It’s a game of ‘cat and mouse,’ and regrettably, the mice (i.e., hackers) appear to have a competitive edge. Healthcare data breaches have tripled since 2017 with 44 percent of healthcare organizations experiencing a cryptomining or ransomware attack.

Healthcare data is lucrative, and—luckily for attackers—there is an endless supply of it to steal and manipulate as organizations shift from paper to electronic records, unveil sleek new patient portals, launch telemedicine platforms, and feed patient-generated data from medical devices into the electronic health record (EHR).

Every access point presents an opportunity for attackers to take advantage of healthcare data. Attackers seek patient names, birth dates, policy numbers, diagnosis codes, and billing information that they use to create false or fraudulent identities, file fraudulent claims, or sell on the dark web.

Sadly, when an attacker strikes, an organization’s most valued commodity—its data—suddenly becomes its biggest liability. This puts patients at risk.

New and Potential Security Threats

Today’s healthcare data breaches aren’t only about stealing the data. Increasingly, attackers access data simply to manipulate it. Imagine the negative consequences if a hacker gains access to a hospital system and changes lab results, allergies, or blood types. The hacker may also utilize the patient’s identity to receive medical care, resulting in conglomederated records. Doctors reading inaccurate information could make incorrect diagnoses or prescribe life-threatening medications. Attackers can even manipulate medical device data from pacemakers, defibrillators, insulin pumps, or neurostimulators that feed directly into the EHR. Again, if this data is inaccurate, it can compromise patient care, causing harm or even death.

Another new and emerging threat is ransomware. A form of malware, ransomware encrypts data so organizations can’t access that data without paying a ransom to obtain the decryption key. Attackers can initiate ransomware through phishing scams that prompt employees to click on infected email links or open infected attachments. According to recent research, a whopping 78 percent of providers reported a ransomware or malware attack in 2017.

Over time, cyberattacks will continue to become more sophisticated, malicious, and harder to detect. Attackers will evolve to overcome barriers and safeguards, stopping at nothing to get what they want.
False Sense of Security
Interestingly, organizations appear to be overconfident in their cybersecurity preparedness despite the growing number of breaches occurring in the industry. Fifty-eight percent of organizations, for example, believe the cybersecurity of their online patient portal is above average, according to a 2019 LexisNexis State of Patient Identity Management Survey.1 Likewise, LexisNexis found that 50 percent of survey respondents are confident they have the necessary controls in place to prevent unauthorized access to patient information.
This confidence is ironic given the fact that 93 percent of respondents protect data with a basic username and password that hackers can easily penetrate. Only 65 percent of survey respondents deploy multifactor authentication—often viewed as a baseline protective measure—to prevent unauthorized access to patient information via the telemedicine platform or patient portal. Clearly, there's a disconnect between perception and reality. Organizations perceive themselves as safe when, in fact, they've never been more vulnerable to attacks.

Seven Best Practices for Patient Identity Management
The most secure organizations take a proactive and comprehensive approach to cybersecurity threats with a focus on identity management. Consider the following seven best practices:
1. Change corporate culture. Adopt a mentality of ‘when we get hacked,’ not ‘if we get hacked.’ Prioritize patient identity management by devoting staff and resources to the effort. Strike a balance between layered security controls that deter hackers and frustration-free access for patient engagement.
2. Make multi-factor authentication your baseline protection. For example, verify patient identity using name, date of birth, and home address. Organizations increasingly rely on a variety of sources—knowledge-based questions, one-time passwords, email verification, facial recognition, device analytics, or voice biometrics—to authenticate users based on the criticality of the transactions.
3. Deploy step-up authentication, when necessary. For example, use low-friction verification when patients initially log in to the portal and layer in high-friction verification and authentication for transactions such as payments and data transfers.
4. Adopt a cybersecurity framework. Combine elements of multiple frameworks (e.g., NIST, HITRUST, ISO, or COBIT) into one set of guidelines or choose a single framework that works best for the organization.
5. Reduce duplicate records. Focus on patient matching to ensure each patient has a single, comprehensive record that organizations can secure and exchange with greater confidence.
6. Provide employee training. Test employees to ensure they can recognize and avoid email phishing scams, vendor spoofing (i.e., an attacker posing as a vendor on a service call), and IT/IS spoofing (i.e., an attacker posing as internal IT or IS staff). Teach them to verify identity and obtain call-back information prior to answering any questions requiring disclosure of protected health information.
7. Think outside the box. Cybersecurity isn't only verifying patient identity for patient access. It's also about validating employees and vendors. Any point of entry into a system should be protected.

The time to act is now. Organizations need to acknowledge and address security vulnerabilities before an attacker takes advantage of their data and their patients.

Notes

Erin Benson, MA, MBA, director, market planning at LexisNexis Risk Solutions, works with a focus on the development and execution of strategic planning for member identity and socioeconomic determinants of health solutions.
HEALTHCARE PROVIDERS DEAL with electronic information on a daily basis. Providers must expect that volumes and varieties of electronic information will increase exponentially with, for example, the rise of artificial intelligence in the diagnosis and treatment of patients. That electronic information likely will be defined as electronic protected health information (ePHI) and fall within the definition of the electronic health record (EHR), although a provider will create, store, and maintain electronic information that may not be included in the EHR, such as nursing notes.

Whatever the format of the data and wherever it might reside within the information technology (IT) structure of a healthcare provider or within the structure of a business associate (BA), there may come a time when it must be located or retrieved, preserved, and produced for litigation-related purposes. When relevant electronic information is “lost,” the provider who should have preserved it may be sanctioned. Courts across the country use different tests to determine whether sanctions should be imposed for the loss of electronic information or, as it is commonly known, electronically stored information (ESI). This article will look at the meaning of lost ESI under the Federal Rules of Civil Procedure. Examples of litigation in which ESI might be relevant include, for example, medical malpractice causes of action in which the content of the EHR might be used to prove or rebut an allegation of misdiagnosis or improper treatment.

What Does ‘Lost’ Mean?
Federal Rule 37(e) governs the imposition of sanctions for the loss of ESI. The rule authorizes sanctions if four conditions are met:
1. The ESI at issue should have been preserved in anticipation or conduct of litigation
2. The ESI is lost
3. The loss is due to a party’s failure to take reasonable steps to preserve it
4. The ESI cannot be restored or replaced through additional discovery

This article focuses on the third condition. “Lost” must be considered in context. Although not related to healthcare, Franklin v. Howard Brown Health Center, No. 17 CV 8376, 2018 WL 4784668 (N.D. Ill. Oct.4), report and recommendation adopted, 2018 WL 5831995 (N.D. Ill. Nov. 7, 2018), provides an example. The plaintiff in Franklin, which was an employment discrimination action, requested that the defendant produce emails and text messages to support the plaintiff’s claim he had been harassed by the defendant’s personnel. The plaintiff was actually seeking instant messages, the purported method by which he was harassed. The defendant produced two instant messages and could not produce any others. The plaintiff moved for the imposition of sanctions under Rule 37(e). Here are some of the findings of the court in ruling on the motion:

• The defendant’s general counsel had issued an untimely and ineffective legal hold that gave “no indication what employees were to do with documents or electronic files and information that had to be preserved, or how they should be preserved, and there was no indication they should forward or deliver the information, files, etc., to defendant’s legal department.”
No attorney supervised the preservation efforts of the defendant’s employees. Rather, employees decided “on their own what was relevant and what wasn’t.”

Additional instant messages had existed on a hard drive of a former employee of the defendant but the hard drive’s data had been deleted.

The plaintiff’s work computer, on which the additional instant messages were presumably stored, could not be located even though it had been supposedly preserved.

Any instant messages that had existed on the computers of the plaintiff’s harassers—other employees of the defendant—had been autodeleted.

Based on these and other findings the court concluded that the defendant had been grossly negligent in its failure to preserve the additional instant messages and recommended that the parties “be allowed to present evidence and argument to the jury regarding the defendant’s destruction/failure to preserve electronic evidence in this case, and that the jury be instructed as the trial judge deems appropriate.”

In reaching its conclusion the Franklin court necessarily found that the ESI had been “lost” under the meaning of Rule 37(e). However, is the loss of ESI within a healthcare provider’s IT systems self-evident when that ESI no longer resides within the system? Envy Hawaii LLC v. Volvo Car USA LLC, Civ. No. 17-00040 HG-RT (D. Hawaii Mar. 20, 2019) provides an answer.

Envy Hawaii arose out of a contract dispute and allegations of improper business practices between a Hawaiian car dealership and the national distributor of Volvos. After two years of litigation, which included document production and depositions, the defendants moved for sanctions against the plaintiff for its failure to preserve “Google e-mail accounts and electronic dealer management system records.” The court denied the motion, finding that that ESI had not been lost.

