HBMA

LEADING THE BUSINESS OF HEALTHCARE

RCM Advisor

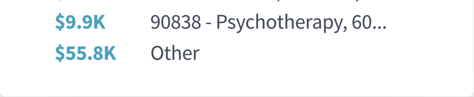
THE JOURNAL OF THE HEALTHCARE BUSINESS MANAGEMENT ASSOCIATION VOL 24 • QUARTER 2 • 2019

THE COMPLIANCE AND DATA SECURITY ISSUE

RETURNED MAIL A Threat to Security?

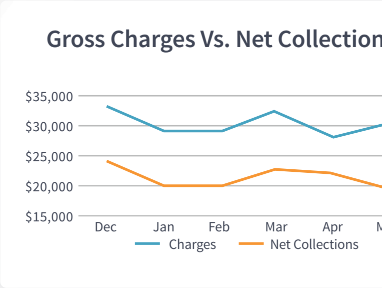
How to properly prepare for RCM risks.

▸▸▸ PAGE 6



$9.9K 90838 - Psychotherapy, 60...

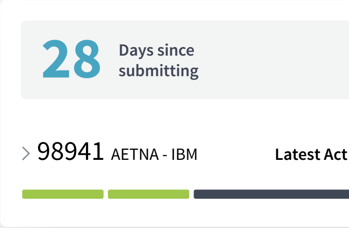
$55.8K Other



Gross Charges Vs. Net Collection

Designed for billers. Trusted by practices.

Kareo's intuitive, cloud-based platform puts billing companies in control of the entire claims process. Whether you're a contract biller, starting a new billing company, or an established organization—Kareo's integrated solution optimizes your workflow and helps you run a more profitable business.

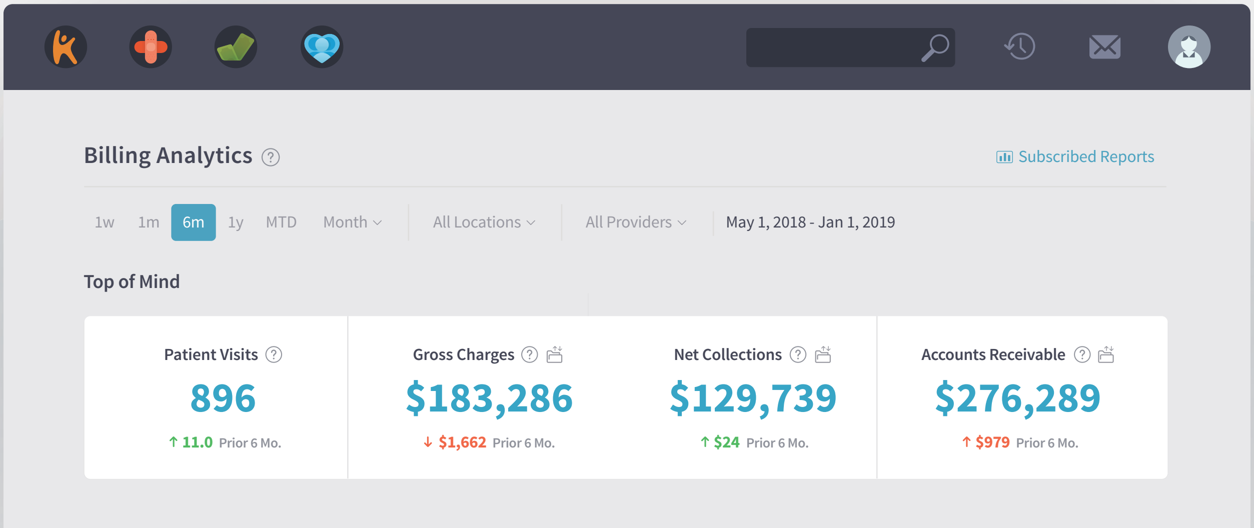


28 Days since submitting

> 98941 AETNA - IBM Latest Act

Use your smartphone camera to learn why 1,600 billing companies trust Kareo. Or visit **www.kareo.com/billing-companies**

Scan Me



Billing Analytics

Subscribed Reports

1w 1m 6m 1y MTD Month All Locations All Providers May 1, 2018 - Jan 1, 2019

Top of Mind

Patient Visits	Gross Charges	Net Collections	Accounts Receivable
896	$183,286	$129,739	$276,289
↑ 11.0 Prior 6 Mo.	↓ $1,662 Prior 6 Mo.	↑ $24 Prior 6 Mo.	↑ $979 Prior 6 Mo.

Staying on Top of Compliance

Our medical billing and revenue cycle management industry is evolving continually. Our companies must be adding expertise, implementing more technology, generating new ideas, and finding operational efficiencies to keep up with competition, pricing pressure, and ever growing client needs and demands. In such an intense environment, it is easy to lose track of the details. It is also often difficult to distinguish our services from those in rival bids for new business.

However, one significant factor that can set our companies apart and show we have moved beyond "billing" into our new world of RCM and more is the level of compliance and security that we have solidified in our daily processes, as well as our overall corporate philosophy and approach. Recognizing this, I engaged with our HMBA vendor partner, the Healthcare Compliance Pros, to embark on the journey to achieve the HBMA Compliance Accreditation. My initial evaluation showed the per FTE model to be a cost-effective way to move into full compliance while keeping my budget tight and internal team focused on daily billing responsibilities for our clients.

To this point, in my own company's compliance efforts, we had developed and implemented a comprehensive compliance plan as well as maintained an active compliance committee for monitoring internal activities and keeping updated on official requirements. However, with the speed of business these days, my concern was not with the strength of our efforts but rather in the information overload that was occurring trying to stay abreast of current regulations or what exposure we may have to risks that we were not even aware existed. As a small- to mid-size RCM company, I was also concerned that regularly scheduled committee meetings, formal minutes, and follow-up tasks could get overlooked in light of prioritizing everyday revenue-generating work. Compliance is not a place where today's RCM company can afford to relax their standards.

Working through the accreditation process has been simple and effective. It is a self-paced, staged, gradual, and customized process. I was relieved to learn that all our existing compliance information could be incorporated into the HCP platform, so all our efforts to this point were not in vain and all our prior records were retained. We have continued to progress through the list of requirements with the assistance of helpful HCP representatives for training, questions and answers, and periodic check-ins to keep us moving forward. Regular reminders are emailed as needed monthly and/or quarterly to keep compliance information up to date and recurring events on the schedule. As we progress with completing each accreditation standard, we receive additional reminders to keep them on track so the program builds on itself and you can continue to meet HIPAA and OIG essentials to maintain the proper level of compliance.

In a recent HBMA Snap Survey, we found that 64 percent of members who responded provide compliance training for clients. The HBMA Compliance Accreditation program is a great way to add credibility and validity to these services, as well as provide clients with more comprehensive assistance. Additionally, 71 percent of respondents provide coding compliance to clients. Included in the HCP package is the ability to ask questions and get advice and consulting to avoid other outside costs, legal fees, etc. while providing these expanded business services to clients. And without surveying, it is fair to say that 100 percent of our companies cannot afford the risks associated with a compliance violation, both financially or to our corporate reputations. I encourage all of you to explore the HBMA Compliance Accreditation program, a great member value. Several members are already completing and being awarded the accreditation seal and certificate and, as a result, are achieving a higher level within the RCM community.

How well does your compliance program measure up? Begin the HBMA Compliance Accreditation process and find out. Already involved? What stories do you have to share about the accreditation process? HBMA wants your feedback.

– Mick Polo, CHBME, HBMA President
mickp@ncdsinc.com

TABLE OF CONTENTS

VOL 24 • QUARTER 2 • 2019

AROUND THE HBMA

DEPARTMENTS

FEATURE ARTICLES

About RCM Advisor

RCM Advisor is published quarterly for the members of the Healthcare Business Management Association, Inc. (HBMA). Editorial offices are located at:

2025 M Street, NW, Suite 800
Washington, DC 20036
T: 202-367-1177
F: 202-367-2177
rcmadvisor@hbma.org
www.hbma.org

EXECUTIVE DIRECTOR
Kurt Gallagher

EDITOR
Alexa Schlosser

GRAPHIC DESIGN
JRocket77 Graphic Design

Articles in ***RCM Advisor*** are the work of the authors and do not reflect the position or opinion of HBMA. No part of ***RCM Advisor*** may be reproduced without the permission of HBMA. Advertising of products or services in ***RCM Advisor*** does not constitute an endorsement by HBMA of those products or services.

LETTERS TO THE EDITOR: Send to **rcmadvisor@hbma.org**, and include contact information. We reserve the right to edit all letters. All published letters become the property of ***RCM Advisor***.

RESULTS

Snapshot Survey on Data Security and Compliance

How do you safeguard your PHI? *RCM Advisor* asked HBMA member companies a short series of questions to find out. Interesting tidbits include 98 percent have a user ID and password policy, but only 42 percent use a password manager, which suggests a lot of passwords may be written on paper. Meanwhile, 68 percent have encryption policies for their servers, but only 43 percent do the same for their workstations. And RCM companies continue to take a wait-and-see position on leading-edge security technologies, with 33 percent adopting multifactor authentication and only 4 percent adopting biometrics (fingerprint, face recognition, etc.). More results are below.

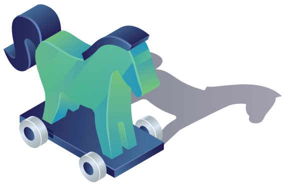
What Are Your Biggest Cyber Security Concerns (Ranked)?

1.

Data theft/hack resulting in breach

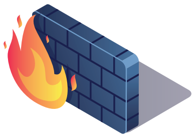
2.

Ransomware attack

3.

Spyware/malware attack

4.

Unauthorized access

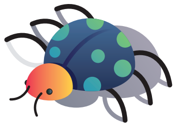
5.

Cyber espionage

6.

Lost device (e.g., laptop, thumb drive) with PHI

7.

Unintended data destruction/loss

8.

Unpatched software

How Much Cyber Liability Insurance Coverage Do You Have?

None

9.4%

Less than $1M

13.2%

$1M to $5M

71.7%

$5M to $10M

5.7%

More than $10M

0%

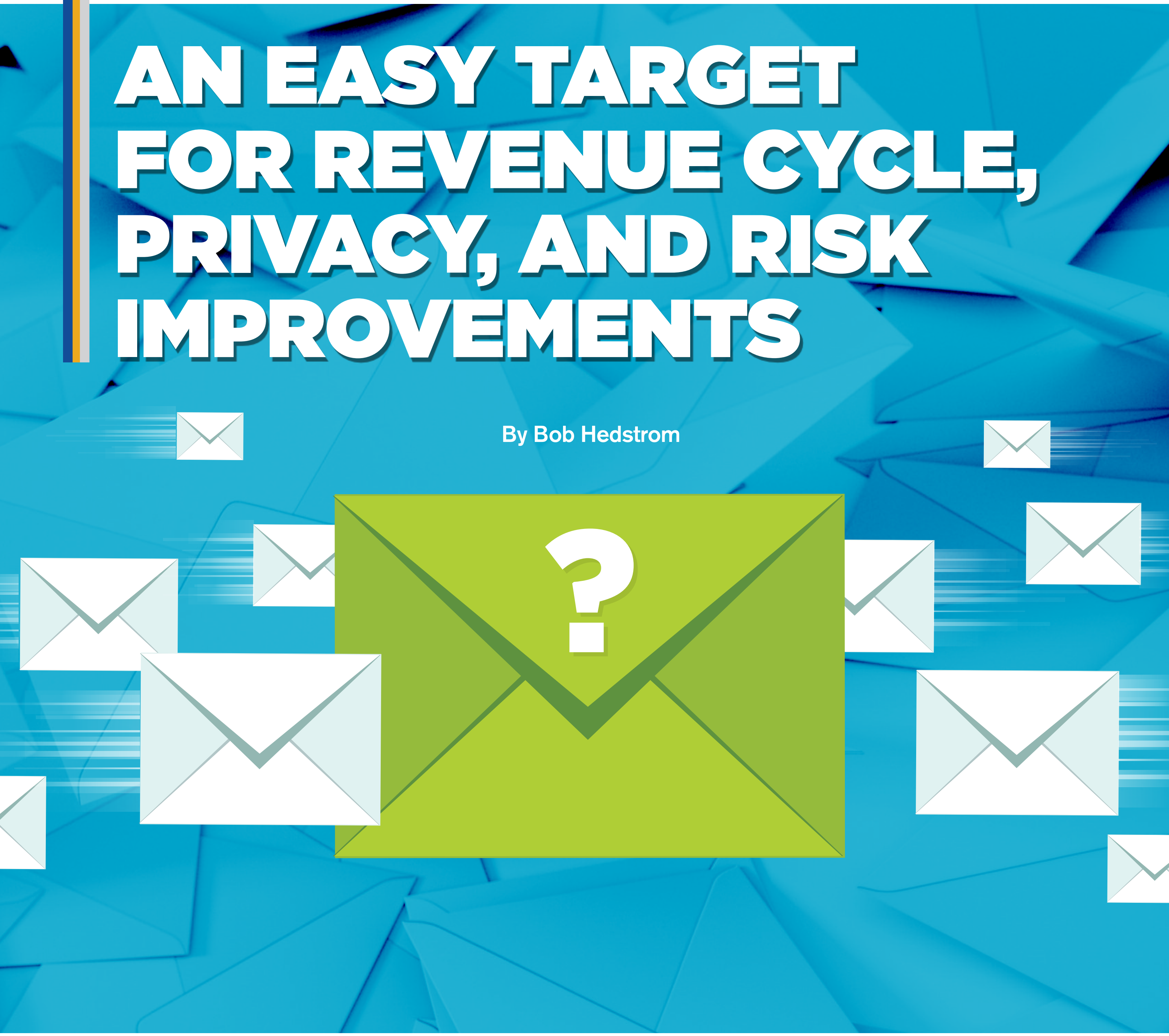
Percentage of Companies that Employ the Following Data Security Safeguards

98.1%	User ID and password policy
96.2%	Data backup or data redundancy
81.1%	Encrypted email
73.6%	Data and hard drive destruction policy
68.0%	Secure attachments
68.0%	Encryption policy for servers
64.2%	Locked server room
43.4%	Encryption policy for workstations
43.4%	Bring your own device (BYOD) or mobile phone policy
41.5%	Password manager
34.0%	Multifactor authentication for workstations
24.5%	Interactive login security message
3.8%	Biometric workstation security

RETURNED

AN EASY TARGET FOR REVENUE CYCLE, PRIVACY, AND RISK IMPROVEMENTS

By Bob Hedstrom



MAIL

The risk of returned mail and how to properly prepare for it.

