# So what’s RCM?

By Neale Pashley

Revenue Cycle Management (RCM) refers to a payment process that integrates an all-inclusive range of tools, practices, techniques and solutions that are closely interconnected to information and operational healthcare services. The goal of RCM is to ensure the healthcare provider or facility has a friction-free billing and payment process.

Neale Pashley VP, Partner Services

## An RCM Strategy Should Benefit the Provider and Patient

A well-thought-out RCM strategy uses both preemptive and responsive methods to optimize the profits of healthcare facilities while providing each patient with improved healthcare services. In addition, the integration of healthcare providers, patients, insurance payers and billing companies while processing patient claims makes it possible for healthcare facilities to raise their revenue.

## Reduce Payment Process Friction

When it comes to the payment process, friction refers to any issue that interrupts an otherwise smooth transaction. Examples of payment process friction include when a patient calls in to complain about his or her medical bill, or when insurance companies are denying submitted claims.

## An insurance denial brings with it an array of questions:

- Was all the information that was obtained from the patient correct?
- Did the administrative team fail to verify the patient's information?
- Were the wrong CPT codes used?
- Does the insurance need additional information? If so, what information is being requested?

## Correct Patient Information is Vital for Friction-Free Payment Processes

To have a successful Revenue Cycle Management strategy, focusing on front-end tasks is key. Many of the medical billing errors that occur result from incorrect patient information. This incorrect information carries on throughout the revenue cycle, thus, disrupting claims reimbursement. Needless to say, when incorrect patient information is collected during the registration process, the payment process is interrupted. This delay in payment could cause the relationship between the patient and the provider to become strained. As a means to eliminate the frustrations associated with billing issues and payment processing, many healthcare facilities are choosing to hire an RCM company that can provide them with a solution for the issues related to claim denials due to missing patient information.

## The Role of Technology in the Payment Process

Technology can be used to assess potential points of friction and then analyze that information to ascertain which issues are more likely to interrupt a healthcare facility’s payment process. Once this information is collected, healthcare facilities can use it to fine-tune their RCM.

## Possible friction points include the likelihood of:

- the health insurance company denying claims due to missing patient information.
- the insurance company inappropriately denying claims.
- claims being denied due to the use of incorrect CPT billing codes.
- denials due to additional information requests.
- denials due to inaccurate patient information.
- a patient’s ability to pay his or her portion of the bill.

A good Revenue Cycle Management company can analyze this information for the healthcare facility and create a personalized plan to reduce the friction that is occurring in their payment process.

## Changes in Healthcare Can Cause Payment Disruptions

The continuous changes within the healthcare industry can make it difficult to maintain financial stability, however, RCM companies stay abreast of these changes, thus, preventing any disruption to their clients’ payment processes.

# 4 Tips for Improving Patient Satisfaction and Front-End Tasks

As the healthcare industry continues trending toward consumer convenience, the importance of reducing friction must be recognized. Especially considering that patient satisfaction scores and value-based outcomes directly affect payments. Offering patients an easy way to pay and update their information can decrease friction and increase revenue.

**1- Offer Individualized Platforms**

Allowing patients to pay their bills online makes the payment process easier, which is likely to increase patient payments.

**2- Provide Patient Portals**

A patient portal provides a way for patients to update their insurance information and set up payment plans for any outstanding medical bills. Providing patients with a platform they prefer will increase the likelihood that the patient will settle his or her account.

**3- Verify Patient Information**

Technology can be used to reduce the number of insurance denials that occur due to incomplete or inaccurate information. This verification process is possible because the patient’s information on a claim can be compared to his or her policy information. This allows the medical biller to ensure there are no discrepancies that could delay payment.

**4- Verify Patient Eligibility**

Checking a patient’s eligibility as well as verifying that a statement is correct before sending it to the patient also reduces friction.

Technology can reduce the incidence of many issues that are

responsible for impeding the payment process. Healthcare facilities that neglect to prioritize their clientele will fall behind, leaving the door open for their competitors. Especially since patient satisfaction serves as the main component in today’s value-based era.