The court began with a review of Rule 37(e): “The text of Federal Rule of Civil Procedure 37(e) provides that evidence is ‘lost’ and subject to spoliation sanctions when a party failed to take reasonable steps to preserve it, and it cannot be restored or replaced through additional discovery.”

The court then focused on the meaning of “lost” under the rule: “Information is ‘lost’ for purposes of Rule 37(e) only if it is irretrievable from another source, including other custodians.”

Moreover:

Cases decided after the implementation of the 2015 amendment to Fed. R. Civ. P. 37(e) have highlighted the 2015 Advisory Committee Notes to the Rule. The 2015 Advisory Committee stated that “because electronically stored information often exists in multiple locations, loss from one source may often be harmless when substitute information can be found elsewhere.”


With this focus, the court turned to the facts before it and found that the defendants (the moving parties) had not met their burden to show that the ESI had been lost. The plaintiffs might not have preserved the ESI but the ESI might be stored with third parties, which maintained the ESI on behalf of the plaintiffs. Moreover, the court observed that the defendants had not subpoenaed the third parties for the ESI or attempted to retrieve it from a system to which they had access. Under these circumstances, the court concluded that the ESI had not been lost and left the defendants to serve subpoenas.

Implications for HIM

What lessons might Envy Hawaii have for a health information management (HIM) professional? There are several, all arising when the professional is called upon for assistance during litigation:

- The professional should consider where relevant information resides within the provider’s IT system.
- The professional should understand whether relevant ESI resides outside the provider, for example, with a business associate or in the cloud.
- The professional should understand the need to preserve that ESI and, as directed by counsel, take steps to preserve the ESI. That necessitates a knowledge of the form in which the ESI was created and how it was stored so that relevant metadata can be preserved.

This role for the professional might exist whether or not the focus of preservation is solely the EHR or whether other ESI, as in the earlier example of nurse’s notes, which might be the subject of preservation.

This means that the HIM professional may have a central role in avoiding the loss of relevant ESI.

Note: For a broader discussion of the role that the HIM professional can have in litigation see the AHIMA Practice Brief, “Health Information Management and Litigation: How the Two Meet,” published in the May 2019 issue of the Journal of AHIMA and available online in AHIMA’s HIM Body of Knowledge.

Reference


Ron Hedges ([r_hedges@live.com]), JD, is a former US Magistrate Judge in the District of New Jersey and is a writer, lecturer, and consultant on topics related to, among other things, electronic information. He is a senior counsel with Dentons US LLP.
Data and Analytics Drive Effort to Curb Opioid Abuse: A Holistic Approach for Health Systems

By Kapila Monga and Harpreet Singh

IN THE UNITED States, five percent of the world’s population consumes about 80 percent of the world’s opioids,¹ a statistic that merits the status of a public health crisis in which the demand and supply side of the issue deserve equal weight. Current efforts to address this crisis focus mainly on managing the supply side of the equation through prescription guidelines and relevant training programs. The reduction in demand that is driven by awareness, treatment, and prevention of opioid abuse through appropriate medical, social, behavioral, and policy interventions merits equal—if not more—focus.

While all players in the healthcare arena have a role to play, some have a specific set of responsibilities. Physicians are uniquely positioned to address this epidemic as they are the first to observe the signs and symptoms associated with opioid abuse and are equipped to treat the illnesses that can result.

However, it must be acknowledged that this is a huge responsibility to place on the shoulders of one part of a complicated system. We need an effective combination of prevention and treatment strategy, which is why health information management (HIM) can play a large role. They can assist with relatively simple tasks such as altering electronic health records (EHRs) to help physicians adhere to safe prescribing guidelines and converting morphine milligram equivalents. Health IT systems can also help identify opioid-seeking behaviors and patients at risk for overdoses and other adverse events. These and other data-centric solutions give health systems a needed boost in helping to predict, plan for, and support prevention efforts to curb opioid abuse.

Prescription Opioid Abuse Engine

Two years ago, AHIMA launched an effort to improve documentation related to the use of opioids.² A review of physician notes in EHR systems since reveals the significant improvement that has happened in this regard. Inclusion of ICD-10 codes for opioid-use disorder and opioid overdose or poisoning has helped further the cause. Much more can and should be done, but it will take time to sort through the challenges inherent in streamlining this documentation. The primary job function of physicians is not medical documentation, and with EHRs being a contributing factor to burnout, asking more of them on the documentation front is tricky.

At the same time, the healthcare industry today stands at a crossroads when it comes to effectively analyzing and mining EHR system data for reducing prescription opioid abuse, identifying social determinants of health, slowing chronic disease progression, and reducing avoidable re-admissions, to name a few.

The diagram on page 37 represents a framework of a clinical decision support system that utilizes data from EHR systems to identify, predict, and eventually prevent prescription opioid abuse.

At the core of this decision support system is a quartet of engines: detection, intervention, monitoring, and prevention.

• The detection engine identifies prescription opioid abuse by tapping into the behavioral indicators hidden in physician notes, including pattern analysis and natural language processing, and predicting the same to help identify opioid abuse at an early stage.

• The intervention engine recommends next-best actions based on patients’ current needs, such as medication-assisted therapy, nonopioid pharmacological treatments, and nonpharmacological treatments.

• The monitoring engine ensures that the patients adhere to the treatment provided and sends real-time alerts to
physicians or nurse practitioners in case of an alarming situation. The engine also lets the provider know if the intervention is not working as intended.

- The prevention engine's objective is to generate insights that can aid policy design and collaboration among various stakeholders within the healthcare landscape to reduce the incidents of prescription abuse.

Quartet of Engines Decoded

The design of the detection engine rests on syntactic and semantic analysis of physician notes from the EHR system using context free grammars and medical-specific data dictionaries by the Unified Medical Language System (UMLS) and SNOMED. At the core of this analysis is the mining of physician notes based on ontologies created along these three dimensions: prescription opioids typically abused by patients; behaviors and symptoms that prescription opioid seekers complain about; and diseases and conditions that such patients typically report. These ontologies can be either created through systematic text mining of physician notes of opioid-use disorder patients or can be developed in collaboration with clinicians utilizing the information available in SNOMED, research journals published in PubMed, and the UMLS.

In either case, validation by clinical experts will help the engine become more accurate relatively faster. Mining of physician notes will reveal a list of patients who are currently suffering from opioid abuse. Superimposing this analysis with the creation of a lexicon specific to problems at hand then helps in the identification of patients who are at risk of opioid abuse. While there is no shortcut to ensure that this engine will flag minimal false positives, with continuous feedback from clinicians and recalibration by data scientists, it is fair to assume that the engine will become reasonably reliable in a short amount of time.

Coupling the above results with analysis of laboratory data, patient demographics, and social determinants of health can help identify the right interventions to treat prescription opioid abuse. The intervention engine can analyze the data available for all treatments across the patient population, identify historical success rates, and recommend the best intervention.

The engine can also consider prescription events from state prescription drug monitoring program (PDMP) data so that adverse interactions among medications are avoided, as well include rules corresponding to guidance from the Centers for Disease Control and Prevention (CDC) and the Substance Abuse and Mental Health Administration (SAMHSA), on handling opioid prescriptions.

The need for the monitoring engine is clear—human lives are at stake. The monitoring engine takes a two-pronged approach to track and measure the effectiveness of interventions, including patient adherence to the treatment and efficacy of the treatment, respectively. Wearables, Internet of Things (IoT) data, and remote health monitoring will have to come together to make this engine a reality. There are niche companies who are doing work in the direction of making remote patient monitoring a reality, and collaboration with them might be the best way forward. The data from wearables and remote health monitoring, when coupled with EHR data, can help in tracking adherence to, and measuring the effectiveness of, interventions.

The prevention engine is the most elusive in the data science world. It is intended to help policymakers and lobbyists gather real-world evidence on how prescription opioid abuse is being treated, what is working, and what is not. This engine generates self-service reports on efficacy of various interventions, under various conditions. These reports to executive management can aid policy directions and decisions. Output from the other three engines can help generate these reports.

In an ideal scenario a collaboration, created through colla-

Continued on page 54
IN 2014, THE American Recovery and Reinvestment Act required and incented hospitals to demonstrate "meaningful use" of an electronic health record (EHR). Hospitals, desiring to maintain existing Medicaid and Medicare reimbursement levels and avoid penalties, spurred a rapid digitization of medical records. Unwittingly, they also created an irresistible incentive for hackers.

In 2015, practitioners recognized the value of networking medical device data directly into the EHR, which could reduce errors, increase real-time documentation, and improve workflow. While these connected medical devices resulted in numerous new benefits, they also increased the risks to compliance and patient safety. To prevent harm to patients and to protect a hospital's assets, understanding the threat and understanding strategies for an effective response is imperative. This article covers the scope of current threats and resources for providers.