Any company engaged in healthcare that mails critical communications may run into challenges when it comes to returned mail.

The first time I saw a mail piece with a yellow sticker around 2000, I had no idea what it was. I visited with thousands of organizations—hospitals, banks, insurance, utilities, and everything in between. It seemed everyone was getting these pieces of mail. Even with an increase in electronic bill presentment and payment and reduction of first-class mail, everyone was still getting trays and trays of returned mail.

Not long thereafter, I was asking many questions to better understand what departments were and were not doing with all of this returned mail and with resolving customers' accounts. I then thought healthcare would be a good place to start to fully understand the issue, because as patient bill amounts were large, systems and processes were fragmented, and the complex nature of information technology was increasing. This had to be an issue in revenue cycle, with something as simple as a lost patient and a bad address. Even if a patient wanted to make a payment, would they really be thinking about it if they never received their statement? Much worse, what if they never received their statement and then ended up in collections because of a bad address? This was, and still is, a reality. I started walking out of hospitals with boxes of returned mail for analyzing, without a business associate agreement.

Why Mail Is Being Returned

Let's start with the patient. We encourage healthcare providers to take all possible steps during an encounter with a patient to properly verify insurance information, their ability to pay, and their address in order to collect a full or partial payment at time of service. This can certainly help volumes decrease but by no means will take care of the issue. The patient encounter could be today, and the patient could move tomorrow. In 2017, 11 percent of the population moved—96,000 people each day. The USPS reported in 2017 that there were 2.1 billion pieces of undeliverable mail, or 3.6 percent of all outbound first-class mail. We estimate this issue costs U.S. businesses up to $65 billion each year, with provider and payer returned mail comprising 20 percent of the overall U.S. issue.[1] For percent of outbound mail, provider-returned mail averages 4 percent, depending upon the volume of repeat statements being mailed.

When you do the math, if there are 100,000 statements mailed and 3,600 returned, at $500 average patient due, then that equals $1.8 million in outstanding patient debt that must be resolved. The main questions are how fast does that happen and at what total cost?

Seventy-six percent of all returned mail is because of movers. The USPS has a National Change of Address (NCOA) process, in which the consumer or business files a formal move. Approximately 50 percent of the population completes this process and informs of the move; 50 percent do not, and this is the main reason you have an issue.

Trends for Dealing With the Issue

Even today, I am still amazed that the healthcare sector believes that NCOA takes care of the issue. This misconception is further complicated by companies claiming that their solutions will eliminate returned mail. There is only one way to eliminate returned mail: do not mail. The reality is that mail will always be here and, while overall volume of first-class mail has decreased over the years, 77 percent of providers still use paper-based patient billing methods.[2]

There are also now a wide variety of solutions being touted in the market. Many companies, and even the USPS, have solutions that will alert you if the mail has been returned. I'm not sure of the real value here, because the mail is not issue—it is the lost patient, their pending receivable, and probable move to collections that is the problem. Some companies offer a more integrated approach, with patient search capabilities, but the overall solution may not yield optimal results for finding patients and avoidance of risk. An easy and inexpensive solution does not necessarily mean the best total solution in terms of savings and risk. It is the vast amount of resources and costs that are expended to try to process, flag, locate, call, and collect the payment from the patient that is the issue. A USPS database called NCOA doesn't take care of this, nor does it give you any phone information or workflow for follow-up. Accounts are not magically resolved when using NCOA, with only 50 percent of the moving population actually filing the move.

I've also noticed a trend where companies are suggesting suppression as the logical answer. Patients are suppressed prior to statements being generated because their postal software stated the address was not deliverable. While the industry would like to save money by not mailing to undeliverable addresses, the short-term savings of 60 cents per mail piece for print and postage unfortunately goes invisible for the issue as the patient account worth $3,000 moves into collections. By this example, at a 15 percent collections rate, the savings of 60 cents ends up as a real cost of $450.

Why are we capturing data from the yellow stickers that separate forwarding addresses from non-deliveries? New addresses make up less than 10 percent of the issue, and these are old addresses as reported by the USPS. Combine that with many errors on the yellow stickers due to lack of carrier consistency and coding reasons, and you have a lot of expense for very little return. For now, it is not a regulatory requirement for providers that information be captured, imaged, or archived from the envelope itself. While we do look at these reasons for some customers due to regulatory requirements, we recommend bypassing this process with the bulk of our customer base, as software yields positive results on the majority of bad addresses processed and records new moves and phone information as recent as yesterday.

The patient must be resolved by some means before they move to greater resources and potentially a collections activity.

The Rise of Omnichannel

Collections should be viewed as an omnichannel opportunity. A true omnichannel approach is integrated where outcomes and interactions are stored centrally using SMS, email, chat, letters, IVR, web, and kiosk. According to Fiserv, 43 percent of consumers say having multiple billing and payment options improves satisfaction with their biller. When options are seamlessly managed across different channels in a way that presents a single, customer-focused entity, chances of success collecting a debt increases significantly.

Fifty-six percent of smartphone users would be more encouraged to make a payment via a mobile phone if it was as simple as paying with a single click.[3] Giving power to the consumer for how they want to interact is key to any omnichannel approach. Enabling customers to choose to be notified through outbound messages regarding upcoming payments and past due accounts has the potential to greatly reduce delinquencies.

The omnichannel approach has to make it easy for the consumer to do business and avoid confusion—something as simple as a traditional paper statement with links to a secure online payment form for self-service payments. Some of the biggest roadblocks with true omnichannel lie with systems, IT and integration, and the fact that there is no silver bullet for making it all seamlessly happen.

The use of mail as a key form of communication and driver of action still exists today. Use of mail with SMS, web, IVR, and other forms of omnichannel communications can only help drive more positive outcomes. Having a robust platform for managing the resolution of lost patients from returned mail, along with technology for reminders, updates, validation events, and payments, can make the customer experience seamless.

Connect Earlier With Lost Patients Through Automation and RPA

With rising patient populations of self-pay and high deductible plans, managing accounts receivable is becoming increasingly difficult. Many providers do not have staff to manage the post-encounter process and have opted for early-out collections on day one, with turning bad debt accounts over to contingency agencies thereafter. Increasing patient bad debt increases the workload to handle more, low-value self-pay accounts. Bad debt now comprises 60 percent of uncompensated care, while self-pay has increased 10 percent in the past five years.[4] With the patient now becoming the number three payer behind Medicare and Medicaid, self-pay and high-deductible plans leave patient balances that must be collected upon.

Collecting a bill earlier in the patient life cycle means it does not have to be collected at the back end. It costs four times more to collect from a patient than it does from an insurance company.[5] Odds on collecting on any debt grows worse the longer the debt remains unpaid. The national average for bad debt is 3.31 percent, with the Southeast region of the United States having the highest percentage of total uncollectable accounts at 9.92 percent.[6]

Chief financial officers and other senior finance executives from more than 350 hospitals, health systems, and other healthcare organizations say the No. 1 priority for 2018 was cost reduction.[7]

The goal should be to get to the patient early, connect with them, and collect early by deciding upon a payment plan without allowing the account to age. While all companies have priorities, solutions should be reviewed that can have the most value and highest payback with minimal disruption.

The issue of patient financial responsibility and AR is made worse by outdated patient information. Robotic process automation (RPA) can provide many automation tools for processing, locating, reconnecting and receiving address updates, validation, payment, fraud, risk, and compliance.

There are very flexible and configurable RPA solutions in the market today that can intercept returned mail, find lost patients, proactively reconnect, drive payments, provide a validation process when needed, feed auto dialers, update multiple HIS platforms, and even provide automated work queues to customer service, compliance, and risk, and can be implemented in 30 days, not one to two years. The problem with healthcare is healthcare. There are changing regulations, privacy policies, cybersecurity threats, rising costs, fewer patient payments, decreasing resources, manual processes, errors, and a virtual technology jungle of systems that don't connect.

At least for this issue, the future can be brighter. Instead of sending patient accounts right away to an early-out activity or to that the person who sits at the front desk and "finds patients," why wouldn't you look at using multiple solutions in tandem to get visibility to the issue, find a resolution and lower overall costs? Like any omnichannel strategy, there is no silver bullet here either. Use RPA solutions for immediate impact—and at a much lower cost structure—then move remaining accounts with issues to a more expensive, more involved process or activity.

According to a recent InstaMed Payments Report, 30 percent of the average healthcare bill now comes from the patient's pocket. The problem with looking at more effective technologies like RPA is that healthcare is too busy—too focused on the daily fire and the never-ending list of other priorities. While not ideal, status quo is acceptable.

The High Cost of Not Reviewing Other Technologies

With the chart below, the cost of resolving 1,000 accounts from early-out day one at 7 percent is $35,000. As a similar comparison, the cost of resolving 1,000 accounts from RMS is $19,170, or nearly 50 percent of early out. By this example, a more expensive early-out solution could be used after RMS and/or a set number of days. The combined solution will help reduce accounts receivable days and at the same time the cost to collect.

EXAMPLE: 20,000 patient accounts, each with a patient due responsibility of $500, equals $10 million

Industry Tools	When	New Address	New Phone	End-to-End SSN/DOB Match	Customized Workflow	Risk RPA	AR to Collections	%
Early Out	Day 1	Yes	Yes	Input	NA	NA	$5,000,000	100
USPS NCOA	Pre-Mail	6%	NA	NA	NA	NA	$4,900,000	98
Skip Tracing	Post-Mail	30%	Yes	Input	NA	NA	$4,625,000	94
RMS	Post-Mail	60%	Yes	Yes	Yes	Yes	$4,100,000	85

**Assumes a 30% self-pay rate on mailed items, deliverability rates vary*

Be Open to Alternative Technologies and Industry Improvements

Today, most providers we speak with know they have the issue, but a high majority will state they have it taken care of. Oddly enough, healthcare is the industry with the biggest dollars to lose to the issue, and one of the biggest for telling us they "have it covered." In speaking with many revenue cycle and finance executives, the majority are not fully exposed to the issue, and they lack good metrics, analysis, and data that provides a solid understanding to the overall financial impact of this issue. We've looked at net gains of up to $50 million annually with providers, implemented in 30 days across all systems—no call back. With approaching the subject of improvements, typical responses include:

- This isn't a priority.
- This isn't that big of a problem.
- My early-out vendor/collections team manages that.
- IT is backed up for the next one to two years with a systems conversion.
- We're not taking on any new vendors.
- We're solving that problem before we mail.
- We're trying to eliminate mail.
- We already have that solution with another vendor.
- The USPS takes care of that.
- We text and email.

We strongly encourage you to at least look at options and all of the differences in the various technologies that are in the market, as they are vastly different. We're meeting more and more with privacy, risk, and compliance as a major driver to ensuring the safeguard of patient information, risk with incidents, and with chain of custody to patient data. One of the biggest issues they have right now with patient data is with chain of custody. With all of the vendors, devices, systems, and business processes, providers don't know where all of their data is, nor have an audit trail on data. The industry has to change with technology as payments decrease and self-pay and patient responsibility increases.

Solutions can also operate and work in tandem with existing infrastructures, programs, systems, and technologies; they configure to your environment, governance, and unique requirements instead of the opposite. I've broken a life cycle process into a few segments.

Capture

The process starts with the capture of physical returned mail, and with providing an audit trail behind every single patient that is lost due to the issue. Most companies cannot provide an audit trail to the account and actions taken internally and/or externally as to the life cycle of resolution to the problem, thus providing operational risk. The mail is not the issue—the issue is lost patients, usually with an outstanding AR. Patients most likely would support a warm introduction and plan options for payment, delivered to their mailbox as well as pushed through omnichannel means, rather than a collection call or letter to ask them how they are going to immediately pay their $3,000 patient balance.

Each document is a carrier of data that can be extremely important to RPA and AI. Have we seen the patient before? When? How? Can accounts be moved automatically for workflow based on low, medium, and high-balance collections? Can the patient account be auto-managed and electronically moved to an appropriate vendor(s) or internally managed through automated work queues for subsequent follow-up? Providers mail on average 3.5 patient statements per encounter. What if RPA could recognize patients historically over time and make automated decisions based on frequency, outcome, and overall revenue cycle strategy?