## Choosing a Revenue Cycle Management Company:

To choose the RCM company that will meet all your needs, there are several questions that need to be answered.

**Questions for a Revenue Cycle Management Company**

- What is the strategy for identifying, validating and solving patient registration issues and missing claim information?
- How do you ensure correct coding and how is coding accuracy audited?
- What is the source of truth for auditing billed charges and what is the process for ensuring all charges are billed and paid appropriately and per contract with each payer?
- How do you optimize denial management?
- How are Worker’s compensation claims handled differently?
- How are governmental payers handled differently?
- What are the unique needs of Medicaid in my state?
- How do revenue cycle strategies differ for 3rd party liability, Ideal provider organizations, Better managed care, Guaranteed insurers?
- Do you perform automatic write-offs, if so, why?
- Is every unpaid claim viewed at least once by an experienced denial management representative?
- What access is given to data and reporting to ensure transparency and evidencing success?
- How do you maximize patient collections, patient

satisfaction and manage the patient’s perception of the medical group?
- How does your technology enhance human interactions in the billing process?

A reputable RCM company takes care of all these issues and more, thus, reducing the stress on the healthcare professional by keeping the payment process moving along smoothly.

---

# Why The Real Number Of Ransomware Attacks Is Higher Than You Think

The number of ransomware attacks is higher than you think. Recently, a University of Vermont network found that even more ransomware attacks have infected their hospitals.

The same cybercrime gang that infected at least three other hospitals recently has also attacked University of Vermont Health Network, according to two sources from the investigation.

Last week Wednesday, federal agencies warned US healthcare providers of an “increased and imminent cybercrime threat” by a gang that uses ransomware called Ryuk.

On Thursday, the FBI and Cybersecurity and Infrastructure Security Agency (part of the Department of Homeland security) sent an update with new technical information regarding the attacks.

It’s rumored that 20 medical facilities have been hit by the recent wave of ransomware, although the investigation is

ongoing and nothin has been officially confirmed. Many of these facilities are within the same hospital chain.

The FBI and the Cybersecurity and Infrastructure Security Agency, part of the Department of Homeland Security, sent an updated alert Thursday night with new technical information, adding that they have “credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers.”

Ryuk has been confirmed to have hit the following: the Sky Lakes Medical Center, with 21 locations in Oregon; Dickinson County Healthcare System in Michigan and Wisconsin; and the St. Lawrence Health System in northern New York..

The infections of Ryuk made Sky Lakes Medical Center inaccessible, which halted radiation treatments for cancer patients, according to the Center’s spokesperson, Tom Hottman.

“We’re still able to meet the care needs for most patients using work-around procedures, i.e. paper rather than computerized records. It’s slower but seems to work,” he wrote, in an email.

A major wave of ransomware attacks began at the end of September when Universal Health Services, one of the biggest hospital chains in the U.S., was hit, forcing doctors and nurses to use pen and paper to file patient information. Ransomware typically gains access to secure systems and encrypts their files, demanding money to decrypt the files.

Trickbot is the notorious cybercrime botnet that transmits Ryuk. Both Microsoft and reportedly U.S. Cyber Command have undertaken efforts recently to disrupt Trickbot, but not with success.

Attacks on theU.S.’s healthcare systems have risen this year, said Allan Liska, an analyst at the cybersecurity firm Recorded Future, who monitors known infections.

“We’ve tracked 62 reported healthcare ransomware infections this year. Compared to 50 all of last year,” Liska said.

“Keep in mind that unless an incident becomes public, there is a couple-of-month lag between the incident and reporting. So the real number is much higher,” Liska said.

A Department of Health and Human Services security memo produced for health care providers this year, which was reviewed by NBC News, shows that private security companies and the U.S. government attribute Ryuk ransomware to Russian cybercriminal groups.

The private security firm CrowdStrike assessed with “medium confidence” that Russian threat actors use Ryuk, and the cybersecurity company FireEye said the “most likely hypothesis” is that Ryuk operators are Russian cybercriminals, according to the memo.