Medical Device Vulnerabilities
A 2017 Ponemon study of anonymous respondents, "Medical Device Security: An Industry Under Attack and Unprepared to Defend," found 44 percent of hospitals had experienced an attack on a medical device that resulted in adverse events or harm. Inappropriate treatment was the outcome in 38 percent of the events. Patient beds alone have an average of 14 medical devices that can be connected, built in, or incorporated into their design.

In addition to fighting escalating cyberattacks, healthcare privacy and security professionals are also focused on meeting regulatory compliance for the confidentiality of electronic protected health information (ePHI). They also are now realizing that compromising the integrity of data or the availability of systems will adversely impact patient care. Medical device risk management is now evolving to address all three areas of the CIA Information Security Triad: Confidentiality, Integrity, and Availability.

Emergency room doctors rely heavily on a CT scanner's availability and integrity to quickly diagnose stroke patients and determine if a stroke is hemorrhagic or ischemic. A delayed diagnosis could easily result in loss of motor functions, brain damage, or even death.

Besides medical devices, major healthcare systems possess tens of thousands of networked devices that are part of what is often referred to as the Internet of things (IoT) and operational technology (OT) devices. These devices can be elevators, HVAC units, video conferencing equipment, printers, and blood refrigerators, all of which are critical to patient care and—like medical devices—extremely vulnerable to cyberattacks. In addition to being directly compromised, medical, IoT, and OT devices can be used as a hacker's entry point into the hospital network, putting patient safety, ePHI, billing records, and intellectual property at risk.

A recent industry-wide survey from ZK Research found that a disturbing 61 percent of network professionals have little confidence they know what devices are connected. Many IT departments believe the same security tools used to protect general network infrastructure can secure healthcare environments. However, unlike other IT endpoints, connected medical, IoT, and OT devices are hardly visible in native IT control systems. This puts non-healthcare-focused security solutions at a profound disadvantage.

Network access control (NAC) systems are commonly used...
to manage traditional endpoint devices such as servers, desktops, laptops, and portables. Traditional NAC takes a broad view of the network. However, most NACs provide inadequate contextual information about medical and IoT device use, traffic flows, or operational status, which would render an administrator, for example, unable to determine why one Baxter infusion pump is communicating with North Korea while the other 999 pumps are not. Typically, NAC cannot see the IP or networking information, which reveals the true nature of a device and the context of its communications within the network. A NAC’s inability to distinguish medical devices often fails to identify MRI machines and instead classifies them as unknown devices.

This poor device visibility results in system administrators continuously mixing unknown vulnerable devices into network segments without thought to the National Vulnerability Database’s recommendations on mitigating their risk. Because these devices were never designed to support an authentication certificate, system administrators simply configure a NAC bypass allowing the unknown devices’ automatic authentication. The solution isn’t as simple as restricting access. These devices are incredibly sensitive to vulnerability scans and blocking these devices is not an option as it may interrupt practitioners administering patient care. A key medical device management maxim is “Don’t inadvertently shut off the device administering life-saving medication to the patient.”

**High Profile System Vulnerability Events**

In recent years, several incidents and compromised devices have threatened patient care. A few examples include:

1. **BlueKeep**, a self-replicating malware worm that exploits Microsoft's Remote Desktop Protocol (RDP) and allows bad actors to remotely access and control the endpoint. In May 2019 Siemens reported vulnerabilities in several medical devices that could be exploited by BlueKeep. The severity of these vulnerabilities are rated a 9.8 out of 10 on the MITRE’s Common Vulnerability Score System (CVSS). ECRI, a federal patient safety organization, forecasted RDP as the top healthcare technology threat for 2019. Many medical devices, including critical radiology devices, run legacy Microsoft Windows operating systems, making them likely targets to hackers and indiscriminate malware.

2. Becton Dickinson’s Alaris Gateway Workstation (AGW) provides power and network connectivity to infusion and syringe pumps. An improper access control vulnerability allows hackers to remotely upload malicious firmware to infusion pumps, causing them to dispense all the patient’s medication in minutes instead of hours. During the 2019 RSA Conference, doctors simulated the emergency on stage. In June 2019, the FDA recalled Medtronic’s MiniMed pump for this vulnerability. The United States Department of Homeland Security’s advisory on the AGW has a CVSS rating of 10 out of 10.

3. At Israel Deaconess Radiology System, a network tech connected to the internet for a firmware upgrade and went to lunch. Malware was downloaded and 2,000 X-ray images were stolen. According to media reports, the X-rays were sold to Chinese nationals with lung diseases who wanted to travel outside the country for treatment.

**Suspicious Activities Worth Monitoring**

1. All unpatched devices vulnerable to the BlueKeep virus are not quarantined.
2. The elevator control system is trying to communicate with human resources application.
3. Ninety-three percent of your IP-based security cameras are using default passwords and security configurations.
4. You’re considering contacting the US Department of Health and Human Services’ (HHS) Office for Civil Rights because 20 devices on the “gone missing” list are not using data encryption.
5. It’s unclear which medical devices are running Windows 7, which will be discontinued in January 2020.
6. Heart monitors recalled by the FDA are still in use.
7. A CT scanner is sending payment card industry data to an IP address in Ukraine.

The CHIME CEO and the Association for Executives in Healthcare Information Security (AEHIS) chair recently wrote to Senator Mark Warner (D-VA), an author of the 2015 Cybersecurity Act (CSA). Under Section 405, the CSA requires the Secretary of HHS to address improvements for cybersecurity in the healthcare industry. They voiced their support for several FDA policy proposals, including the draft guidance that will address the “serious threats to patient safety stemming from cybersecurity threats to medical devices.” Their letter covered eight primary points, including the following five, which specifically address medical devices:

1. Regulators need to understand medical device risks extend to the entire network, thus posing a real risk to patient safety.
2. The FDA should expand the definition of medical device risk to include networks, switches, firewalls, applications, and other components.
3. Global WannaCry 2017 patches have not been released for certain medical devices.
4. Medical device manufacturers need certification standards similar to EHRs.
5. The FDA’s premarket guidance on medical devices should explicitly reference the voluntary guidance provided by HHS, in response to the CSA Section 405 mandate “Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients,” to serve as a resource to improve their cybersecurity posture.

Continued on page 55

Journal of AHIMA September 19 / 39
Developing and Defining a Legal Health Record Policy

By Cindy Zak, MS, RHIA, PMP, FAHIMA

YALE NEW HAVEN Health (YNHH) began implementing the electronic health record (EHR) across four delivery networks in 2012. As the system moved to the electronic world, it became evident that YNHH needed to address the issue of defining the organization’s legal health record (LHR), a subset of the designated record set (DRS).

YNHH began this initiative by creating a work group that included members from information technology, Yale Medicine, and corporate health information management (HIM). At YNHH, the new EHR vendor included both the university medical record and the system medical record as one component. Yale Medicine is a separate entity from the YNHH, although Yale University physicians (Yale Medicine) admit their patients to Yale New Haven Hospital. Yale Medicine physicians are credentialed by the medical staff office. Their clinic medical records are a component of the YNHH EHR. The residents and fellows further their training at Yale New Haven Hospital.

Clearly, with the EHR on the horizon, Yale New Haven Health needed to define the LHR with YNHH and Yale Medicine stakeholders.

At YNHH, an EHR is maintained for each patient who is evaluated or treated as an inpatient, outpatient, or emergency patient at the delivery network and clinics, care centers, and physician offices both for the Northeast Medical Group, the physician entity, and Yale Medicine.

At the first work group meeting, the work group established steps to defining the LHR. The group:

1. Determined what legal entities enforce regulations, guidelines, standards, or laws within healthcare referencing the LHR definition and the LHR and/or designated record set (DRS).

2. Determined whether the records are created or referenced in the course of business at YNHH.

3. Addressed retention requirements.

4. Created a matrix that defines each document in the LHR and/or DRS.

5. Established if the document is released to third parties in response to legally permissible requests.

Designated Record Set

The DRS is defined by HIPPA. The DRS consists of the patient medical records, billing records, patient enrollment, payment information, claims, adjudication and cases, and medical management record systems maintained by or for a health plan; or information used in whole or in part to make care-related decisions.

YNHH determined it was important to define and differentiate explicitly the LHR from the DRS, which includes clinical data stored on any medium and collected and directly used in documenting healthcare or health status. The DRS is broader than the LHR and includes all protected health information and billing information.

Definitions

YNHH’s policy defines the LHR and DRS as follows:

- The LHR is the collection of information created and maintained to document healthcare services provided to a patient by YNHH in the course of the covered entity’s business. The LHR is a subset of the DRS and is the record that is released for legal proceedings or in response to requests for release of patient medical records.

- The DRS is the group of records that include protected
YNHH determined it was important to define and differentiate the LHR from the DRS, which includes clinical data stored on any medium and collected and directly used in documenting healthcare or health status.

health information along with business information that is maintained, collected, used, or disseminated by or for a covered entity for each individual that receives care.