RPA can automate these functions for capture and conversion of documents to usable or smart data, and can provide the audit trail and functionality for subsequent automation of platform and patient resolution events.

Customer Resolution and Search

Most internal revenue cycle, early-out and collections vendors utilize tools and databases from well-established companies. These companies represent traditional skip tracing and can provide last known addresses and phone numbers that they individually have on file; these tools have minimums and different costs depending upon specifications around the actual search requirements. Unlike the USPS, they mainly use proprietary and public databases in their process. However, no two databases are the same, and many databases contain errors and even fraud. Even the USPS National

Change of Address database contains fraud. Our customers have also told us there are issues with traditional sources of data. While they are necessary in many instances, with providing data for follow-up and collections, they also can contain a lot of errors on their own right.

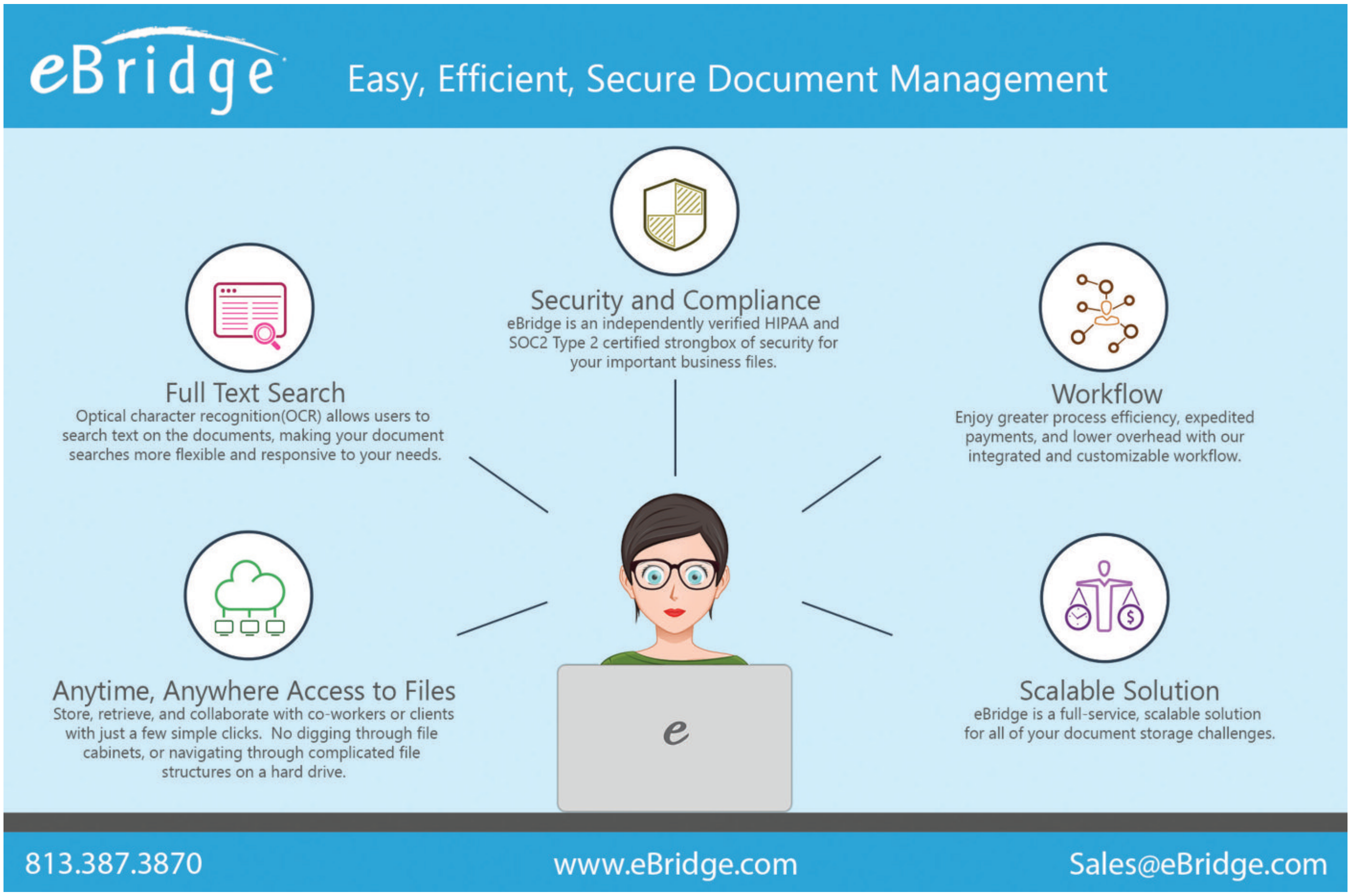
There are new software tools that have been built to outperform single skip and database providers, and can fully integrate with physical returned mail, drive workflow, RPA, and AI. Addresses and phone information can be pulled from thousands of databases and providers, and auto compared, scrubbed, worked, and intelligently processed all in the software. This new paradigm shift for resolving patient accounts is much different than by current methods, which typically rely on a single source, or provider of truth.

When we started building software tools, we thought a high address update rate was king. That has changed over time, with data containing more fraud and errors. Even fraud and errors exist within databases when running SSN-only searches. Individuals sometimes use Social Security numbers that do not belong to them, either in error or deliberately. Thirteen percent of the U.S. population have multiple names associated with a single Social Security number.[8] We have the software built now to yield better results with risk, fraud, and deliverability, but also balancing with a higher update rate. It's an ongoing balance.

Automated software is able to super-scrub addresses against many and also provides an additional layer of privacy and compliance protection. This can all be done without SSN and/or date of birth integration. Those data points and compliance filters within the software can make additional checks, comparisons, and scrubs in mitigating risk with address changes.

Repurposing and Follow-Up

RPA can also be utilized with these new tools for automating the receipt, capture, process, update, reconnection, and



No matter how good you think your current system, vendor, and/or people are—there can always be improvements, and, in this case, there are technologies that are ahead of industry normal practices.

overall management and resolution with the lost patient. Seamless audit tracking of 100 percent of the issue—with updating of data into host system(s)—can be followed by automatic sending of original documents with security information, and/or specific notices, directly to the patient at their updated address. These options can automatically drive the patient to make a payment by web, phone, or payment center and adopt paperless billing, auto pay, and/or even automated validation of address changes. There are also solutions that can proactively feed revenue cycle teams with automated patient collections data for follow up based on specific accounts and outcomes from the overall process.

Companies do not need to employ manual, costly, and delayed resources in doing what can be done automatically through the use of technology. With the use of RPA in automated communications comes configurable workflow based on inbound documents (returns), data elements within the returns (forms and actions), and outcomes from search. Even specific work queues can be driven to different internal associates, and/or routed to departments, tracked, and auto managed for specific events on specific accounts, specific compliance results, and the list goes on.

The ultimate goal is to connect to the patient as quickly as possible, through automation, without human intervention, for the appropriate self-pay or insured balance payment—without restraints associated with inflexible systems, processes, and the errors and delays associated with manual labor. These platforms do exist; you just need to seek them out. I would recommend caution when looking at new solutions, as there are big differences in performance, outcomes, and associated savings.

Compliance

We are seeing big challenges and opportunities with patient privacy, risk, and compliance. We work with compliance officers in all industries in driving new RPA that can provide proactive actions based on regulatory requirements, their individual risk approach, fraud identification, and so on. Combining good compliance with good business operations and full automation is a recipe for success.

One of our first returned mail customers was a very prominent teaching hospital. They had a patient who used a bogus name and address each time they came to their facilities so they could receive free care. At the time (2007), we received the undeliverable billing and kept updating the address to the wrong person. The authorities became involved at a high federal level, and we were put in the hot seat to develop a solution to the problem.

Address fraud is when the thief uses an inaccurate or fictitious address in order to gain money or some other benefit or service they are not entitled to. Medical identity theft occurs when the thief uses a name or insurance numbers to see the doctor, get drugs, or file claims, and can cause major issues, even with collections and credit reporting. Address fraud is usually associated with identity theft.

We helped solve this issue by developing an auditable, trackable technology with fraud alerts that helps identify these issues—especially when patients use old addresses, wrong addresses, and other names just to get free medical assistance. The technology now helps compliance by mitigating risk with patient fraud and address changes and with mitigating HIPAA incidents and reporting.

We do have customers that must legally validate address changes before they update host systems, others that for compliance reasons have chosen to validate, and others that do no validation and rely on us for ensuring we've provided the best, risk-adverse outcome without humans.

By the nature of PHI, we receive many types of documents from many types of providers—some with detailed information about the patient, some without. For over 10 years, we have been sending original patient statements back out to the patient at the updated address, with security information but without validation. We've done this because it was still the better answer for compliance, without resources for validation.

We're now continuing to work with compliance executives in maximizing automation and limiting risk. Instead of mailing original patient documents, we're now sending notices with limited PHI—name and address only, asking the patient to take an action, such as pay a bill, validate via the web, contact customer service, and so on. This has drastically reduced PHI exposure by putting limits on exposure, and with avoiding the need to file a HIPAA incident. Any direct mail piece now has the same information as the notice, therefore reducing risk while automating the location, connection, and payment associated with the patient.

Add to this automatic fraud alerts and/or auto-managed compliance work queues based on visibility to potential fraud and what is seen in data. RPA for compliance can work throughout an integrated platform, if the platform has the capabilities to be fully configurable and flexible. Would there be risk if a patient who visited a healthcare facility in Florida has suddenly moved to Alaska? Perhaps. Every company is different with their own level of risk tolerance and requirements around privacy. These solutions exist today and can be integrated into your overall compliance program for this issue. From receipt of mail to finding the lost patient, to resolution, including automated compliance flags, alerts, and work queues, RPA can be used for compliance and provide a solid answer to typical manual issues processes and decisions.

The Business Case

There are so many challenges within healthcare today that this is an easy target for improvement. No matter how good you think your current system, vendor, and/or people are—there can always be improvements, and, in this case, there are technologies that are ahead of industry normal practices.

With compliance, companies should be looking at operational and financial risk and their own programs. For returned mail, most companies do not have ongoing programs, nor metrics or reports, auditing to align with PHI, gaps, and lost patients.

First, we need to get the industry to stop thinking about returned mail as "mail," with little to no value. It has tremendous value and can provide a quick and financially proven return on investment.

Paper will always be here, and returned mail will not go away. Finding better ways to automate these processes and minimizing the financial and operational impact will be key. ■

Bob Hedstrom is the director of sales, marketing, and product development at Horizontech Inc., a global technology company that solves mission-critical challenges with paper documents and digital data from inefficient, disparate processes, and systems. He founded Returned Mail Solutions Inc. (RMS) and developed, launched, and managed industry-leading complex workflow technologies, Platform as a Service (PaaS) and Software as a Service (SaaS) for end-to-end customer life cycle issues associated with returned mail. RMS was acquired in 2010 by Horizontech and has continued to implement many new technologies for the issue. Hedstrom is considered an industry innovator and leading expert on the subject, has written articles, executive case studies, and spoken at numerous industry events.

Resources

[1] Source: Research performed by Horizontech, Pitney Bowes, data contained within the Christensen Report (an independent Company), as well as the USPS

[2] Source: Medical Group Management Association (MGMA)/Navicure® Digital Payment Progress Report™ Sept. 27, 2017

[3] Source: Focus Financial Services white paper, by Oxygen

[4] Source: 2016 HFMA Self-Pay Study

[5] Source: The Rise of Self-Pay Accounts, The Association of Credit and Collection Professionals, Collector Magazine, February 2015

[6] Source: The Hospital Accounts Report Analysis on Third Quarter 2013

[7] Source: Kaufman Hall 2018 CFO Outlook Performance Management Trends and Priorities in Healthcare

[8] Source: ID Analytics

How Data Analytics Can Revolutionize RCM

Even among the already large amount of information in the industry, data is the way out of the problem.

By Nitin Somalwar

"When I first started out, you could mail out a bill and payers would cover 80-100 percent of what you billed," says Josh Santillan, chief operations officer for Medical Billing Unlimited. "It was pretty straightforward. You didn't have any denials. Now you have denials for CCI edits, LCDs, and specific CPT codes for each payer, and fixing claims is a lot of work on the back end. Claim denials can cause payments to be delayed for six to eight weeks or more."

This quote from a hardworking billing professional sums up the daily dilemma for billing companies and independent practice billing departments across the United States. With the demands of value-based reimbursement looming and the constantly increasing paperwork imposed on all healthcare practices, billing companies and practice billing departments are constantly looking for ways to boost efficiency, enhance collections, and increase their value to their practices and the ones they serve. When every office seems to be drowning in information and its management already, it appears contradictory to suggest that data is the way out of the problem—but those are the facts.

Large healthcare networks and billing companies have already recognized that data analytics can put them ahead of the pack in making informed decisions about patients, practices, and payers. They're implementing data analytics professionals and departments in order to give billers the insights they need to optimize reimbursements and revenues. Independent practices, however, haven't had the personnel or resources to take advantage of the data analytics revolution. Already overworked billing professionals have been stuck with cumbersome manual practices. To determine cross-practice productivity, the biller has had to export data for each practice monthly, then aggregate that into Excel and put it into pivot tables and chart it—just one of dozens of time-consuming tasks.