Russian cybercriminal groups sometimes work with the Russian government, but in other instances they can work on their own.

Read these simple things you can do to help avoid a ransomware/malware attack

---

# The importance of Cybersecurity in This Era of Radiology

Continued digitization has brought tremendous benefits to health care, making the industry more connected and efficient than ever. However, with an overwhelming number of data and patient records located on interconnected networks, the

importance of actively protecting it all cannot be overstated. Hackers have continually evolved and adapted with technology. They are always seeking new sectors to attack, including in the health care space.

For radiology departments, the risks of experiencing cyber attacks has increased over the past several years with the profession becoming a mainly digital practice and widespread industry consolidation. With many radiologists now working remotely due to COVID-19, hackers are more likely than ever to jump at the opportunity to breach private data with employees working on mobile devices on less secure wireless networks.

Practices must begin to invest in and strengthen their cybersecurity immediately to prevent the possibility of an attack. As our industry transitions to a more virtual environment, taking immediate action may save the future of your practice and, more importantly, the future of your patients.

## Understanding cyber attacks on health care practices

The incredible growth of industry technology has enhanced the medical profession, making data and information instantaneously accessible. However, this immediate access to private data also creates opportunities for hackers to invade organizations' systems, majorly affecting the entire industry.

Cybercrimes cost the health care industry around $6.2 billion annually, with organizations individually losing an average of $3.7 million. There are also many other costs organizations could face with cybercrimes, including post-breach costs, potential fines from HIPAA and even lawsuits. What's more, employees can be major contributors to potential network breaches as well. According to a 2016 report from BakerHostetler, 24% of health care data breaches were the

fault of employee errors.

Organizations are not the only ones affected by cyber attacks, however. Their patients suffer just as much, and in some cases, even more so. In 2019 alone, more than 40 million people were affected by health care data breaches, doubling the amount recorded in 2018. This trend is expected to increase as more data and protected health care information (PHI) becomes digitized on network servers across the industry.

## Knowing where hackers will strike

It’s hard to predict where hackers will attack next and how they will do so. Cybercrimes can stretch from breaching systems for patients’ PHI, infecting networks in malware attacks or deliberately tampering with images and scans in ransomware attacks. This uncertainty can make securing data and preparing systems for attacks a challenging process.

While there is uncertainty in exactly how hackers will attack, they have been pretty consistent in targeting small and medium sized medical practices. This is because many of these specific practices don’t have the manpower nor financial resources to field a full cybersecurity team, making their data less secure and easier to breach.

Hackers have also become interested in targeting health care networks consisting of consolidated practices. With scans, patient information and other data streamlined across multiple networks and facilities, there are more opportunities for hackers to breach, steal and manipulate private data.

## Figuring out how practices can

# prevent cyber attacks

Practices can take many different avenues to bolster their cybersecurity efforts. One of the most important steps is implementing proper security systems, such as Artificial Intelligence (AI) solutions. These systems are designed to constantly understand patterns and protect data automatically while anticipating and identifying any nefarious activity. In a time where hackers can attack systems in various forms at various times, AI solutions will intuitively protect your network and patient data.

Another step, especially in this remote era of health care, is to have added protection for any mobile devices used by employees. While the amount of mobile devices at our disposal is helpful to radiologists and their practices, they also pose a great threat to network privacy and security. With the pandemic forcing many radiologists and physicians to work remotely, they have relied on their mobile devices and wireless networks at home to accomplish their work. These devices and networks are much less secure than those at their practices, easing the challenge for hackers to attack.

To decrease the possibility of hackings or any unauthorized access, all used mobile devices must be equipped with stronger authentication and access control settings. Regularly changed passwords, further authentication steps and even limiting the amount of mobile devices used are a few ways to increase protection when utilizing mobile devices. Implementing these settings can be a major step in keeping all data and private information secure as remote work could be the future of the industry, at least for the rest of this pandemic, and maybe even beyond.

Network breachings can be detrimental to practices and their patients in numerous ways. It is important that practices improve, and maybe even overhaul, their cybersecurity efforts.