The primary reason for the development of the LHR policy was to identify those documents that YNHH and Yale Medicine would release for formal business and legal purposes and to ensure that the integrity of the health record is maintained so that it can support business and legal needs.

In reviewing Connecticut state law, the LHR was not addressed from a state law perspective. The work group’s primary references were the AHIMA practice brief and the HIPAA regulations referencing the DRS.

Defining the components of the LHR required the work group to inventory the documents maintained in the EHR that included scanned documents. The work group reviewed each document and determined if that document was referenced and used to document healthcare services provided to the patient.

The work group wanted to keep the matrix simple to include as an attachment to the policy for all to reference. The LHR could be generated by departments other than HIM, including:
- The regulatory department when the Department of Public Health and the Joint Commission perform site visits.
- IT when depositions occurred.
- The privacy officer when working with patient complaints.

The work group limited the matrix to include the document name and a column defining the document as the DRS and/or LHR. There are a total of three columns in the final matrix that are posted on the system intranet. All the documents included in the matrix are components of the EHR documents.

Overall, the policy applies to all uses and disclosures of the health record for administrative, business, or evidentiary purposes. It encompasses reviewing documents that were recorded on a variety of media including, but not limited to, electronic, paper, digital images, video, and audio.

It was the intent of the work group not to compromise the LHR and to include all documents that are created and authenticated in the ordinary course of the hospital’s business during the patient’s encounter.

The matrix also addressed external content used in decision-making and care of the patient, such as record forms and reports from other healthcare providers.

YNHH has a policy that requires physicians to identify which external documents they referenced in the care of the patient. Those are the documents that are scanned into the EHR.

Numerous documents required review and consensus. The following documents were discussed and it was then determined if they were part of the LRH and/or DRS:

**LHR components:**
- EKG and EEG tracings
- Clinical photographs
- Diagnostic images
- Fetal monitor strips

**LHR and DRS components:**
- Personal health records (PHR) at the time the PHR was accepted by the provider
- Patient portal messaging was accepted both in the LHR and DRS
- Physician queries were also part of the LHR

**Documents that were not included in LHR nor DRS:**
- Administrative data
- Employee health records
- Video/audio

The LHR is printed when the button to print is selected in the EHR. This was programmed by IT. It is not uncommon for the regulators to ask for the LHR policy and matrix when they are onsite and reference it throughout their visit.

IT ensures appropriate access to the LHR and DRS occurs in compliance with the delivery networks’ archiving and retention schedule.

An ongoing quality control program is in place to monitor timeliness and accuracy of scanning and indexing. Where decentralized scanning is deployed, HIM remains accountable for all aspects of the quality control and verifies the completeness of the medical record in accordance with established guidelines.

All medical records are completed within 21 days following discharge, with a less than one percent suspension rate across all YNHH networks. Audit trails of user access, action, and date of action to the EHR are monitored by the IT security area.

The LHR and DRS policy is reviewed on an annual basis and updated as needed.

Cindy Zak (cindy.zak@ynhh.org) is the executive director, revenue services, Yale New Haven Health.
Recruitment, Selection, and Orientation for CDI Professionals

Editor’s Note: This Practice Brief supersedes the July 2013 Practice Brief titled “Recruitment, Selection, and Orientation for CDI Specialists.”

THE GOAL OF a strong clinical documentation improvement (CDI) program is to validate that the documentation supports the highest level of specificity based on the clinical evidence provided. An effective CDI program begins with proper recruitment, careful selection, and adequate orientation of CDI professionals, whose purpose is to initiate concurrent and/or retrospective reviews of the health record for clear, consistent, complete, precise, reliable, legible, and timely documentation. CDI reviews can occur in both inpatient and outpatient settings and should include the level of documentation necessary to accurately assign the appropriate International Classification of Diseases, tenth edition, Clinical Modification and Procedural Coding System (ICD-10-CM/PCS) and Current Procedural Terminology (CPT) codes.

These efforts result in greater integrity of the documentation, which supports appropriate reimbursement and accurate quality scores. Defining the goals of the CDI program, as well as the purpose of the CDI professional’s role within the organization, will assist providers in developing a process that results in the consistent hiring of quality staff.

Individuals qualified to serve as a CDI professional include, but are not limited to:

- Health information management (HIM) professionals
- Coding professionals
- Physicians
- Nurses
- Other professionals with a clinical and/or coding background

In this diverse population of possible candidates, having an appropriate knowledge base is one piece of the overall process and does not guarantee success. This Practice Brief will provide guidelines for the ideal successful recruitment, selection, and orientation processes for CDI professionals in the development of a sustainable and high-quality CDI program.

Recruitment Best Practices

Researchers agree that the best way to recruit top talent is to create a culture that promotes a positive work environment, which leads to greater job satisfaction and employee retention. Creating a culture in which staff members are treated with respect and consideration while compensated with a competitive salary and benefits package will help your organization stand out as a place where people want to work. A positive setting, salaries, and benefits are significant components of a job search for new hires so it’s important to create a workplace where top talent would want to work.

Managers can seek opportunities to involve CDI professionals in committees and/or meetings that promote CDI activities and physician education. Another opportunity would be to leverage CDI professionals as contributing writers for the CDI newsletter. Newsletters can be created specifically for CDI topics and dispersed throughout the organization. This helps promote the benefits of having a CDI program and identify the current documentation topics impacting the organization. Developing increasingly influential roles for existing staff may assist in recruiting for the organization as current staff communicate the value of their own roles within the organization and demonstrate the rewarding nature of the program. Opportunities to learn and grow professionally will cascade from current employees to peers who may be seeking to make a job change. These individuals can also add value to the interview process, allowing them to more easily identify applicants who fit the team and who will enhance the selection process.

Finding the right individuals does not end with acknowledging experience. Successful CDI programs also consider cultural compatibility, leadership skills, effective communication, and intellectual ability to excel in a complex healthcare environment. The recruitment process can take several months and should not be rushed or neglected.

Recruitment often goes beyond traditional candidate searches, job hiring sites, and word-of-mouth recommendations. Furthermore, many organizations lack the infrastructure and processes for recruiting CDI professionals because of a focus on internal talent development. Internal talent development is always a preferred method for growth and development, but it is not the only recruitment option available.

Recruiting Internally

There are advantages to recruiting internally—hiring from within the organization. These candidates are already ingrained in the organizational culture and are knowledgeable of the organizational goals and needs as well as the focus of the CDI program. Internal candidates often approach the new positions with positive outlooks and knowledge of how they can make a difference.

When recruiting internally for CDI positions, there are many potential candidate streams. Internal candidates can be located within the HIM, coding, quality, nursing, or case management de-
partments. These candidates often require an additional skill or knowledge development if the CDI position is outside their current scope. For example, if a unit coordinator has completed their associate-level degree, is credentialed as a registered health information technician (RHT), and demonstrates the skills to advance into a CDI position, they still may need additional training on the specifics of CDI.

There are also potential disadvantages to recruiting internal candidates, including the promotion of organizational cultural complacency, restricting the candidate pool, perpetuating poor performers, and constraining creative ideas.

**Recruiting Externally**

Many organizations utilize external recruitment as a balance to internal recruitment activities. Recruiting external candidates facilitates new ideas and brings fresh candidates into the organization. It allows the organization to choose from a larger pool of applicants. It also can lead to a more experienced and diverse workforce, and can decrease training costs because the candidate comes into the organization with the skills and knowledge required for the job with little or no development needed.

For example, if an external candidate holding the registered health information administrator (RHIA), certified coding specialist (CCS), and certified documentation improvement practitioner (CDIP) credentials applies for a position in the CDI department, they will come into the organization with specific, required knowledge. For example, a candidate who is a registered nurse (RN) may already hold a CCS credential and have case management experience.

Organizations should also consider the disadvantages of hiring externally, as it is much more of an unknown for the organization. Even with a solid recruitment effort, selection pool, and orientation process, new candidates are still relatively unknown. It can be difficult to identify how they will fit with other staff members and react in certain situations. External candidates—for example, an experienced CDI professional—may find it difficult to adapt to a new process. Adding in questions during the recruitment phase regarding their comfort level with changes can help identify those individuals who may struggle with the program’s structure. Candidate misplacements can cost the organization time and financial resources.

**Selecting the Right Employee**

Prior to selecting employees for new positions, the organization must decide if it is open to recruiting entry-level professionals without CDI experience or if it prefers professionals with little-to-extensive CDI experience. It is also essential to define the format of the program—for example, in-house/onsite reviews vs. offsite/remote reviews. There has been an upward trend in hybrid programs which are attractive to many candidates and allow for flexibility, increase employee satisfaction, and increase productivity. Defining these parameters helps filter the candidate pool and streamlines the hiring process.