Now that's changing. Medical practice software is available with practice management software integrated into the EHRs and billing programs that the independent billing professionals are already using. This data analytics software captures more data than ever before, but it makes it easily accessible without the need for IT professionals or analysts that independent practices don't have. This means billers can get the right data in minutes (rather than hours, days, or never) and can spend their time uncovering revenue opportunities. After implementing a robust data analytics module at Medical Billing Unlimited, Josh was able to reduce the time spent on monthly reporting for their practices from almost an entire week to only four hours. Now Josh can repurpose his time elsewhere.

Analytics for independent practices, however, are all over the map in terms of value and limitations, so billers need to review closely to be sure what they're getting is going to give them the knowledge they need. Beware of a lack of transparency regarding formulas and definitions. For example, look at net collection rate. A basic tool calculates this rate using an industry standard formula but doesn't provide any transparency into the actual data and time periods that are used. Without this insight and information transparency, it becomes difficult to draw accurate conclusions and make important decisions related to performance, payroll, and more.

Basic analytics tools also tend to provide a summary view without the ability to drill down into the details. For example, billers may be able to view a sum of payments each month but not dive into a specific line item at the claim level to see precisely where that revenue originates and what services or procedures are denied.

A really robust analytics tool is highly transparent. It will tell users how things are calculated and give them access to the source data. If billers want to do their own calculations manually, they can more easily verify that the information is correct and gain confidence in the analytics tools.

With a robust data analytics tool, billers are able to provide their practices and practitioners with the customizability and flexibility to see their data the way they want, drill in how they want, see any level of detail, and see the values they need.

Robust analytics tools designed with independent practices in mind offer out-of-the-box reports that make the tool immediately useful, while billing professionals go to work on customization. Having these tools at their fingertips, billing professionals can realize greater revenue for their practices and lower expenses through efficiency in their business operations in a number of ways.

There's a great operational benefit to having advanced analytics capabilies. Beyond speeding up regular monthly reporting, like the vast improvement Medical Billing Unlimited has seen, and allowing a biller to deliver on highly customized requests, many practices and billing organizations are also achieving notable improvements in process efficiency by having the ability to use their data effectively. Saved subsets or bookmarks of data allow users to review staff productivity or view a summary of an account manager's practices and drill this info all the way down to line item specific detail, if needed. Managers can easily identify the most valuable activities related to a practice or a billing team and produce a quick but detailed worklist to tackle A/R, denials, etc.

Visibility and visualization of individual practice data helps billing professionals understand their practices more intimately so they can prioritize their work smartly. Using robust analytics for practice data to understand which codes or payers are their biggest moneymakers or have the highest net collection rate, billing managers make productive and targeted worklists for their teams in just minutes so their labor realizes the most revenue for the practice. This visibility also helps billing professionals like Josh play a consultative role in helping the practice prioritize their hiring, organizational, and marketing efforts. When billers can provide this kind of granular data, they become vital and integral partners to the clinicians in the growth and prosperity of the practice.

Among the revenue optimizing insights that robust data analytics can uncover are easy ways to:

- Quickly identify accounts receivable revenue by procedure code, payer, practice, provider, patient by age, amount, or status so that the practice can collect it.
- Check lag times between posting charges, receiving payments, and applying them for faster time-to-revenue.
- Locate claims that have been rejected or denied to get them rebilled quickly and properly.

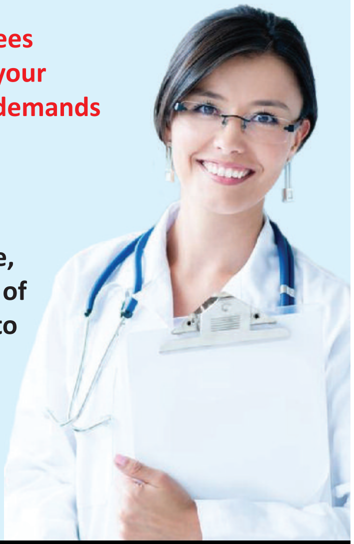
By having the capability to view the entire book of business as a whole, and also to slice and dice it by specialty/size/region/payer/etc., billing companies can identify their most successful practices along with quantifiable reasons they're successful that can be emulated by practices that are identified as less profitable. For example, one billing company was able to help motivate a struggling practice to be more thorough and accurate in its capture of patient demographic and insurance information. In reviewing claim denial rate details across its book of business in a specialty-customized view, the billers compared the claim denial rates between practices, drilled into denial reasons, and gave quantifiable numbers to the practice regarding how updating its front office processes would positively affect its cashflow. When billers use robust analytics tools, especially when managing multiple providers and practices, they benefit not only in terms of being able to trust in the data, but they're also able to answer important questions like:

- **Is the Practice Growing?** With robust billing analytics designed for independent practices, billers can track and trend data related to appointments, visits, and patient volume to determine whether changes in volume are seasonal or whether the business is truly growing. Having this data helps physicians determine whether they may need to hire additional full-time or seasonal staff, including non-physician practitioners.

- **Where exactly is the practice missing revenue?** Billers can glean missed revenue opportunities by identifying the root cause of denials, such as repeated coding or demographic errors. Having this data helps identify the need for physician or staff education.
- **What is the status of cashflow?** A basic tool provides the percent of accounts receivable over 90 days old, but a robust tool allows billers to drill down into why those payment delays occur. For example, is it a lag on the payer side (and if so, why) or an unpaid patient responsibility? Billers become vital consultants to the practices on cashflow.
- **Which payers should the practice contract?** Some payer billing requirements are far more stringent than others, and some take significantly longer to pay. With robust billing analytics, billers can easily glean whether payers pay correctly based on their contracted rates and whether they pay in a timely manner.
- **What data can be used to demonstrate efficiency and accountable care practices?** A robust analytics tool provides data that billers can use to justify the practice's potential contributions to an ACO or other type of innovative care model. Customizable reports can serve as a 'data resume' to prove efficiency.

No matter how overburdened billers feel with the torrent of data they collect, the ability to answer questions like these and to customize and shape that data into the vital information they need is an advanced capability that takes billing professionals to the next level and secures their position as a vital resource to their clinicians. It's a secret to success. ■

Nitin Somalwar is vice president and general manager of the billing company channel, Kareo. More information can be found at www.kareo.com



We Must Be More Than Just Aware of Our Offshore Vendors

Navigating regulations overseas.

By Chad Schiffman

The digital revolution is in full swing, as paper processes disappear across industries. Mail volumes declined by 5 billion pieces, or almost 4 percent, in 2017, according to the United States Postal Service. Online shopping increased six times faster than brick-and-mortar shopping during the 2017 holiday shopping season (First Data), while a record 7,000 retail stores closed or were set to close in 2017 (Fung Global Retail and Technology). The world we live in is being shaped by tech giants like Apple, Amazon, and Uber who are giving us access to more and more at our fingertips. Yet the healthcare industry has somehow managed to resist the digital revolution and continue to rely on inefficient paper processes.

Not too long ago, we were asked a question regarding a CMS requirement for plan sponsors to account for the identification of offshore vendors. Specifically, does the requirement of identification of offshore vendors and activities apply to RCM companies?

This question was sparked by an article we published regarding a final rule issued by the CMS stating certain requirements for plan sponsors and their first tier, downstream, and related entities (FDRs) being removed. In recent years, CMS has required plan sponsors to oversee their FDRs; and from there, plan sponsors would ask for FDRs to attest to have the following compliance elements implemented:

- Written policies and procedures and standards
- Exclusion list screening
- The availability of a system to receive reports (reporting mechanism) of suspected noncompliance and/or fraud, waste, and abuse (FWA) that is confidential, allows anonymity, and includes a policy of non-intimidation and non-retaliation
- Monitoring and auditing downstream entities
- Identification of offshore contractors that are responsible for functions involving PHI
- General compliance and FWA training (the "deeming exception" applies)

Of these elements, as of 2019, CMS is no longer requiring plan sponsors to ensure that annual general compliance and FWA training on unmodified CMS content is being completed by FDRs and their employees. However, CMS did mention that plan sponsors may develop and distribute training materials to FDRs, and still require FDRs to attest that the training was completed. For that reason, training on general compliance and FWA is still encouraged to ensure organizations are remaining compliant.

All other elements are still requirements and important for healthcare organizations that directly or indirectly contract with federal programs to have in place. The reason I mention healthcare organizations is the requirements not only extend to first-tier entities, etc. In fact, these requirements extend to downstream and related entities, and identification of offshore vendors is not excluded.

OIG Report

Almost five years ago, the OIG issued a report to CMS and OCR.[1] In that report, the OIG mentioned that for PHI that went to contractors operating outside the United States, there might be limited means to enforce the provisions of the business associate agreements (BAAs). While OIG's review was limited in scope to state Medicaid agencies, the report points out that the requirements to safeguarding PHI through reliance on BAAs alone would be the same on all HIPAA-covered entities, as well as their contractors and vendors. Some of the OIG's specific guidance issued in the report includes the following:

- BAAs did not specifically address the offshore outsourcing of functions involving PHI.
- Security risks greatly increase when administrative functions that involve PHI are outsourced offshore.
- Most countries do not have privacy protections equivalent to those of the United States to support HIPAA compliance.
- Warehousing of data offshore highlights the risks to the confidentiality, availability, and integrity to PHI faced by healthcare organizations (including RCM companies) that send data overseas.

In other words, organizations that send PHI offshore may have limited means of enforcing provisions of a BAA. Therefore, relying on a BAA alone is not enough and may not be of much value to ensure that PHI is adequately protected.

OCR Guidance

Following the OIG report—just a few years later—the OCR issued Guidance on HIPAA and cloud computing.[2] As part of their guidance, the OCR stressed the importance of entering into a BAA with a cloud service provider (CSP) and acknowledged the potential risks of offshore activities. For example, the OCR's frequently asked questions section included the following question:

> ***Do the HIPAA Rules allow a covered entity or business associate to use a CSP that stores ePHI on servers outside of the United States?***

In summary, the OCR answered this question by saying yes as long as a BAA is entered with the CSP and otherwise complies with the applicable requirements of the HIPAA rules. Also, while the HIPAA rules do not include requirements specific to ePHI processed or stored by a CSP, or other business associates or subcontractors processed or stored outside of the United States, "OCR notes that the risks to such ePHI may vary greatly depending on its geographic location." From there, the OCR said that "outsourcing storage or other services for ePHI overseas may increase the risks and vulnerabilities to the information or present special considerations with respect to enforceability of privacy and security protections over the data." To asses these risks, the OCR suggests taking them into consideration when conducting a security risk analysis (SRA) and risk management that is required by the HIPAA security rule. This includes determining such risks as whether the ePHI is maintained in a country where there are documented increased attempts at hacking or other malware attacks. If so, these risks should be considered significant and appropriate technical safeguards to address such threats must be implemented.

Real-World Example

I had the opportunity to be an expert witness in a case, just a few short years ago, wherein a medical professional hired vendors (software engineers) to help develop the software and ensure patient data was properly managed. At some point, these software engineers decided to subcontract data storage responsibilities to an offshore vendor. The software that engineers sent offshore for storage included several years of patient medical records (that were supposed to eventually be scanned into the system). The medical professional and his vendors had a contract in place to pay for work being performed, but they failed to execute a BAA.

After several months of working together, the medical professional and vendors had a falling out. As a result, work was not being performed, payments were not being made, and communications were cut, including with the offshore vendor responsible for storing the medical records. In fact, the offshore vendor was never located and the whereabouts of thousands of medical records is still unknown.

Ultimately, the provider and vendors had no idea who this offshore vendor really was and failed to have anything in place to ensure the information would be properly safeguarded. It's this type of scenario that explains why CMS, OIG, and the OCR are very concerned with offshore vendor activities.

When Might Your Organization Be Asked to Identify Offshore Vendors?

While very few RCM companies may be asked to actually complete an attestation from a plan sponsor, RCM companies usually are considered downstream entities. We like to think of this as a "not if, but when" situation. In other words, RCM companies should be prepared in the event they are required to attest. Usually, this would be in the form of an attestation to a provider; however, on rare occasions, plan sponsors may contact an RCM company directly and for identification offshore vendors and attestation, PHI is being used for functions offshore or overseas in a HIPAA compliant manner. For example, at a minimum, you may be asked for the following:

- Do you contract with a vendor that operates in an offshore location (non-U.S. location) that handles PHI as defined under HIPAA?
- If yes, please provide a list including vendor name (e.g., ACME Billing Company), their functions (e.g., billing and coding), location, and if a BAA is signed.

Lately, we have seen organizations being required to provide additional information. In other words, simply identifying the vendors is not enough. Plan sponsors have been asking FDRs to provide the information regarding offshore vendors they contract with such as:

- Describe the PHI that will be provided to the offshore vendor.
- Discuss why providing PHI is necessary to accomplish offshore vendor objective.

Organizations are also being asked to attest that they have offshore arrangements that ensure policies and procedures for safeguarding PHI and other personal information. And, in some instances, attesting that the arrangement prohibits access to any data beyond what is necessary for offshore functions, an agreement and process that allows for immediate termination upon discovery of a significant breach, and other HIPAA requirements.

Conclusion

Healthcare organizations, including RCM companies, may be required to identify their offshore vendors. As part of that process, you may be asked to attest making sure PHI is being used in accordance with HIPAA requirements. And while it is very difficult for enforcement of HIPAA requirements overseas, healthcare organizations may be held accountable for the functions or activities that involve the use and storage of PHI and other data outside of the United States.