The expansion and evolution of industry technology only increases the chances of network hackings and practices losing invaluable data and information. As many practices struggle to survive during these turbulent times, one network hacking could be the ultimate kiss of death.

---

# Healthcare Institutions Are Under Ransomware Attacks Warns FBI

Healthcare institutions across the country are being warned by the FBI regarding emerging ransomware attacks.

Ransomware is increasingly being used by hackers to extort money from companies. Many Healthcare organizations are being targeted. Ransomware is a type of malicious software that takes over your computer and prevents you from accessing files until you pay a ransom. Those hackers understand the value of PHI which is why they are targeting the healthcare industry specifically.

Arun Douglas, MSc, Chief Technology/Security Officer

Many healthcare companies including Collaborative Imaging maintain controls to help protect the networks and computers from this type of attack. However, some hackers change attack scenarios quickly which is why it is important for all healthcare employees to understand that they are the first line of defense. Here are some simple things you can do to help avoid a ransomware/malware attack:

## Think Before You Click:

The most common way ransomware enters corporate networks is through email. Often, scammers will include malicious links or attachments in emails that look harmless. To avoid this trap, please observe the following email best practices:

- Do not click on links or attachments from senders that you do not recognize. Be especially wary of .zip or other compressed or executable file types.
- Do not provide sensitive personal information (like usernames and passwords) over email.
- Watch for email senders that use suspicious or misleading domain names.
- If you can’t tell if an email is legitimate or not,

please contact the IT helpdesk.

- Be especially cautious when opening attachments or clicking links if you receive an email containing a warning banner indicating that it originated from an external source.
- Personal Email platforms like Gmail, Yahoo, Hotmail, Outlook are also at risk. Please do not access these platforms from company workstations.
- Be wary of links to shared documents (SharePoint, Dropbox and the like) from outside the network

## If Something Seems Wrong, Notify IT

If your computer is infected with ransomware, you will typically be locked out of all programs and a “ransom screen” will appear. In the unfortunate event that you click a link or attachment that you suspect is malware or ransomware, please notify IT immediately.

**By Arun Douglas, Chief Technology/Security Officer at Collaborative Imaging.**

---

# New Research Says CT Radiomics Can Help Predict Tumor Behavior

Neale Pashley VP of Partner Services

Researchers from the H. Lee Moffitt Cancer Center and Research Institute in Tampa, FL, have found strong evidence that CT radiomics features can help predict tumor behavior in screening-detected lung cancer. PET/CT radiomics have also shown possibility to non-small cell lung cancer (NSCLC) treatment decisions.

Two CT radiomics features and a tumor volume doubling time (VDT) threshold found a high degree of accuracy for predicting survival outcomes. This was reported by first author Jaileene Pérez-Morales, PhD of Moffitt Cancer Center at the recent virtual 2020 North American Conference on Lung Cancer.

“Utilizing VDT and radiomic features, decision tree analysis identified subsets of screen-detected lung cancers associated with very poor survival outcomes suggesting such patients may [need] more aggressive treatment, such as adjuvant therapies, and more aggressive surveillance/follow-up,” the authors wrote.

## How can this predict cancer

## outcomes?

Moffitt's researchers generated models from cases found in lung cancer screening and looked at radiomics features and tumor volume doubling time to predict outcomes. Patient data and CT images from National Lung Screening Trial (NLST) were used. They first calculated VDT as the difference between two LDCT exams performed approximately one year apart.

Next, they took 155 intratumoral and 109 peritumoral radiomic features from the LDCT exams. After performing classification and regression tree (CART) analyses using overall survival as the main endpoint, the researchers found that the best predictive performance was achieved by using a combination of a tumor VDT threshold of 234 days and two CT radiomics features – compactness and average co-occurrence.

This isn't Moffitt's first major study in this field. Another study, led by Matthew Schabath, PhD, found that a deep learning algorithm could use PET/CT radiomics to identify the best treatment option for NSCLC. The researchers shared their findings in an article published online October 16 in Nature Communications.