CDI is quickly expanding beyond the adult inpatient scope to include outpatient, psychiatry, pediatrics, rehab, and same-day surgeries/ambulatory care. This expansion is leading to the need for specialized reviews and a mix of CDI staff who can cater to this growing need.

Recruiters often run into issues like information falsification on resumes. When this occurs, the candidate may appear qualified on paper but in reality, isn’t able to offer the expertise required to be successful in the CDI role. Recruiting and selecting the right fit for any CDI program requires a careful and thoughtful analysis of each prospective candidate to ensure the candidate can perform at the level required for the position.

Generally, to be successful in a CDI role, candidates must have the clinical knowledge required to review a health record, the ability to recognize deficiencies or gaps in documentation, and strong critical/analytical thinking skills. Effective communication skills are of the utmost importance as well, because the person in this role needs to be able to confidently converse with providers and other team members. A candidate that possesses these qualities would be ideal for a CDI program.

Optimal candidate selection has the potential to decrease employee turnover. Ultimately, a strong CDI professional can provide a positive influence on the organization’s culture and program effectiveness. In addition, successful selection will save the organization time and money during the orientation and training process.

Throughout the process of hiring a new employee, remember to carefully assess the applicant’s fit with both the team and physicians. Utilizing experience and intellectual capabilities alone will not guarantee an appropriate hire. The ability to seamlessly interact with the team and communicate effectively with physicians is a strong indication of how well the CDI professional will integrate into the organization. To that end, it is important to ensure that final hiring decisions remain under the hiring manager’s authority.

Candidates that are a good organizational fit may be extremely difficult to find so staying flexible is important when making hiring decisions. Still, creating the right culture, maximizing the best workers, and staying involved during the hiring process may not fill every open position. In some instances, the right choice may not be the person with long-term experience, but the person that fits best with the team and culture of the organization. This may mean hiring someone with less experience and committing to providing the necessary training and education to develop the skill set.

**Preliminary Selection**

Selection begins with a preliminary application review and screening interview, which is usually conducted over the phone. This process eliminates candidates who do not meet the minimum eligibility criteria established by the organization. This process should include a thorough review of the candidate's application or resume, skill set, academic background, certifications, and work history.

Depending on the goals of the CDI program—whether looking to hire trainees or experienced professionals—evaluation of a potential candidate may include identifying healthcare experience, prior experience in coding or other related work, and possession of the CDIP/CCDS credential. Establishing these criteria will help narrow down the pool of candidates.

The next step in the selection process may include specific
questions that further narrow down the pool of candidates. This may be completed by either human resources staff or the hiring manager. These questions may focus on items such as:

- Gaps in the application: “Can you tell me why the education section is blank?”
- Additional qualifications: “Do you have any additional certifications or qualifications you would like me to know about?”
- Questions about experience: “Your application indicates two years of healthcare experience; can you explain other experience that may be relevant?”
- Adaptability: “How comfortable are you with change? Can you give me an example of a time when you had to learn a new process and how well you adapted to this change?”

Interview

Interviews are conducted after candidates have been chosen through the preliminary selection process. Interviews can take place on site or via Skype or other video conference options for candidates who cannot come to the physical location, allowing for flexibility to encourage prospective hires. The interview format can be a one-on-one discussion with the hiring manager, a team interview, or a combination of the two. The interview process should be defined in a procedure indicating who will be included and which standard questions will be asked. While the interview format and potential questions should provide a foundation to gain information from each candidate, the format should also be flexible, allowing members of the interview team to introduce new questions based on the interviewee’s responses. To create a flexible interview atmosphere that is most conducive to candidates, it is important to include key stakeholders in the interview process, including:

- Hiring manager
- CDI director/manager
- Members of the CDI team
- Coding professionals
- Nursing specialists
- Physician advisor

The interview process can be intimidating for candidates so it is important to make an effort to reduce their anxiety. Allow space for the candidate to talk about their personal experiences, which can help the hiring manager gauge the candidate in an informal manner. It can also help the interviewer generate questions based on the information offered by the candidate.

It is very important for interviewers to avoid distractions like checking notes to read questions. This approach takes the spontaneity out of the interview and may create a restrictive atmosphere that doesn’t allow candidates to better express themselves.

Questions can be asked about candidates’ previous CDI experience, with the potential to identify and articulate connections between their experience and the processes in place at the interviewer’s organization.

Plan an Organizational Orientation

Organizational Orientation

To ensure success and sustainability, a successful CDI program requires structure. Organizations should address staffing and management of the CDI program within the current human resource dynamics of the organization. A comprehensive department-specific training program with clear objectives should be incorporated into an overall training program for the CDI professional. In addition to organizational training, the CDI professional should have a plan for training specifically geared toward educating the CDI professional.

CDI Program Orientation

It is important for organizations to ensure CDI staff are “thoroughly trained in the principles of high-quality clinical documentation as well as the review of patient records to identify possible deficiencies in documentation.” A collaborative training session where nurses, doctors, allied health professionals, and seasoned CDI professionals are present is highly recommended in order to give the new CDI professional a well-rounded view of the program.

Training for CDI staff should include three parts:

- Training in the theory of high-quality clinical documentation
- Training in the physician query process
- Training on how to collect and analyze data for the program

Training in the theory of high-quality clinical documentation

Training in the theory of high-quality clinical documentation should include the fundamentals of coding and reimbursement, and should cover how high-quality clinical documentation affects the reimbursement process. CDI staff should be knowledgeable of current coding guidelines in order to determine if documentation provided in the health record is sufficient to appropriately identify the severity of illness and risk of mortality of the patient being treated. The CDI professional should also be trained on the basics of quality indicators and how inadequate documentation can affect the organization’s quality scores.

Diagnosis Related Group (DRG) Training

An important aspect of CDI training and education is understanding the impact of severity diagnoses and its relation to Diagnosis Related Groups. Some organizations provide a specific list of diagnoses to be queried by the CDI professional as ongoing initiatives. This list is usually comprised of commonly occurring severity diagnoses—comorbid conditions or major comorbid conditions—while other organizations educate their associates on query opportunities per major diagnostic categories. The final group of CDI programs educate CDI professionals on understanding DRGs and coding concepts. For further guidance on educating CDI professionals on understanding DRGs and coding guidelines and practices, please refer to Appendix A, included in the online version of this Practice Brief.

Training in the Physician Query Process

Training in the physician query process is a critical component of the clinical documentation improvement process. CDI pro-
fessionals should be trained on appropriate ways to review a health record to identify documentation deficiencies, when a physician query may be needed, and the parameters for constructing a compliant query. According to Hess, “The record review process should include addressing all components of the patient record as possible sources for query opportunities.”

In general, physician queries should be constructed to clarify conflicting, ambiguous, or incomplete information, obtain clinically relevant information not previously addressed within the current documentation, and clarify present-on-admission indicator assignments.

For more information on constructing a compliant query, reference AHIMA’s 2019 Practice Brief titled “Guidelines for Achieving a Compliant Query Practice” and the AHIMA Inpatient Query Toolkit. Both are available online in AHIMA’s HIM Body of Knowledge.

Training On Data Collection and Analysis
CDI professionals should be trained on how to collect data, how to analyze the data collected, how to enter information into the program database, and how to formulate and organize the data for a physician query.

The collection of program data should include the identification of:

- All cases reviewed
- The number of cases with queries
- The nature of the query
- The physician’s response to the query

Post-Training Evaluation
After initial training of CDI staff, a post-training evaluation should be conducted to ensure the appropriate transfer of knowledge has occurred and the CDI professional has a strong grasp on key concepts. Post-training evaluation can also include a “shadowing” program in which more experienced CDI professionals within the organization shadow newer staff in order to ensure an effective training process.

Ongoing Education for CDI staff
Ongoing education for CDI staff is crucial to the ultimate success of the CDI program. Ongoing education can include additional coursework to obtain credentials such as the Certified Documentation Improvement Practitioner (CDIP). Ongoing training can also include choosing specific cases for review within the CDI group as a learning opportunity to help all staff continue to develop skills.

For more on current and future trends in CDI, please see the extended online-only version of this Practice Brief, available in AHIMA’s HIM Body of Knowledge.

Notes
2. Ibid.
IN 2007, THE Institute of Medicine set a vision for the evolution of the healthcare record in the digital age. That vision, Learning Healthcare System, described a future in which data recorded in an electronic health record (EHR) would support clinical care and decision-making. That data would then be securely re-used to improve the process of healthcare delivery, clinical research, and the needs of public health for population health management in a continuous cycle of process improvement. To achieve that vision, data in the EHR should be managed to support semantic interoperability, expecting that a data item can be transmitted to a different computer system, recognized for its meaning or semantics, and re-used by that computer system without human intervention. Although the Office of the National Coordinator for Health Information Technology (ONC) has specified a plan for achieving interoperability in the United States, data re-use still faces major challenges due to inconsistent and incomplete terminologies, fragmented information architectures, and proprietary information management schemes.