We recommend RCM companies take a few moments to consider what PHI is being used or stored by all their vendors, including offshore vendors. Have you made sure BAAs are in place? Have you determined if PHI and data being used or stored is necessary for the intended functions of the vendors? Have you made sure vendors have a compliance plan in place that addresses all HIPAA requirements? By completing these steps, RCM companies can demonstrate they are doing their due diligence and are more than just aware of all vendors, including offshore vendors. ■

Chad Schiffman joined Healthcare Compliance Pros in 2014 as the director of compliance. Schiffman's seasoned background includes over 20 years combined experience in healthcare, information technology, and compliance consulting services. He is primarily involved in consulting with healthcare clients about their HIPAA and HIPAA HITECH-related issues, including breach determination, breach mitigation, and corporate compliance.

References

[1] https://oig.hhs.gov/oei/reports/oei-09-12-00530.asp

[2] https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html

Cybersecurity Risks for Billing Providers/Companies

During a period of growth, don’t forget to stay ahead of data threats.

By Jeffery Daigrepont

Healthcare technology for revenue cycle management services is evolving at a rapid pace, and today’s billing providers/companies leverage these advances to reach more customers, deliver faster service, and gain a competitive advantage. As your company (or billing department) embraces the new opportunities presented by technology, it is equally critical to stay ahead of the corresponding threats to data and information. When we think of patient privacy, we often think of clinical data because your personal medical information is considered more sensitive than your date of birth or address. However, under the HIPAA security guidelines, financial data is also considered protected health information (PHI), and it is in much higher demand on the dark web since criminals can use it for felonious actions leading to financial gains. Therefore, any organization—MSO, billing company, employed physician network, and private contractor—must comply with these rules.

In some cases, these entities may be required to enter into a business associate agreement (BAA). (Note: A BAA establishes permitted disclosures, requires the disclosure of breaches to HIPAA, and sets up other guidelines for handling provider-originated PHI. A BAA is a critical document that protects covered entities and their business associates alike.)

In the most basic sense, a BAA is a legal document between a covered entity (CE) and a contractor. The provision of the BAA is extremely critical to understand and comply with because it clearly states obligations to protect electronic PHI from being compromised by hackers—specifically, as a BAA agreeing to the Security Rule. The Security Rule requires appropriate administrative, physical, and technical safeguards to ensure the confidentiality, integrity, and security of electronic protected health information. The Security Rule is located at 45 CFR Part 160 and Subparts A and C of Part 164 (www.hhs.gov/hipaa/for-professionals/security/index.html).

Let’s examine the essential safeguards now that we know billing service providers and those responsible for revenue cycle management services are expected to secure PHI from cybercriminals. The security rules necessary to minimize the threats of cyber security breaches fall into three categories:

- **Administrative Safeguards.** Administrative safeguards are the policies and procedures that help protect against a breach. They determine documentation processes, roles, and responsibilities, training requirements, data maintenance policies, and more. Administrative protections ensure that the physical and technical protections are correctly and consistently implemented.
- **Physical Safeguards.** Physical safeguards ensure data is physically protected. They include security systems and video surveillance, door and window locks, and locations of servers and computers. They even include policies about mobile devices and removing hardware and software from certain sites.
- **Technical Safeguards.** Technical safeguards are the technology and related policies that protect data from unauthorized access. Each covered entity must determine the technical safeguards that are necessary and appropriate for the organization to protect its

ePHI. The Department of Health and Human Services states that you need to "establish a balance between the identifiable risks and vulnerabilities to ePHI, the cost of various protective measures, and the size, complexity, and capabilities of the entity."

Most organizations are well equipped to address the administrative and physical safeguards, as these tend to be static areas of concern—meaning, once a lock on a door is installed, the only action necessary is to activate the lock. The technical safeguards, on the other hand, are indistinct because this environment is more dynamic and fluid. This area is also where the cybercriminals attack since it contains access to the databases and patient electronic financial records.

Cybercriminals use various tactics to gain access to IT systems, most commonly using phishing campaigns and spoof emails. Despite all advances to prevent cybercrimes, no known technology on the market today can prevent staff members from clicking on links and opening emails they shouldn't. Given this known threat, organizations first should use every possible means to filter out unsafe emails from reaching their staff. Also, an enormous amount of ongoing effort should be dedicated to training staff on how to spot unsafe links/emails.

Fake emails are usually easy to spot once you know how to look for them. For example, the hyperlink has an easy-to-see red flag to indicate security. Most web links will start with HTTP or HTTPS. Hyper Text Transfer Protocol Secure (HTTPS) is the secure version of HTTP, the protocol for sending data between your browser and the website to which you are connected. The "S" at the end of HTTPS stands for "secure." It signifies that all communications between your browser and the website are encrypted. If this "S" is not part of the hyperlink, you are communicating without any encryption to the outside world. Most internet users are unaware of this simple clue for spotting an unsafe hyperlink.

Other threats include malware software that is specifically designed to disrupt, damage, or gain unauthorized access to a computer system. These threats generally stem from staff members downloading files or opening attachments. Again, a good internet traffic filtration system at the firewall level will reduce this threat.

A more serious (and less obvious) threat may come from the inside when a trusted employee (or remote worker) steals information from within the organization to sell and/or use it to commit fraud. This theft is extremely hard to detect because most systems in place today are set up to keep people out. According to a 2016 IBM study, insiders are responsible for 60 percent of all data breaches. Of those breaches, 75 percent were with malicious intent, and 25 percent were accidental.

Four actions you can take to prevent insider threats:

1. **Automate the process of wiping devices.** Many enterprises use Microsoft's Active Directory (AD) for file sharing. When an employee departs, someone in HR typically deactivates that employee's AD access. That deactivation should serve as a trigger to automatically wipe the data off the exiting employee's devices with mobile management tools. Automation of the deactivating processes is key to minimizing the insider threat. This is where identity management solutions come into play because they can automate

the de-provisioning process to ensure that users are removed from systems when they leave the company even before they leave the building.

2. **Establish strong internal governance.** Conduct internal audits to verify that the accounts were removed and that there is accountability to identify and correct gaps in the system, such as managers who don't follow the off-boarding process promptly. Two-factor authentication can also help by making it harder to crack back into systems.
3. **Set up role-based system access.** The employee user rights should be limited to their specific role. If the employee is working denials, they may only need access to the part of the system that is germane to denial management. Most systems will allow you to set up system access based on the role of the end user.
4. **Leverage monitoring technology and employee behavior.** IT and frontline managers need to have a see-something-say-something approach to monitoring employees. Frontline managers are more likely to know when employees are disgruntled or are getting ready to leave, which could be threat predictors. The IT department should be monitoring all of the system logs that track things like files being shared, copied, deleted, removed, system sign on/off, changes to data, etc. Someone logging on to the system at 3 a.m. should trigger an immediate alert requiring an investigation. Staff should be fully aware of these monitoring efforts as a deterrent to nefarious attempts.

Unfortunately, there is no universal answer or one-size-fits-all when it comes to security. The answer depends in part on the company, its line of business, its employees, and the defenses it has in place.

Billing companies and billing departments have access to sensitive data and PHI. Therefore, they fall under the same legal requirements of all covered entities (CE) for providing safeguards to protect the privacy of their patients, employees, and customers. To ensure compliance, the ONC requires all CEs to perform annual security risk assessments. The guidelines for conducting these risk assessments are at https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool. An alternative to doing a manual security risk assessment, there is now low-cost technology on the market that can scan entire networks in just a few hours to look for threats and vulnerabilities. These scans can produce the necessary testing and documentation necessary to satisfy much of the required security risk assessment. After the scan is complete, a full report of all threats and how to remediate each threat is available, allowing an organization to take immediate action against any and all cyber threats.

Organizations like Coker are now providing these scans for their clients as a low-cost alternative to the manual efforts. For more information, or for a free security risk assessment checklist, please contact me at jdaigrepont@cokergroup.com or by phone at 770-597-0590. Subscribers of *RCM Advisor* will receive a 10 percent discount on security scans. ■

Jeffery Daigrepont, senior vice president of Coker Group, specializes in healthcare automation, system integration, operations, and deployment of enterprise information systems for sizable integrated delivery networks. A popular national speaker, he is frequently engaged by highly respected organizations across the nation, including many nonprofit trade associations and state medical societies.

HBMA RCM Advisor
THE OPERATIONS ISSUE
Maximizing Revenue and Relationships
Modern solutions to boost revenue collection. PAGE 6
Taming the Medical Billing Beast
Picture This: Mobile Payments
Medical Coding and Documentation

The Ever-Shifting Sands Beneath the Billing Enterprise

Electronic health record (EHR) systems aren't as safe as you might think.

By Reed D. Gelzer, MD, MPH

The records a billing company receives as outputs from electronic health records (EHR) systems are commonly accepted on trust. However, now that nearly everyone is using EHRs, we're finding that they aren't "records" at all. Insurers and law enforcement professionals are increasingly recognizing that EHRs are well-suited for records counterfeiting, with predictable (and long-anticipated) results. This presents special challenges (and opportunities) for billing companies seeking value-added services and risk reduction.

First of all, readers often ask, "What is an EHR?" (Or EMR,[1] as often the terms are used interchangeably). For this article, to be brief, the main issue is more what an EHR (or EMR) isn't. EHRs are not records keeping systems in that EHRs are not designed, and often are not configured, implemented, or used in a manner that meets federal or state requirements for business records. As a result, EHR "records" are commonly not records.

This profound oddity arises because there are no regulations for these systems, nor does any agency (federal or state) oversee them for accuracy, safety, or security. Furthermore, most EHR contracts stipulate that the user holds all the risk and, in some instances, even indemnifies the EHR vendor.[2] EHR records systems, unregulated and without oversight, produce records-like outputs. These "record-like" objects, unless the user sees to it, frequently won't qualify as valid, accurate, complete episode of care records according to payer agreements or to federal and state laws defining business records.

Furthermore, there's no market transparency for EHR systems because errors, harms, and defects are not publicly reported anywhere and EHR contracts often stipulate that harms cannot be reported to anyone but the vendor. Since competitive markets require transparency, there is no normal market, and the purchaser/user is fully exposed to "buyer beware" risk, but blindfolded.

How This Applies to Your Company

Given the current absence of any public or private organization that requires or assures that EHRs actually capture and produce accurate records, what does this mean for your company? A foundation of the billing enterprise is the presumption that clinical care records are authentic and therefore suitable for coding and as support for service claims, regardless of payment model. What, if any, duty does a billing company have to exercise some due diligence on the clinical records that, in one way or another, fulfill your intention that you add real value based on real records of care actually and properly provided? On what basis may a billing company protect itself from problematic records whose purchase and use is entirely out of your control?

One way to think of this is the dilemma of companies building cars or airplanes. These companies don't make the steel; they buy steel based on technical specifications that assure that the steel meets the necessary requirements for safe cars and safe airplanes. What are those companies' exposures when they learn, as GM, Ford, and Boeing did last year, that one of the major suppliers, Kobe Steel, had been faking steel specifications for years?[3] We're also all familiar with the Volkswagen "gaming" of emissions reporting systems.[4]

For one thing, it certainly doesn't reflect well on your company if it turns out you simply eyes-wide-shut believed that the steel delivered was the steel expected, especially when a car crashes or a plane fails. Furthermore, if you actually observe oddities that give you concern, inaction under such circumstances produces risks to your firm, too.

Among the long, long list of unenforced or under-enforced rules, there's this key warning: Under HIPAA, the "awareness" requirement for False Claims Act was expanded from "knew" to "knew or should have known."

The obvious dilemma for the billing company is, do you tell your customer you have concerns about the veracity of their records, and then watch them take their business elsewhere? Since the federal government has chosen to underfund fraud investigations and since payers have similarly been ill-disposed to call out records counterfeiting, it is unlikely you'll get caught up in litigation. Nonetheless, what is the prudent path for you?

What You Should Do to Protect Your Company

In the world of EHRs, first and foremost, protect yourself from the start. The "start" is your engagement agreements with your customers. Review with your legal counsel how to add language that insulates you as much as possible from liabilities that properly reside with your customers.

Another key area will be your internal policies and procedures for what to do if you are presented with problematic records in the course of your normal business operations. One anecdote, for example, was a billing firm presented with records with "impossible" service dates, where it was known that the clinician of record was out of the country. Another common anomaly is the "nonsense" record. An example of this is the record with the presenting complaint of "headache" but the review of systems says explicitly "no headache." This is a definitively non-accurate "nonsense" record. It is increasingly likely that payers will begin kicking out such records and some payers report doing this already.

Consider at least offering, as a service, a records quality review option that will open the door to a discussion with your client where you end up with a definitive agreement that you are accepting their records as "complete and accurate" and, by mutual agreement, keeping the burden on the client to maintain quality controls. The Association for Healthcare Documentation Integrity (AHDI), for example, offers resources for supporting clinical documentation quality assurance (not be confused with revenue-enhancement directed CDI).

Lastly, there's at least one example where EHR companies are quietly inserting tools that will permit insurers and other investigators to easily reveal counterfeit records. They are not necessarily telling their customers those features now exist, so your customers aren't telling you. Watch out, for example, for a new option button in the billers view that indicates something like "Hide copied." If you see that, test it, and make sure your policies and procedures clearly define what you do with that new view.