In that project, the group retrospectively used F-18 FDG PET/CT data from two hospitals in China for training a deep-learning model to classify a NSCLC patient's epidermal growth factor (EGFR) mutation status, an important predictor for patient treatment. Patients with an active EGFR mutation status respond better to tyrosine kinase inhibitor (TKI) treatment than immune checkpoint inhibitor (ICI) therapy.

After analyzing the images, the model generates an EGFR deep-learning score to classify their EGFR mutation status. The researchers subsequently tested the algorithm on patient data from a different hospital in China as well as Moffitt.

The deep-learning score yielded an AUC of 0.81 on the training

set for discriminating between EGFR-mutant type from wild type, much higher than the AUC of 0.50 produced by the commonly used SUVmax measure, according to the authors.

## Progression-free Survival Research

Progression-free survival was found to be significantly longer ($p = 0.01$) in TKI-treated patients who had a high EGFR deep-learning score than those who had a low deep-learning score. Equally, patients who had lower deep-learning scores and who had received immune checkpoint inhibitor treatments also had significantly longer progression-free survival than those with higher deep-learning scores ($p < 0.001$).

“We found that the EGFR deep-learning score was positively associated with longer progression-free survival in patients treated with tyrosine kinase inhibitors, and negatively associated with durable clinical benefit and longer progression-free survival in patients being treated with immune checkpoint inhibitor immunotherapy,” said co-author Robert Gillies, PhD, in a statement. “We would like to perform further studies but believe this model could serve as a clinical decision support tool for different treatments.”

Past studies have utilized radiomics as a noninvasive approach to predict EGFR mutation status, noted first author Wei Mu, PhD. But Moffitt’s had the best results.

“Compared to other studies, our analysis yielded among the highest accuracy to predict EGFR and had many advantages, including training, validating and testing the deep learning score with multiple cohorts from four institutions, which increased its generalizability,” she said in a statement.

**By Neale Pashley,  VP of Partner Services at**

# Study Shows Fast MRIs Effectively Detect Traumatic Brain Injury in Children

Annually, throughout the US, Traumatic Brain Injury (TBI) in children results in more than 1.5 million emergency room visits, with up to 70 percent of these children being exposed to ionized radiation while undergoing computed tomography (CT) scans. This exposure to ionized radiation during CT scans prompted a group of researchers from the University of Colorado School of Medicine (CU SOM) to find a safer option for the detection of traumatic brain injury in children. The CU SOM researchers conducted a study to determine if a form of MRI (magnetic resonance imaging) could be used instead of a CT scan for accurately diagnosing TBI. Specifically, these researchers wanted to know if a fast MRI could replace the computed tomography scan.

## Children Are at a Greater Risk of Experiencing the Negative Side Effects of Radiation

While radiation exposure can have negative consequences for people of all ages, the risk to children is greater because their tissues are still growing. These growing tissues are more vulnerable to the effects of radiation. Furthermore, children’s neurologic exams are less reliable and since children are at the beginning of their lives, they have a

longer period of time for harmful mutations to accumulate.

## Fast MRIs Are Commonly Used for Children with Shunted Hydrocephalus

Children who have shunted hydrocephalus have been undergoing the fast MRI procedure for some time. The fast MRI procedure eliminates ionized radiation exposure and offers a motion-tolerant protocol that does not require the use of sedation. Despite being a regular protocol for children with shunted hydrocephalus, fast MRI procedures have yet to be validated for use in children with a TBI. This critical gap led to the investigators measuring the diagnostic utility and feasibility of substituting a fast MRI for the gold standard CT scan which is typically used for children with TBI. The study, Fast MRI for Young Children with Traumatic Brain Injury, concentrated on children with traumatic brain injury who were under 6 years of age.

## The Study: Fast MRI for Young Children with Traumatic Brain Injury

The study began on June 2, 2015, and its completion date was June 4, 2018. This study aimed to determine if the fast MRI could correctly identify radiographically apparent traumatic brain injury that had already been discovered with a CT scan.