Data Maps
One common approach to the re-use of data from one computer system to another is to employ a data map, sometimes called a cross map. The International Standards Organization (ISO) defines a data map as the creation of links from concepts or terms in one classification, terminology, or ontology to another for some purpose of data re-use. Maps are built to meet specific business requirements and serve one or more use cases, activities, or step-wise descriptions of events that describe real-world employment and expected outcomes resulting from a piece of software or data map, for re-use. The links that are used in constructing the map are driven by the use case and the editorial features of the two terminologies. For semantic (the meaning of a concept) interoperability, an equivalence between the two concepts would be desirable, but this is not always achievable. Theoretically, identifying computable semantic equivalence is only reliable between two well-constructed ontologies with overlapping semantic domains—they apply to the same types of concepts such as diagnoses—and also share a concept model, or “the set of rules that determines the permitted sets of relationships between particular types of concept.” Since this is seldom true, the majority of maps have a directionality to the link, mapping from a concept usually in the source terminology from which the data originates to a concept in the target terminology, and the terminology to which the concept links. This helps employ a type of link or relationship which serves the pragmatic purpose of the use case. Maps can be developed, published, and shared as simple tables identifying pairs of concepts from source and target, “triples” in Resource Description Framework format constructed as records linking source, relationship (link type), and target, or as a knowledge resource which might consist of a network of IF-THEN rules supporting context-based mapping.

Mapping Purposes
Maps may be employed throughout the healthcare domain for a variety of purposes and to meet many different use cases. ISO suggests that there are three general goals or purposes for data mapping:
1. Converting legacy data to newer coding schemes
2. Re-using data for purposes other than originally intended
### Table 17.1 Purposes of data map creation and interoperability of clinical terms

<table>
<thead>
<tr>
<th>Table</th>
<th>Use Case</th>
<th>Example</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data conversion</td>
<td>Map EHR data from a legacy coding system to new standards</td>
<td>Convert coded diagnosis records from ICD-9-CM to ICD-10-CM: General Equivalence Mappings (GEMs)</td>
</tr>
<tr>
<td>Re-use</td>
<td>Choose medication records from the EHR corresponding to orders with a specific treatment reason</td>
<td>RXCLASS mapping of RxNorm medications to VA drug classes to identify cancer therapies</td>
</tr>
<tr>
<td>Re-use</td>
<td>Map SNOMED CT conditions to ICD-10-CM for reporting morbidity and mortality</td>
<td>NLM release of SNOMED CT – ICD-10-CM rules-based map</td>
</tr>
<tr>
<td>Interoperability</td>
<td>Extend and integrate terminology standards across domains for interoperability</td>
<td>The SOLOR project</td>
</tr>
</tbody>
</table>

3. Semantic interoperability of data where computer systems are using different coding schemes. (See Table 17.1.)

### Types of Maps

Historically, data maps have been constructed employing a variety of approaches and can serve many different use cases. There is no standard for classifying data maps, although the ISO technical document does specify a set of quality indicators as noted in the following section. A data map may be described minimally based upon the protocols involved in creating map records, the nature of the link used in the map, or by the characteristics of the terminology resources that are linked. Therefore, a descriptive map type may be assigned as a list of one of each of the following descriptive sets.

#### Mapping Protocol:

- **Lexical mapping:** Identifies sets of terms to be linked by comparing words or character strings and is very dependent upon the language and dialect employed. The National Library of Medicine’s (NLM) MetaMap program supports mapping of biomedical text to concepts in the Unified Medical Language System (UMLS) and is an example of a lexical approach.

- **Semantic mapping:** Employs the full defined meaning of a concept in a source reference terminology or ontology to identify equivalent or related concepts in the target. A reference terminology is a controlled terminology employing a set of terms and relationships which capture and define the meaning of each concept. The map of SNOMED CT to ICD-10-CM discussed in the use cases later in the chapter is an example of a map that was constructed semantically.

#### Nature of the Link Relationship:

- **Equivalence maps** are designed to identify pairs of identical concepts between the source and target. Semantic equivalence and lexical equivalence can lead to very different types of map sets that may not serve the same use cases well.

- **Hierarchical (Taxonomic) maps** order sets of concepts as having more or less specificity when traversing from source to target. They employ link relationships such as “less-than,” “child-of,” “more-specific than,” or “is-a.” A classification such as ICD-10-CM includes such implicit relationships which specifies its hierarchical structure.

- **Knowledge-based (Rules-based) maps** employ features of coding context, business case, and workflow assumptions, which apply to the interpretation and application of map records, in order to create maps for terminologies where the standards developer imposes constraints on the use of the terminology scheme. The best example of a knowledge-based map is the map of SNOMED CT to ICD-10-CM in which World Health Organization (WHO) classification guidelines and additional context from the patient demographics and problem list are employed by a set of rules to map each SNOMED CT concept recorded as a problem (condition) in the EHR.

#### Characteristics of the Source and Target:

Maps may be typed based upon the nature of the terminologies involved in the map records, which may include classifications, controlled terminologies, reference terminologies, or ontologies. A map such as the SNOMED CT to ICD-10-CM map may be described as “reference terminology to classification.”

### Notes


*James R. Campbell is a board-certified physician and a professor of medicine at the University of Nebraska Medical Center.*
CAPTURING SOCIOECONOMIC DATA, also referred to as social determinants of health (SDOH), is rapidly becoming a necessary element of documentation. SDOH “are among the most influential factors that determine health outcomes of individuals,” according to the National Quality Forum. The move toward pay-for-performance in the United States has led more health care providers to use and report SDOH, including accountable care organizations (ACOs) that rely on providers to help identify patients at risk due to SDOH. As capturing this data becomes a necessary part of encounter documentation, clinicians and allied health staff can turn to the ICD-10-CM code set for help.

Before considering the following three sample determinants, consider who can report them. Historically, coding professionals have relied upon the patient’s provider to explicitly identify circumstances reported with an ICD-10-CM code. There are exceptions in the guidelines, however, including pressure ulcer stage, body mass index (BMI), and coma and stroke scales. For 2019, Guideline I.B.14 has been amended to allow coding professionals to report SDOH using the documentation of clinicians other than the patient’s provider. When using documentation provided by non-physician clinicians, SDOH codes may be assigned. With that in mind, consider the following three determinants.

**Determinant One: Low Income**

Low income has been identified as a key social determinant of health. While the effect of income on health has been the subject of debate and study, research appears to uphold the link between low income and health.

ICD-10-CM coding options include:
- Z59.5 extreme poverty
- Z59.6 low income

There are no Coding Clinic references for these codes or their ICD-9-CM predecessor, V60.2. The federal government’s definition of poverty may provide guidance. Poverty-level income, according to this definition, is as follows:
- $12,140 for individuals
- $16,460 for a family of two
- $20,780 for a family of three
- $25,100 for a family of four
- $29,420 for a family of five
- $33,740 for a family of six
- $38,060 for a family of seven
- $42,380 for a family of eight

Of course, poverty is not synonymous with low income. Low income has been defined as less than 200 percent of the poverty value. The poverty values above can be extrapolated for Low Income as follows:
- < $24,280 for individuals
- < $32,920 for a family of two
- < $41,560 for a family of three
- < $50,200 for a family of four
- < $58,840 for a family of five
- < $67,480 for a family of six
- < $76,120 for a family of seven
- < $84,760 for a family of eight
Values at the low end may be helpful, but noting the US median household income of $61,372, values at the upper end may be less useful. Nonetheless, this table may be helpful in setting a definition for the "low income" relevant to Z59.6.

The US Census Bureau defines "deep poverty" as living in a household with a total cash income below 50 percent of its poverty threshold. Substituting "deep poverty" for "extreme poverty" and applying the "deep poverty" definition to the poverty level tables yields the following numbers for deep poverty/extreme poverty income:

- < $6,070 for individuals
- < $8,230 for a family of two
- < $10,390 for a family of three
- < $12,550 for a family of four
- < $14,710 for a family of five
- < $16,870 for a family of six
- < $19,030 for a family of seven
- < $21,190 for a family of eight

These values, the highest of which barely surpasses one-third of median household income, seem to reflect dire economic circumstances. Having established some parameters for low income and extreme poverty, the next challenge would be verifying the same.

Collecting tax return data would impose a number of burdens upon providers and allied health staff before consideration of what is arguably the financial equivalent of HIPAA—1999’s Gramm-Leach-Bliley Act. At the provider level, collecting and retaining objective data may be unworkable. If the provider is part of a health system, some data may be available at the system level—for example, if the patient is in the system’s Health Care Assistance Program. Absent the same, and given a likely unwieldy circumstance of gathering and retaining income data at the provider level, using subjective data provided by the patient may be necessary.