Your business has other areas where unregulated EHRs can have substantial impact. For those of you who are looking at acquisitions, or are involved in healthcare acquisitions, similar cautions apply. Since EHRs are not regulated in any manner for fitness as business records, and since there is no market expectation that they comply with any accounting rules (e.g., GAAP), it is also prudent to add "records authenticity risk" to any due-diligence checklist. Unfortunately, in 2019 and for the foreseeable future, U.S. markets remain subject to the uncertainties of unregulated EHRs and the counterfeit records they can generate, whether intentional or not. Thus, for example, no AR valuation methodology can be safely presumed to be reliable if records counterfeiting isn't part of the analysis. ■

Reed D. Gelzer, MD, MPH, has 30-plus years' service in the healthcare field, including 11 years in rural primary care practice and in data quality and legal record attributes of medical records, then three years as an EHR vendor. At Trustworthy EHR LLC, he's focused on clinical trustworthiness, data quality, and business record accuracy.

References

[1] EMR = Electronic Medical Record. For our purposes here, the same problem of propensity to counterfeiting, exists in both.

[2] Koppel, Ross, Kreda, David, "Health Care Information Technology Vendors' "Hold Harmless" Clause: Implications for Patients and Clinicians" in Journal of the American Medical Association, 2009;Vol. 301 Issue 12, pp.1276-1278.

[3] Stapczynski, Stephen, Suzuki, Ichiro, and Suga, Masumi, "Japan's Kobe Steel May Have Faked Data for Over a Decade" in Bloomberg News, October 17, 2017, (accessed 10/17/18 at https://www.bloomberg.com/news/articles/2017-10-17/kobe-steel-is-said-to-have-likely-faked-data-for-over-a-decade)

[4] For example, see https://theconversation.com/how-volkswagen-got-caught-cheating-emissions-tests-by-a-clean-air-ngo-47951 and https://www.wsj.com/articles/volkswagen-shares-plunge-as-emissions-scandal-spreads-1446628400

Could a Data Breach Be Lurking in Your Copier Room?

Three lessons to learn from the case of the Affinity Health Plan data breach.

By Mike Bamberger

As if you don't have enough to worry about, now you have to worry about your photocopier. A $1.2 million settlement with the U.S. Department of Health and Human Services (HHS) by a New York not-for-profit managed care plan, in August 2013, was the result of a failure to delete protected health information from a leased photocopier before returning it to the leasing company. Affinity Health Plan Inc. filed a breach report with HHS after being notified by a representative of "CBS Evening News" that, as part of an investigative report, CBS purchased photocopiers that had been returned to a leasing company, including from Affinity.

The copier used by Affinity was analyzed for CBS, and electronic protected health information (ePHI) was found on the hard drive. In fact, the protected health information of over 340,000 individuals may have been compromised. Further, HHS' investigation found that Affinity "failed to incorporate the electronic protected health information (ePHI) stored on photocopier hard drives in its analysis of risks and vulnerabilities as required by the Security Rule, and failed to implement policies and procedures when returning the photocopiers to its leasing agents."

We live in an age of smart devices and machines that are indispensable in our businesses, organizations, and private lives. These devices are capable of creating, receiving, maintaining, processing, and storing enormous amounts of data. Much of this is sensitive data requiring protection under best business practices and various state and federal laws, such as state breach laws and the HIPAA Privacy and Security Rules (for Covered Entities and Business Associates as defined by HIPAA). The risks, as well as the benefits, of these devices must be understood and managed.

There are lessons to be learned from the facts of this case about what your business or organization should be doing to protect sensitive consumer/client information that resides on electronic systems and devices (e.g., Social Security numbers, credit card numbers, financial information, ePHI, financial information, etc.) and the cost of not doing so, in

Ongoing risk analysis and updated safeguards are essential.

terms of reputation, liability, business disruption, and costs.

First, have a process in place to identify everywhere sensitive data resides on electronic devices, carefully analyze the threats and vulnerabilities to that data, and operationalize appropriate safeguards to protect it. That may be easy to say in one sentence but actually doing it can take significant time and resources, depending on the size of the organization, the type and amount of electronic equipment, and the type/magnitude of data involved (see "Resources" below).

Second, it's important to understand that this is not a one-time thing. Ongoing risk analysis and updated safeguards are essential because, among other things, technology changes, new devices are added to businesses, ePHI and sensitive information shows up in unexpected places, and employees must be trained on keeping up with the required protections. For example, it's not just copiers, faxes, and scanners where electronic information may be found. What about laptops, smartphones, tablets, flash drives, and medical devices that store patient information?

The list goes on, as should the analysis and the planning to protect from any breach of information. Hopefully, once that first step is accomplished, the ongoing process will not be so overwhelming.

Third, develop and document policies and procedures for risk analysis and for implementing the plan to protect sensitive information. Hint: make sure that one of your policies states "that all personal information is wiped from hardware before it's recycled, thrown away, or sent back to a leasing agent." Documentation of policies and procedures communicates the plan internally and externally. Adequate documentation will demonstrate diligence if there is ever a question about whether best efforts were directed at risk analysis, developing policies and procedures, providing employee training, and other activities related to safeguarding individuals' data.

Fox Point Programs

Fox Point Programs is a specialist agency licensed to do business in all states. Our experienced staff has been servicing the insurance needs of HBMA members since 2009. CapSpecialty is one of the agency's premier carrier partners. Come to us for a free, no-obligation quote on your professional and cyber liability coverage. Fox Point is a subsidary company of Rockwood Programs Inc. Visit us here: www.foxpointprg.com/page_display.aspx?pID=9.

About CapSpecialty

CapSpecialty Inc. provides specialty insurance solutions for small- and mid-sized businesses across the U.S. CapSpecialty's experienced management and underwriting teams come from top insurance companies and bring with them a wealth of knowledge and an innovative approach to risk, providing the pricing its customers need for the exposures they are trying to protect. ■

Resources

Below are resources about safeguarding sensitive information.

Federal Trade Commission "Copier Data Security: A Guide for Businesses"
business.ftc.gov/documents/bus43-copier-data-security

For Covered Entities and Business Associates per HIPAA HHS' Office of Civil Rights provides free training about compliance with the HIPAA Privacy and Security Rules
www.hhs.gov/ocr/privacy/hipaa/understanding/training/index.html

Understanding HIPAA Privacy for Covered Entities and Business Associates
www.hhs.gov/ocr/privacy/hipaa/understanding/coveredentities/index.html

HHS' guidance on risk analysis requirements under the Security Rule
www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidance.html
www.healthit.gov/providers-professionals/security-risk-assessment

HHS' information about ePHI on mobile devices
www.healthit.gov/providers-professionals/your-mobile-device-and-health-information-privacy-and-security

RANSOMWARE

How to Prepare and Minimize the Damage

Attacks can take a well-oiled business and completely sideline it in a matter of minutes.

By Terry Schladetzky

Ransomware has, without a doubt, been on the uptick over the last five years. We have seen it go from a nuisance in its early stages to becoming a critical disrupter of business. Very few companies have been immune to ransomware attacks, and that has cost U.S. businesses plenty as police, fire, healthcare, infrastructure, commerce, logistics, and major shipping ports have all been attacked—the port of San Diego and the city of Atlanta being two of the most notable. Within a matter of minutes of infection, a business can go from operating like a well-oiled machine to being completely sidelined.

Ransomware is similar to a virus in the way that it infects your computer and how it propagates, but it can be far more destructive. Almost immediately after infection, all the data on the computer is scrambled, encrypted, and locked with a special key. The infection then branches out and targets other computers on the same network. It works very quickly to replicate itself across network drives and lock down any data it encounters. Upon trying to open the file, the user is met with a nasty message letting them know that their data is locked and they have a specified amount of time to pay a ransom before it is permanently lost.

Specialized IT companies prepare their clients for ransomware attacks and prevent their destructive results. These IT firms can put in place preventative measures as well disaster recovery programs to assist their clients to weather the storm should an attack occur.

"As part of our ransomware prevention, all critical data, applications, and operating systems are copied onto an image," says Lot De Leon, systems engineer for Emend Informa. "If the ransomware makes it past our countermeasures, then the disaster recovery plan we put into place will protect the business. To recover, it's usually just a matter of restoring the previous image, and the client can be operating again in a matter hours."

It's when there is no disaster recovery plan or prevention program in place that fighting ransomware becomes really expensive and can shut down the business.

In October 2018, Emend Informa systems engineer Jeremiah Byerley received a call for service from one such company.

"This was a new client that we had not worked with before and had no ransomware plan in place," he says.

The business had been working with their credit card processing company to install an updated version of their credit card processing software when a technical support agent for the credit processor was logged into the company's server via the internet, uploading the files necessary to complete the upgrade, and an infected file was inadvertently uploaded during the process.

"The technician ran the installation application for the program, and immediately a screen popped up on the server stating that the file was locked and demanded a $50,000 ransom to unlock it," Byerley says. "Within 10 minutes, the entire computer network was shut down and the business had stopped."

The company contacted Emend Informa for assistance after it was unsuccessful in its attempts to remove the malicious code and bring the system back online.

"Our biggest challenge was that even the backups had been corrupted by the ransomware, and what normally is the fastest and least expensive solution to bring the business back online was now part of the problem," he says. "This changed the entire strategy from contain and recover to rebuilding the system from scratch."

Even after the system was rebuilt, the work still was not finished. Byerley and his team then needed to determine the strain of the ransomware and work on getting the data back. Thus began the long process of trying to crack the encryption.

While it may seem next to impossible to break the encryption, Byerley explains that understanding who creates ransomware and why plays a big part of being able to decode the data files and use them again.

Most ransomware is created using a tool kit and designed for hackers to cast a wide net to see what they can reel in. The more data the ransomware can catch in the net, the better for its creator.

Byerley explains that these tool kits are often a one-size-fits-many solution for the person trying to steal the data, and often the tool kits are used to target companies just by using their default settings.

When all else fails and a backup cannot be restored, Byerley and his team turned to the very spot the problem originated from: the dark web.

"We were able to identify the tool kit that was used to create the ransomware. By using the default settings of the tool kit, we were able to backtrack through the program and come up with the encryption keys to unlock the data files," he says.

Even after identifying the tool kit that created the ransomware, recovery still takes time. The process of removing the encryption is a slow and painstaking process, and the business isn't able to use their computers while that process is running.

It took Byerley and his team at Emend Informa just over three weeks to recover all of his client's information. In the end, it cost just over $25,000 in IT repairs, and that doesn't include what the business lost while it was shut down during the process.

There are things that a business can do to limit the damages of ransomware. Make sure that your IT professional has implemented the following measures to combat

NEW HBMA MEMBERS

- **Heather Turcany**
  Merchants' Credit Guide Company
- **Jennifer Hicks**
  Sceptre Management Solutions
- **Manjunath An**
  Netzealous
- **Tara Vosler**
  Medical Claims Assistance Inc.

ransomware. In the end, it could make the difference between several hundred dollars and several hundred thousand dollars.

Perform Backups

Backups are the most important weapon in your arsenal against ransomware. Make sure you have multiple backups of your data. When creating your backup strategy, make sure you have the following covered:

1. Use a rotation set so you always have several backups offline that cannot be attacked by ransomware.
2. Use multiple backup platforms so you are not relying on only one solution.
3. Consider implementing a cloud-based backup solution as part of your strategy. Companies like IDrive offer a cloud-based backup designed specifically with ransomware in mind and to keep your data protected by keeping the backup inaccessible from the ransomware.
4. Make sure your backup solution supports bare metal restore.
5. Image servers and key computer systems so that you can quickly recover these systems if they become infected.

Use Enterprise Malware Protection

While there are quite of a few freebie antivirus programs out there such as AVG, Spybot, and Avast, with malware prevention, keep in mind you often get what you pay for.

Enterprise malware protection products such as Vipre from ThreatTrack have a central management console making it easier to monitor for and track infections. Enterprise products also release frequent updates. In the event that your system becomes infected, they will remotely connect to your infected system and help you to remove the infection. An enterprise antivirus product is most likely to contain a ransomware attack to a single system if not thwart the attack altogether.

Install a Commercial ANTISPAM Software

A lot of malware is distributed via email and can be headed off when it enters the network. Antispam software on your server will help to eliminate the threat before it makes it into a user's inbox. Products like GFI Mail Essentials do a good job to combat spam and malware by helping to prevent it from entering the mail server.

Tighten the Security on Your Network and Segment it into VLANS

A lot of people like to skip setting up security on their servers because it is easier if everyone on the network just has access to everything. Since ransomware relies on the permissions of the user in order to infect the network, it cannot change any files to which the user does not have access.

If you have administrator rights on your login, create a second account and use your admin account only when performing admin functions. It happens often that an unsuspecting admin happens across an infected web page and downloads a virus that infects everything because he has permission to everything.

Consider implementing group policies that restrict access to certain features in windows that can be compromised by malware.

Also consider dividing your network into segments called VLANS. This will isolate devices on their own virtual network and in the event of a data breach will confine the breach to the segment that was infected and prevent a widespread outbreak. This is especially important for large networks, companies with multiple locations, and agencies that connect with allied agencies.

Use a Commercial Firewall

Routers from Best Buy, WalMart, and Target are designed for consumer/residential use. They aren't sophisticated enough to monitor, track, and log activity on an enterprise network.