There were 225 children who participated in this study. All patients were under the age of 6 when they began their participation in the study. Each participant had visited a Level 1, pediatric trauma center’s emergency department. While receiving emergency medical care, each study participant underwent a head CT scan.

The children enrolled in this study received a fast MRI scan after having their head CT scan, ideally, researchers wanted the fast MRIs to be performed within the 24-hour timeframe following the head CT.

Two of the three pediatric radiologists independently interpreted the fast MRIs. These radiologists were denied access to the other imaging and clinical results as well as to the patient's initial clinical interpretations.

The fast MRI's accuracy was to be established by the presence of a radiographically apparent traumatic brain injury: The researchers used the results of the participant's earlier head CT scan as the criterion standard.

## Study Results

A successful completion of the fast MRI occurred in 99 percent of the participants. The head CT scans median imaging time was 59 seconds, whereas, the fast MRI scans was 365 seconds. A traumatic brain injury was identified by the computed tomography scan in 111 of the children. Meanwhile, the fast MRI identified 103 TBIs (of the 111), thus, offering a sensitivity of 92.8 percent.

The researchers determined that a fast MRI is a plausible alternative to the computed tomography scan for the evaluation of children who have TBI. These findings are reported in, Feasibility and Accuracy of Fast MRI vs. CT for TBI in Young Children, which is published in the Oct. 1, 2019, Volume 144, Issue 4, of Pediatrics.

Lead author Daniel Lindberg, MD, who is the associate professor of emergency medicine at CU SOM, stated, "We found that fast MRI is a reasonable alternative to CT. Nearly all (99 percent) of fast MRIs were completed successfully, with accuracy that was similar to CT, while avoiding the harms of radiation exposure." In the same statement, Lindberg said,

“While we believe our findings reveal a feasible alternative to CTs in pediatric specialty centers, further study is necessary to test the results in other settings.”

---

# How Artificial Intelligence Can Help the Global Pandemic

New Study shows how Artificial Intelligence (AI) can help with the global pandemic. Recently, an (AI) algorithm was able to distinguish between cases of COVID-19, influence, pneumonia, and healthy subjects on CT exams. Chinese researchers published an article online on October 9th yielding a very high accuracy rate.

Not only did it have a very high accuracy rate, but it outperformed five experienced radiologists who participated in the study. The algorithm also showed good generalizability when applied to external test sets, according to first co-authors Dr. Yukun Cao of Tongji Medical College in Wuhan and Cheng Jin of Tsinghua University in Beijing.

The authors write, that since radiologists can perform an individualized diagnosis of COVID-19 with the AI system, this system, could be a new driving force for fighting the global spread of the outbreak.

How did they train and test this system? They used 4,260 CT scans gathered from 3,177 subjects from three centers in Wuhan. Of these studies:

– 2,529 were COVID-19 scans

– 1,338 were cases of community-acquired pneumonia

– 135 were influenza A/B studies

– 258 were normal patients

Another plus is that the AI system is that much faster. It took an average of 2.73 seconds to analyze each study, compared with an average of 6.5 minutes by the radiologists. Although the algorithm performed slightly worse in distinguishing between pneumonia and nonpneumonia, it outperformed the radiologists for the more challenging tasks of distinguishing between community-acquired pneumonia and COVID-19, as well as between COVID-19 and influenza, according to the group.

The AI system even performed with slightly less errors than the radiologists did. Of the 26 errors made by radiologists in distinguishing between COVID-19 and community-acquired pneumonia, 23 (88.5%) were correctly classified by the AI system. Similarly, 20 (86.9%) of the 23 mistakes made by radiologists in distinguishing between influenza and COVID-19 were correctly categorized by the AI software, the researchers noted.

## What do these results mean?

These prove that AAI can be used as an effective reader to provide reference suggestions, independently, the authors wrote. It can also screen out suspicious patients for radiologists to confirm/ Or, it can give possible diagnosis error warnings made by radiologists.

As they continue with their research, applying radiomics analysis to Ai results can potentially lead to discovering new biomarkers for COVID-19, which would make our knowledge during this pandemic far improved.

See the published article in *Nature Communications* for more about the study.