Subjective measures can gauge objective states. Using subjective data to assess income is not inconsistent with techniques used by the Census Bureau. In the absence of a system mechanism to capture and score objective financial data, providers and practices should consider a set of subjective screening questions to identify circumstances that reflect Z59.5 or Z59.6. Consider permutations of questions for patients about their level of difficulty in completing tasks related to their healthcare, such as filling a prescription, taking into account the subjective data elements used by the Census Bureau. There should be practice- or system-wide consensus in the assignment of codes based upon this subjective questioning.

**Determinant Two: Food Insecurity**

The concept of “food security”—and its opposite “food insecurity”—dates back to the Life Sciences Research Office (LSRO) of the Federation of American Societies for Experimental Biology report based on the ad hoc panel convened in 1989 for the American Institute of Nutrition, subsequently published in the Journal of Nutrition. Studies appear to link food insecurity to a number of health problems among the general population as well as increased assistance with activities of daily living (ADLs) for seniors. ICD-10-CM coding options include Z59.4, lack of adequate food and safe drinking water.

Again, there are no Coding Clinic references for this code, but organizations such as Hunger Vital Sign point to this code as appropriate for reporting food insecurity. There are question sets that can be employed to gather subjective data, the result of which may trigger reporting Z59.4. The USDA has a short questionnaire that has been found to be an effective measure of food security. The form is available at https://www.ers.usda.gov/media/8282/short2012.pdf.

The questionnaire includes a simple raw score template based upon affirmative responses. Results fall into one of three categories: high or marginal food security, low food security, or very low food security.

Reasonably, code Z59.4 is reportable with this measure of low or very low food security. The USDA subjective questionnaire gives providers and staff a tool to assess food insecurity. As previously mentioned, the code description does not explicitly mention food insecurity but Hunger Vital Sign does point to this code for reporting food insecurity. There should be practice- and system-wide consensus to assigning code Z59.4 based upon a standard questionnaire.

**Determinant Three: Housing Instability**

Studies have established a link between housing instability and decreased health outcomes. According to the National Quality Forum, “Individuals who are housing unstable have also been found to be more likely to visit an emergency room, have longer hospital stays ... and have higher likelihoods of readmission.” Housing instability is an important social determinant of health. ICD-10-CM coding options include:

- Z59.0, Homeless
- Z59.1, Inadequate housing
- Z59.2, Homelessness
- Z59.4, Lack of adequate food and safe drinking water
- Z59.5, Food and safe water assistance
- Z59.6, Very low food security
- Z59.7, Low food security
- Z59.8, High or marginal food security
- Z59.9, Food security unknown

ICD-10-CM synonyms for Z59.1 include “lack of heating,” “restriction of space,” and “technical defects in home preventing adequate care.” There are no Coding Clinic references for these codes or their ICD-9-CM predecessors, V60.0 and V60.1. The Centers for Disease Control and Prevention has set forth a definition for inadequate housing, available at https://www.cdc.gov/mmwr/pdf/other/su6001.pdf. According to this definition, “Inadequate housing is defined as an occupied housing unit that has moderate or severe physical problems—deficiencies in plumbing, heating, electricity, hallways, and upkeep.”

The American Housing Survey defines “severely inadequate” based on an affirmative response to any of the following:

1. Unit does not have hot and cold running water.
2. Unit does not have a bathtub or shower.
3. Unit does not have a flush toilet.
4. Unit shares plumbing facilities.
5. Unit was cold for twenty-four hours or more, and more than two breakdowns of the heating equipment have oc-
curried that lasted longer than six hours.
6. Electricity is not used.
7. Unit has exposed wiring, not every room has working electrical plugs, and the fuses have blown more than twice.
8. Unit has five or six of the following structural conditions: a. Unit has had outside water leaks in the past twelve months. b. Unit has had inside water leaks in the past twelve months. c. Unit has holes in the floor. d. Unit has open cracks wider than a dime. e. Unit has an area of peeling paint larger than eight by eleven inches. f. Rats have been seen recently in the unit.

Consider developing a facility questionnaire to accurately report Z59.1. While circumstances that would point to reporting the Z59.0 code might initially appear more straightforward, that may not be the case. Homelessness is a sensitive issue that’s often denied because of shame and stigma. Asking patients if they are homeless may not yield a straightforward response. When individuals do not have a home address, they sometimes provide the address of a local church, shelter, friend, or relative.12

Again, consensus on subjective data can provide the documentation that warrants reporting codes Z59.0 or Z59.1.

SDOH: The Way of the Future
The continued evolution of healthcare reimbursement, including pay-per-performance and emphasis on disease management, makes SDOH increasingly important. If objective income, food, and housing data are gathered and verified at the system level, providers and coding professionals can use that data to report SDOH-related ICD-10-CM codes. Systems may rely upon providers to help identify SDOH-related at-risk patients and obtaining and retaining objective data at that level may be problematic. In the absence of objective data, subjective data gathered through the use of standardized patient questionnaires, coupled with practice or system-wide consensus on scoring, can provide the documentation necessary to report SDOH-related ICD-10-CM codes.

Notes
THERE’S STRENGTH IN NUMBERS. Building a pipeline of highly-qualified health information professionals has been our passion for more than 90 years. Education is the foundation of that charge. That’s why our resources are designed to help move the profession forward by supporting educators, students, and professionals. The HIM profession will thrive as we continue to work together to leverage our individual experiences and build a collective movement to advance learning opportunities.

OUR COMBINED IMPACT COUNTS.

- **45** authors have contributed to more than 50 book titles currently available to support the expansion of HIM knowledge. Visit ahima.org/ahimapress
- **15,000** students are learning to apply theory with hands-on HIM technology experience. Visit ahima.org/vlab
- **114** Council for AHIMA Excellence in Education (CEE) volunteers guide HIM education strategy in six key workgroups. Visit ahima.org/cee
- **30** years of equipping HIM educators to prepare tomorrow’s workforce. Visit ahima.org/aoe

BE COUNTED IN THE MOVEMENT TO ADVANCE HIM KNOWLEDGE. Visit ahima.org/education
<table>
<thead>
<tr>
<th>SUNDAY</th>
<th>MONDAY</th>
<th>TUESDAY</th>
<th>WEDNESDAY</th>
<th>THURSDAY</th>
<th>FRIDAY</th>
<th>SATURDAY</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Privacy and Security Institute, Chicago, IL</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>VUCA &amp; Voices Leadership Training, Chicago, IL</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Clinical Coding Meeting, Chicago, IL</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AHIMA19: Health Data and Information Conference, Chicago, IL</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Privacy and Security Institute, Chicago, IL</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>VUCA &amp; Voices Leadership Training, Chicago, IL</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Clinical Coding Meeting, Chicago, IL</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>AHIMA19: Health Data and Information Conference, Chicago, IL</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>CSA MEETING: NORTH DAKOTA, Fargo, ND</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

52 / Journal of AHIMA September 19
A Look Ahead
Upcoming AHIMA Institutes, Seminars, Workshops, and Webinars

OCTOBER
28–30    ICD-10-CM/PCS Trainer Academy 2.0, Chicago, IL

UPCOMING INSTITUTES, SEMINARS, WORKSHOPS, AND WEBINARS

November
13–15    ICD-10-CM/PCS Trainer Academy 2.0, Baltimore, MD

December
2–4      Inpatient and Outpatient Clinical Documentation Improvement (CDI) Academy, Long Beach, CA

December
2–4      Privacy and Security Training with CHPS Exam Prep, Long Beach, CA

December
2–4      ICD-10-CM/PCS Trainer Academy 2.0, Long Beach, CA

Check www.ahima.org/events for the latest schedule of institutes, seminars, and workshops.

AHIMA Annual Conference

AHIMA19
Health Data and Information Conference
2020 Atlanta, GA
October 13-17

Keep Informed
Resources and News from AHIMA

AHIMA Partners with Area9 Lyceum to Offer Adaptive Learning Features in Educational Offerings
As technology advances, so does the need to evaluate how we approach and deliver education. AHIMA is partnering with adaptive learning systems leader Area9 Lyceum to add an adaptive learning component to health information management (HIM) academic programs. This new technology is being added as an online component to one of AHIMA’s most popular textbooks, Health Information Management Technology: An Applied Approach, Sixth Edition, coming out this spring.

Pitch Competition Coming to AHIMA19: Health Data and Information Conference
This year, the revamped AHIMA Convention and Exhibit, now called AHIMA19: Health Data and Information Conference, will host a pitch competition in collaboration with MATTER, a health technology incubator based in Chicago, IL. According to the challenge statement, the competition is seeking “innovative solutions that improve the connections between people, systems, and ideas to transform health and healthcare.” Possible pitches might address interoperability, patient matching, or social determinants of health, although all ideas are welcome from HIM students and professionals as well as those outside of HIM.