Companies like Sophos, Cisco Enterprise, and Juniper make commercial firewalls that will help to eliminate threats coming into the network before it even reaches your server. Avoid consumer-based products that don't keep logs, have a central point of management, or have built in antimalware/antiransomware features. ■

Terry Schladetzky is the owner of Emend Informa, a group of IT professionals serving Los Angeles, Ventura, and Santa Barbara counties in California as well as the New York tri-state area. For assistance or more information about how to protect your business, contact us at 800-773-9016 or email us at terry@informaco.com

Are Medical Record Numbers Considered Protected Health Information (PHI)?

Law

According to the U.S. Department of Health and Human Services (HHS), under the HIPAA Privacy Rule, identifiers such as names, telephone numbers, and license plate numbers are considered PHI and should be removed in order to de-identify information. For the full list, visit www.hipaajournal.com/considered-phi-hipaa.

In addition, the covered entity may not have actual knowledge that the remaining information could be used alone or in combination with any other information to identify an individual who is subject of the information.

Additionally, Section 164.514(a) of the HIPAA Privacy Rule provides the standard for de-identification of PHI. Under this standard, health information is not individually identifiable if it does not identify an individual and if the covered entity has no reasonable basis to believe it can be used to identify an individual.

Lastly, the HIPAA Rules generally require that covered entities and business associates enter into contracts with their business associates to ensure that the business A business associate may use or disclose PHI only as permitted or required by its business associate contract or as required by law.

HCP Response

Based on the facts restated above, in our opinion, medical record numbers and account numbers are technically considered PHI; however, if the covered entity has no reason to believe that the receiving party would have any way to use that information to identify an individual, it would not be considered a HIPAA violation. HCP manages the HBMA Compliance Accreditation Program. ■

Compliance Checkup

Are your coding practices up to date, and are you ready for clinical decision support?

By Melody W. Mulaik, MSHS, RCC, CPC, CPC-H

The only constant is change. We have all heard this mantra for much of our lives. The speed in which we accept and embrace change varies significantly from person to person. Sometimes we get more accepting of change as we gain more experience (aka get older) and, other times, we find that is not the case. We may ask ourselves, if everything is fine the way it is, why do we need to make any changes?

One of my favorite jokes of all times relates to change management. A man goes on vacation for a few weeks and leaves his cat with his brother. After a few days, he calls his brother and asks how his cat is doing. The brother tells him, "I'm sorry, but the cat died." The man gets angry and says, "How could you just break it to me like that? You know I'm not coming home for another week, you should have said something like, 'The cat is on the roof and we can't get it down,' then the next day I'd call back and you'd say, 'We got the cat down, but the vet says she's in bad shape, she may not make it,' and then the third day I'd call and THEN you'd tell me the cat had died. That way it wouldn't come as such a shock and I'd have been able to build myself up to deal with it!" The brother apologized. Then the first man said, "I'm sorry for snapping at you like that, but you know how sudden tragedy is worse than gradual … Anyway, so how's Mom?" And then the brother says, "Well, she's up on the roof and we can't get her down."

It's that time of year where usually everything is humming along smoothly and there are no major problems. You have a few months until new coding and compliance changes are scheduled to be released, so it is possible that you have mentally put that on the back burner until the fourth quarter. Depending upon your organization's schedule, the summer may be a crazy busy time or it may be the calm before the storm. What better time than now to do a quick inventory to ensure you and your clients are on track and in compliance? In other words, how do you ensure your cat or their cat is not on the roof?

Following are some key items, in no particular order, which you should evaluate to ensure things are as they should be:

MODIFIERS AND DOCUMENTATION

The appropriate assignment of modifiers is as much a reimbursement issue as it is a compliance concern. Briefly stated, modifiers typically indicate:

- Only part of a service was performed
- An adjunct service was performed
- A bilateral service was performed
- A service or procedure was provided more than once
- A procedure was altered in some way from the basic descriptor
- A service or procedure represents only a professional or a technical component

The medical record must contain sufficient documentation and adequate definition of the service or procedure performed to support the use of a modifier. If the service is not documented, or the special circumstance is not indicated, a modifier should not be assigned.

Placement of a modifier after a CPT® code does not ensure reimbursement. It is important to remain current on the latest CPT® guidelines regarding modifiers; it is equally important to become familiar with federal and commercial payers' guidelines. Claims that include modifiers should be monitored until you have determined a pattern of how their use affects payment. The effect of modifiers on reimbursement can often be negotiated in contracts with payers.

CLINICAL DECISION SUPPORT (CDS)

Hopefully this is already on your radar and you are either already reviewing newly released information to ensure that you and your clients are ready for this important regulatory requirement. If you currently bill for advanced imaging services, the implementation of CDS will create a major change in how referring physicians order imaging services. It will also require a tremendous amount of preparation work for imaging provides to not only install systems but perform appropriate education

Starting in 2021, payment will be denied if the furnishing professionals' (both facility and interpreting provider) claims lack the required AUC information unless one of the exceptions previously listed applies, such as a medical emergency.

of their referring community to ensure a successful implementation. In short, as a billing company you will be required to include new information on the claim form if you bill for radiology services, and you need to ensure that you will have access to this information in an efficient and timely fashion. If you bill for non-radiologists, you will need to ensure you are supporting your clients with information so they are not caught unaware.

This new regulation was created by the Protecting Access to Medicare Act of 2014 (PAMA). The Act specifically requires CMS to establish a program to promote the utilization of *appropriate use criteria* (AUC) for advanced diagnostic imaging services. Advanced imaging services include diagnostic CT, MR, and nuclear medicine exams, including PET. Ordering physicians and practitioners ("ordering professionals") will be required to consult AUC for all advanced imaging studies billed under the Medicare Physician Fee Schedule (MPFS), the Outpatient Prospective Payment System (OPPS), and the Ambulatory Surgical Center (ASC) Payment System, including those performed in a physician office, hospital outpatient department (including emergency department), IDTF, or ambulatory surgery center. Keep in mind that if your organization owns advanced diagnostic equipment, utilized for diagnostic studies, then the consultation and reporting requirements will apply.

Assuming that medical necessity is met, CMS will pay for advanced imaging studies regardless of whether they meet appropriateness criteria during the consultation process. But eventually CMS will identify the top 5 percent of ordering professionals who are consistently failing to follow AUC recommendations for studies involving priority clinical areas outlined above. Under PAMA, these "outliers" will be required to obtain prior authorization for any advanced imaging studies they wish to order for Medicare patients.

When it was first released PAMA called for ordering professionals to begin consulting AUC by Jan. 1, 2017, but that deadline has been pushed back several times. In the 2018 MPFS Final Rule, CMS announced that the consultation requirement will not go into effect until Jan. 1, 2020. While there have been questions and concerns raised in the industry regarding the "administrative burden" of this program it is important to remember that the requirement was enacted by Congress so it would literally take a new act of Congress to change or eliminate the requirement, and that is not anticipated to occur at this time.

Beginning in January 2020, there will be an "educational and operations testing period" lasting for one year. During this time, ordering professionals must consult AUC and furnishing professionals (the imaging facility and the interpreting providers) must report information about the consultation (mechanism and consultation result), but claims will continue to be paid regardless of whether the claim includes the required information. Starting in 2021, payment will be denied if the furnishing professionals' (both facility and interpreting provider) claims lack the required AUC information unless one of the exceptions previously listed applies, such as a medical emergency.

CMS will develop a series of G codes and modifiers during the 2020 rulemaking cycle that must be applied to the claims during the testing period. The G code will indicate which mechanism was consulted and the modifiers will indicate at an exam level (Abdomen CT, PET, etc.) whether the exam was recommended, not recommended or not applicable (inpatient, emergent, etc.). This information must be provided by the ordering provider to the imaging facility and interpreting provider. Claims will continue to be paid by CMS whether or not the information on the claim is completely accurate. During the initial testing period, the ordering professional will consult AUC through a qualified CDSM and furnishing providers will report the corresponding G codes and modifiers on their claims (facility and physician). CMS has not indicated how long the G codes and modifiers will be utilized for claims-based reporting.

UPDATE YOUR CHARGES

Last, but certainly not least, is ensuring that your clients' charges are updated and appropriate. For the majority of billing companies, this has a direct impact on your fees as well. With the increase in the number of bundled codes, it is imperative that organizations appropriately adjust their charges to reflect the true costs to provide the services. In our environment of increased pricing transparency, it is important that you are not overcharging for services. In some markets and specialties, patients actively shop for the best practice, so finding the right balance of charges versus cost is critical. This is a key area of concern that you should be discussing with your clients even if they do not believe it is a priority.

There are always opportunities to improve our processes internally and our client facing processes. As revenue cycle professionals, we pride ourselves on our willingness to adapt, change, and improve in all areas of our realm of influence personally and professionally. And, most important of all, remember there is always a cat on the roof—don't let it be yours! ■

Melody W. Mulaik, MSHS, is the president of Coding Strategies Inc. and Revenue Cycle Inc. She is a frequent speaker and author for nationally recognized professional organizations and publications. Mulaik's areas of expertise include coding and compliance, management engineering, and operations improvement, and she is nationally recognized for her extensive radiology expertise.

800.969.3666 | providersales@cognizant.com
* Terms and conditions apply
IS CREDENTIALING A HEAVY BURDEN?
VISIT
trizettoprovider.com/HBMAcred
and enter the below promo code to get
$100 OFF*
your credentialing set-up fee.
PROMO CODE:
HBMAcred
TriZetto Provider Solutions® A Cognizant Company
MEMBER OF HBMA
Discover a faster, simpler route to gaining credentials with the help of
TriZetto Provider Solutions, a Cognizant Company.

CHBME QUIZ QUESTIONS

You can earn 1.0 credit toward your CHBME by answering quiz questions in each issue of ***RCM Advisor***.

1. **According to a 2016 IBM study, those inside of companies are responsible for ___ percent of all data breaches.**
   A. 30 percent
   B. 60 percent
   C. 40 percent
   D. 55 percent

2. **The security rules necessary to minimize the threats of cyber security breaches fall into three categories. Which category is not correct?**
   A. Physical safeguards
   B. Administrative safeguards
   C. Internal safeguards
   D. Technical safeguards

3. **What percentage of the U.S. population has multiple names associated with a single Social Security number?**
   A. 7 percent
   B. 18 percent
   C. 24 percent
   D. 13 percent

4. **Which region of the country has the highest percentage of total uncollectable accounts (bad debt) of 9.92 percent?**
   A. Southeast
   B. Southwest
   C. Midwest
   D. Northeast

5. **A hyperlink sent from a fake email address will not look like a tradition hyperlink, which includes “HTTPS.” What does “HTTPS” stand for?**
   A. Hypo Text Translate Protocol Security
   B. Hyper Text Transfer Protocol Secure
   C. Hyper Transfer Test Protocol Secure
   D. Hypo Translate Text Protocol Security

6. **What percentage of smartphone users would be more encouraged to make a payment via a mobile phone if it was as simple as paying with a single click?**
   A. 56 percent
   B. 83 percent
   C. 42 percent
   D. 76 percent

7. **In 2017, how many undeliverable pieces of mail were there?**
   A. 1.5 billion
   B. 4.2 billion
   C. 2.1 billion
   D. 1.1 billion

8. **The new Clinical Decision Support (CDS) regulation was created by the Protecting Access to Medicare Act of 2014.**
   A. True
   B. False

9. **Where shouldn’t you purchase your company’s routers?**
   A. Sophos
   B. Cisco Enterprise
   C. Best Buy
   D. Juniper

10. **What is a BAA in the most basic sense?**
    A. A legal document between a contractor and the government
    B. A legal document between a covered entity (CE) and a contractor
    C. A legal document between a healthcare provider and the government
    D. A legal document between a CE and an employee

Go to www.hbma.org/ceu or use your smartphone to go directly to the site with the QR code at right.

Arrays Part IV

By Nate Moore, CPA, MBA, FACMPE

Hold on to your hat! This article adds a new degree of complexity to our discussion of arrays. Please review the first three articles in *RCM Advisor* to refresh your memory on arrays. Now that we have worked through several examples with the syntax of arrays and have seen how arrays can make spreadsheets easier, this article goes even further. The most important thing to remember as you follow the examples in this article is to enter the formulas with Ctrl+Shift+Enter to get the curly braces that surround Excel formulas. Manually typing the curly braces will not cause Excel to treat the formula as an array, so you will not get the results you expect. The more examples you see of the power of arrays, the more ways you can find to use arrays to make your spreadsheets more efficient.

Adding and Multiplying TRUE and FALSE

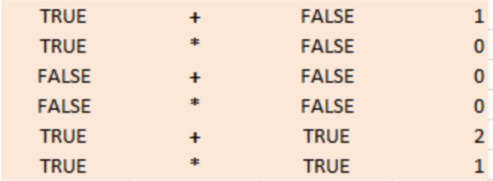
You may be familiar with Excel values of TRUE and FALSE from working with IF statements. The TRUE and FALSE values can also add significant power and flexibility once you understand how Excel does mathematical calculations with TRUE and FALSE. Figure 1 has a summary of the different ways to add and multiply TRUE and FALSE. You might find it helpful to think of TRUE being 1 and FALSE being 0. Just as 1 + 0 = 1, TRUE + FALSE = 1. Similarly, TRUE times TRUE (Figure 1 uses the asterisk (*) as the times symbol) is 1, while TRUE times FALSE equals 0.

Now consider the table of data in Figure 2, which summarizes collections for the past four years for three locations of a medical practice. If the objective is to summarize 2014 collections, one formula that would work is =SUMIF($A$1:$A$15,E1,$C$1:$C$15), assuming cell E1 has 2014, the year we want to sum. Excel's SUMIF and SUMIFS formulas are described in Excel Videos 184 and 185 at mooresolutionsinc.com. The SUMIF and SUMIF functions were also discussed in the March/April 2018 issue of *RCM Advisor*. The array formula to do the same calculation may initially look more difficult, but arrays will give us more powerful filtering capability as our examples proceed.

To make the same calculation summing 2014 collections with an array formula, again assuming the year to sum is in cell E1, the formula would be {=SUM(IF(A1:A15=E1,C1:C15,0))}. Working to understand the formula from the inside out, the IF formula checks to see if cells A1:A15 equal E1, the year in question. If the years match, the IF formula returns the corresponding collection amount in cells C1:C15. Otherwise, the IF formula returns 0. The SUM formula sums the results of the IF formula. Remember that a normal IF function only accepts one cell at a time. Because we use Ctrl+Shift+Enter to enter the formula, Excel treats the entire formula as an array and evaluates all 15 rows in the formula at once.

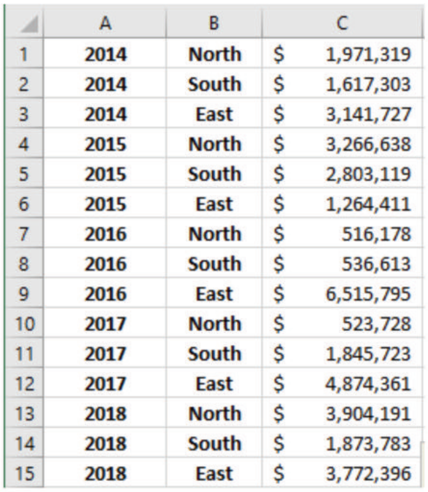
In a similar way, assume that the clinic location is stored in cell E2 and we want to sum all collections in the South location across years 2014 through 2018. A SUMIF formula would be =SUMIF($B$1:$B$15,E2,$C$1:$C$15). A similar array formula would be {=SUM(IF($B$1:$B$15=E2,$C$1:$C$15,0))}. These formulas are very similar to summing years, and again, the SUMIF formula may look easier than the array formula.

FIGURE 1



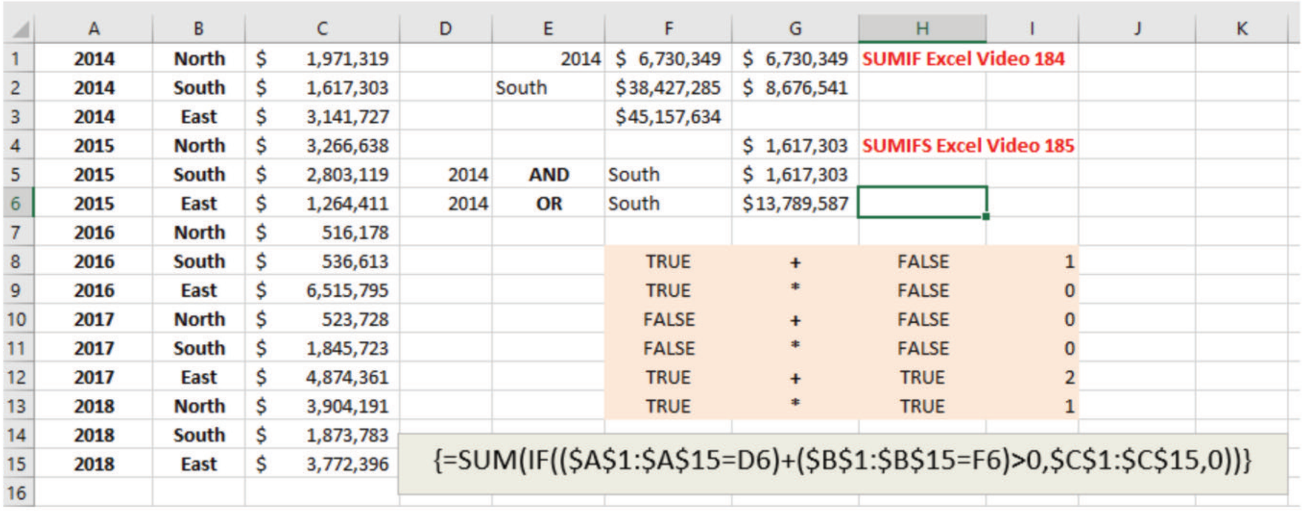
TRUE	+	FALSE	1
TRUE	*	FALSE	0
FALSE	+	FALSE	0
FALSE	*	FALSE	0
TRUE	+	TRUE	2
TRUE	*	TRUE	1

FIGURE 2



	A	B	C
1	2014	North	$ 1,971,319
2	2014	South	$ 1,617,303
3	2014	East	$ 3,141,727
4	2015	North	$ 3,266,638
5	2015	South	$ 2,803,119
6	2015	East	$ 1,264,411
7	2016	North	$ 516,178
8	2016	South	$ 536,613
9	2016	East	$ 6,515,795
10	2017	North	$ 523,728
11	2017	South	$ 1,845,723
12	2017	East	$ 4,874,361
13	2018	North	$ 3,904,191
14	2018	South	$ 1,873,783
15	2018	East	$ 3,772,396

FIGURE 3 All cells (Figures 1 and 2) at once.



	A	B	C	D	E	F	G	H	I	J	K
1	2014	North	$ 1,971,319		2014	$ 6,730,349	$ 6,730,349	SUMIF Excel Video 184			
2	2014	South	$ 1,617,303		South	$38,427,285	$ 8,676,541				
3	2014	East	$ 3,141,727			$45,157,634					
4	2015	North	$ 3,266,638				$ 1,617,303	SUMIFS Excel Video 185			
5	2015	South	$ 2,803,119	2014	AND	South	$ 1,617,303				
6	2015	East	$ 1,264,411	2014	OR	South	$13,789,587				
7	2016	North	$ 516,178								
8	2016	South	$ 536,613			TRUE	+	FALSE	1		
9	2016	East	$ 6,515,795			TRUE	*	FALSE	0		
10	2017	North	$ 523,728			FALSE	+	FALSE	0		
11	2017	South	$ 1,845,723			FALSE	*	FALSE	0		
12	2017	East	$ 4,874,361			TRUE	+	TRUE	2		
13	2018	North	$ 3,904,191			TRUE	*	TRUE	1		
14	2018	South	$ 1,873,783								
15	2018	East	$ 3,772,396								
16											

{=SUM(IF(($A$1:$A$15=D6)+($B$1:$B$15=F6)>0,$C$1:$C$15,0))}

What if you want to sum all cells where the year is 2014 (cell D5) AND the location is South (cell F5)? The SUMIF formula now has multiple criteria (2014 and South), so we need to use a SUMIFS formula like =SUMIFS($C$1:$C$15, $A$1:$A$15,D5,$B$1:$B$15,F5). A similar array formula for 2014 (cell E1) and South (cell E2) is {=SUM(IF(($A$1:$A$15=D5)*($B$1:$B$15=F5)>0,$C$1:$C$15,0))}.

As scary as this formula may look, it is not very different from our first array formula. Again working from the inside out, the inner formula is an IF function. The IF function tests to see if this condition is true: ($A$1:$A$15=D5)*($B$1:$B$15=F5)>0. The condition checks to see if cells A1:A15 are equal to D5, the year 2014. The condition also checks to see if cells B1:B15 are equal to F5, the South location. Remember that if the condition is TRUE, Excel treats the answer as 1. If the condition is FALSE, Excel treats the answer as 0. If the year in cells A1:A15 is 2014, the first half of the IF condition will be TRUE, or 1. If the location in cells B1:B15 is South, the second half of the IF condition will be TRUE, or 1. Since we are multiplying the results, only when both the year is 2014 and the location is South will the result be greater than 0, making the overall IF condition TRUE. When the IF condition is TRUE, the formula returns the corresponding cell in C1:C15. Otherwise, the formula returns 0. The outer SUM function sum the results of each calculation in the array.

Please note that for the SUMIFS formula to work, we need to look for both the year 2014 AND the location South. If we want to sum collections where the year is 2014 OR the location is South, the array's power and flexibility comes through for us. To sum rows where the year is 2014 OR the location is South, our array formula is almost identical to the AND formula above: {=SUM(IF(($A$1:$A$15=D6)**+**($B$1:$B$15=F6)>0,$C$1:$C$15,0))}. The only difference is that we add the two conditions instead of multiplying. The addition is highlighted in the OR array formula. Review Figure 1. When we wanted 2014 AND South, a TRUE value times a TRUE value will equal 1. If either value is FALSE, 1 * 0 or 0 *1 will equal 0, and the row will be excluded from our AND calculation above. Now that we want 2014 OR South, we add. If either the year is 2014 or the location is South, the TRUE value will equal 1. By adding, we capture a 1 where either value is true and sum the corresponding row in column C in our formula.

This is clearly a complex array formula. You will not be the only one who re-reads a paragraph or two in this article. Once you understand the concept, you can build all kinds of complex AND or OR criteria to find exactly the conditions you need to in your data.

Continue to practice using array formulas with your data. Start small. Build test columns and take the array formulas a piece at a time to make sure you get the results you expect. Once the array formula plays nicely, arrays can add a lot of power and flexibility to your spreadsheets. There are more array examples in the Excel Video playlists at **mooresolutionsinc.com** ■

Nate Moore, CPA, MBA, FACMPE, writes custom SQL Server code to mine practice management data for analysis in Excel, web pages, and via email. Nate's second book, Better Data, Better Decisions – The SQL: Business Intelligence for Medical Practices, *was recently published by MGMA. His free Excel Videos have been viewed over 2 million times and are available at mooresolutionsinc.com. Attend the HBMA Annual Conference to get hands-on training with Nate.*

Developing Your Team Members

By Dave Jakielo, CHBME

I realize it is getting a bit harder for medical billing companies to maintain the same profit margins today that we enjoyed just a decade ago. And where you spend your discretionary income takes more thought.

When dollars start to get tighter, an unfortunate consequence is that some companies cut back on training and education for their team members. However, in today's ever-changing healthcare environment, continuous learning is more important than ever. Training dollars should be budgeted for each year.

I often hear owners saying that they stopped spending money on training because people often leave right after, but consider the alternative: you don't train them and they stay.

Some of the critical areas where training should be ongoing are:

- Compliance
- HIPAA certification
- Leadership skills
- Customer service skills

When it comes to compliance training, there are many excellent consultants that can help you establish and maintain a viable program for you billing company. As clients get more knowledgeable about compliance, it will be harder to land larger practices if you can't prove you have an active compliance program in your company.

HIPAA certification is much easier to obtain, and there are many affordable options online. The online options provide study guides and allow you to take the exam on your own time table.

Leadership skills are a necessity in today's workplace. In the past, many didn't take leadership skills into account when promoting someone. Often a super clerk who was really good technically got moved into a position where they were responsible for a team. And without any training you wondered why a great payment poster didn't magically transform overnight into a great payment manager. That is what happens when you promote someone into a leadership role without the proper training.

We must also always remember that we are an extension of our customers' office. How we provide service to their patients reflects more on them than it does on us, as the public doesn't always understand the concept that the practice may be using a third-party billing company. So, when they are upset with one of our employees, they tie that back to the practice, and that can lead to a negative experience for the patient.

To avoid any issues, you should record all your incoming patient phone calls and periodically have your management team review the recordings to ensure everyone who answers your phones is handling calls appropriately. And, if necessary, hold in-service training sessions of the proper do and don'ts of handling patients calls.

While profits may be shrinking, if you do not provide the proper training to your team in the above areas, you'll probably find that profits will continue to tank. The choice is yours, but I hope you'll budget for training in your firm to help it achieve and maintain excellence. ■

Dave Jakielo is an international speaker, consultant, executive coach, and author, and is president of Seminars & Consulting. Jakielo is past president of Healthcare Billing and Management Association and the National Speakers Association Pittsburgh Chapter. Sign up for his free weekly Success Tips at www.Davespeaks.com. He can be reached via email Dave@Davespeaks.com and by phone at 412-921-0976.

HBMA

CS2019

COMPLIANCE SYMPOSIUM

HBMA.org/CS2019

- EXPERT FACULTY OF PROFESSIONALS
- DESIGNED FOR YOUR SUCCESS
- DEVELOP YOUR COMPLIANCE PLAN

REGISTER TODAY!

MAY 8-9 | 2019

CHICAGO, IL

HBMA
HEALTHCARE BUSINESS MANAGEMENT ASSOCIATION

2025 M Street, NW, Suite 800
Washington, DC 20036

HBMA Education On Demand

Now you can access industry-leading education on the topics that matter most to you anytime, anywhere.

Visit the HBMA website to explore the library of webinars available on demand.

Did you miss HBMA 2018 in October? Session recordings are now available! Available recordings include:

- **Denials Management – Identifying and Challenging Insurance Coverage Denials from Claim through Litigation**
- **Revenue Optimization – Maximizing Your Medical Coding and Documentation**
- **State of the Physician RCM Sector – Creating Value in Today's Market**
- **Innovation in the Healthcare Framework**
- **And more!**

Visit hbma.org/meeting_calendar