Five entrants selected by public voting and ranked based on judging criteria by AHIMA and MATTER will be invited to pitch their creative idea in front of an expert panel of judges and a live audience of conference attendees on Monday, September 16, giving them invaluable exposure and feedback they can use to refine their concept. Winners also earn cash prizes to fund their ideas. First place wins $5,000, second place receives $2,500, and third place gets $1,500.
AHIMA Thanks Its Loyalty Program Members

The AHIMA Loyalty Program offers organizations the opportunity to better align their marketing outreach with AHIMA’s print, content, and information channels while delivering year-long exposure to AHIMA’s 103,000+ health information professionals.

To learn more about the AHIMA Loyalty Media Program and position your organization for success, contact:
Jeff Rhodes, 410-584-1940, jeff.rhodes@mci-group.com

EXECUTIVE LEVEL

MRO

MANAGER LEVEL

LexiCode
BY EXELA TECHNOLOGIES

AHA Central Office™
An American Hospital Association Service

TruCode®
YOUR SUCCESS. IT’S IN OUR CODE.

HRG
HEALTHCARE RESOURCE GROUP, INC.
Incredible People | Extraordinary Results

Advertising Index

AHA Central Office..........................................................23
AHIMA...............................................................................10, 27, 51
First Class Solutions..........................................................21
Healthcare Cost Solutions..................................................15
MRO ....................................................................................back cover
OPTUM360 ........................................................................7
Perry Johnson & Associates, Inc............................................19
SourceHOV Healthcare, Inc...........................inside back cover
Textware Solutions-Instant Text.........................................18
TruCode............................................................................inside front cover
University of San Diego....................................................5
YES HIM Consulting..........................................................1

Continued from page 37 (“Data and Analytics Drive Effort to Curb Opioid Abuse: A Holistic Approach for Health Systems”)

tion of various healthcare entities, should manage the hub for the prevention engine, and the various players—such as payers, pharmacies, and pharmacy benefit management companies. Disclaimer: The opinions expressed in this article are the authors’ own and do not reflect the view of the organizations the authors work for, or of any other corporate entity.

Notes


Kapila Monga (kapila.monga@gmail.com) and Harpreet Singh (dhaliwal.harpreet@gmail.com) currently work with Cognizant Technology Solutions in its healthcare artificial intelligence and analytics practice.
Continued from page 26 (“PHI Hide and Seek”)  

they need to visit the information systems (IS) department—or have the IS department visit them if the termination is abrupt—to have access to our email server manually removed from their phones. We inventory and document all the mobile devices that are receiving email. And as part of our bring-your-own-device policy, we have the right to wipe an employee’s entire phone if they don’t allow us to remove their hospital access. So far, we have not had to wipe an individual’s phone involuntarily. However, their awareness of our right to do so ensures compliance with our mandate and assures confidence that we have removed all PHI that we possibly can.

Grady: Every time you repair a hole in the dam, you find three new leaks. That is the nature information security in healthcare. Through rapid adoption, IS evolved too quickly as organizations were eager to take advantage of it. As a result, it’s difficult to mitigate risk 100 percent. What we can do is exercise diligence regarding vulnerability assessments and make sure we fill any identified gaps.

Pesci: About 400 decommissioned workstation hard drives were being stored in one of our storage areas. We weren’t certain about the level of data on them, but we discovered that some had PHI information. Therefore, we engaged a HIPAA-compliant recycling company to properly dispose of them, providing documentation of proof of destruction and recycling.

Hidden PHI can expose any healthcare organization to extraordinary risk, regardless of the provider’s size, location, or complexity. Look under every rock, in every corner, and any other place where PHI might reside. The panelists shared examples, such as a storage room with decommissioned equipment—an area that could easily be overlooked. But these vulnerabilities can be found and addressed with the right assessment and mitigation processes.

Notes

Ken Reiher (ken.j.reiher@complyassistant.com) is vice president of operations at ComplyAssistant.

Continued from page 39 (“The Danger of Being Connected”)  

The HHS voluntary guidance publication, described in the preceding list in item five, identifies medical devices as one of the top five cybersecurity threats to the healthcare industry. Offering practical solutions for small, medium, and large organizations, the guidance can be downloaded from the Public Health Emergency website.

Fortunately, within the last year, solutions designed specifically for medical and IoT device security have appeared on the market. These systems leverage automated and intuitive technology to passively scan the network without disrupting the devices or network activity, then parse the network metadata to automatically classify, manage, and safeguard all the devices.

This new visibility into device inventory and communications promises health systems the ability to apply sophisticated machine learning to accurately classify each device and leverage artificial intelligence to baseline its dynamic behavior within the context of a provider network. This additional level of detail should permit clinical engineers and chief information security officers to engage the IT department in defining and implementing actionable policies that significantly reduce exposure to patient harm and regulatory noncompliance.

Healthcare organizations like CHIME and AEHIS have discovered that patient safety risks attributed to medical devices are not contained to the device itself. These risks extend to the network, firewalls, switches, and operating systems. Healthcare delivery organizations are recognizing that medical, IoT, and OT device privacy and security are components of enterprise cyber and privacy risk management. A holistic approach is the only reliable way to deliver closed-loop security for patient safety and critical assets in our hyper-connected healthcare enterprise.

Notes

Ty Greenhalgh (Ty@CyberTygr.com) is the managing principal and founder of Cyber Tygr.
WHEN FAMILIES UNITE TO COORDINATE care for a sick loved one, getting everyone on the same page can feel like playing a high-stakes game of Telephone.

Even when the logistics of getting the patient to their tests, procedures, or hospital discharge planning sessions at the right time do work out, retaining the information conveyed during these encounters presents an entirely new problem. A study published in the American Journal of Surgery found that less than one-quarter of patients discharged from the hospital are able to adequately comprehend the instructions they’re given when they leave. Getting bad news can also reduce comprehension of crucial care-related information.

David Weekly, who recently left his job as head of product for Google’s data center software, is attempting to address these caregiving conundrums with an app called Medcorder, which patients can use to make audio recordings of their doctor appointments. The patients can then share the recordings and corresponding transcripts with the friends and family involved with their care.

Weekly told CNBC that he was inspired to launch the app while he navigated the nation’s broken healthcare system when his father was being treated for cancer. The news outlet also reported that there’s some concern that physicians won’t consent to being recorded, even though the app’s creators pledge to make their platform HIPAA-compliant. However, CNBC pointed out that physicians also had similar fears about the Open Notes Project, which gave patients access to their own clinical documentation. That initiative was roundly applauded by patient engagement advocates, allowing it to overcome physician fears and empower patients in the process. 

New App Gives Patients a Chance to ‘Share This Appointment’ with Caregivers
Need a Coding Expert?

You can count on LexiCode

AN EXELA TECHNOLOGIES BRAND

Visit us at BOOTH 2202

1,000 Providers rely on LexiCode

14 MILLION Records coded in 2018

1,000+ Credentialed coders and consultants

Lexicode.com • 800.448.CODE (2633)

- Remote Coding
  Includes QA and education

- Flexible
  Onshore or offshore solutions or a combination of both

- Accurate
  Highly experienced, credentialed coders and consultants

- Education Opportunities
  Dynamic coding education

- Auditors/Consultants
  To perform audits and interim coding management

- Ready to scale
  Short and long-term contracts available
“You’re only as good as the company you keep.”

Meet Diana Warner, MS, RHIA, CHPS, CPHI, FAHIMA, Director of Client Relations and Account Management. An industry expert with years of experience as an HIM Director and having worked in various leadership roles at AHIMA, she brings extensive knowledge and understanding to MRO clients. Diana is one of many HIM-credentialed leaders on MRO’s Client Relations and Account Management team, which consults with clients to ensure optimization of our KLAS-rated #1 Release of Information platform and service via ROI playbooks, proactive weekly KPI reviews, quarterly business reviews and client surveys.

Learn more: www.mrocorp.com/experts

Reputation is everything. That’s why HIM leaders across the nation’s best health systems trust and rely on MRO’s KLAS-rated #1 Release of Information services and team of renowned experts. Not only do we have a superior reputation for personalized service and quality, we also work closely with clients to make sure they do too. Together, we respond to increasing PHI disclosure volume and compliance demands. Through a combination of the right people and innovative technology solutions, MRO enables clients to deliver high levels of quality, fast turnaround times, compliance and enhanced customer service.

Gain peace of mind and more time back in your day by partnering with the team that has a proven track record for excellence. Diana Warner is just one of the many expert resources you get when partnering with MRO.

Meet us in CHICAGO
BOOTH #1102

**KLAS RATED #1 FOR ROI • AUTOMATED WORKFLOWS • 99.99% ACCURACY • EPIC INTEGRATIONS**