Report on
Medicare Compliance

Volume 30, Number 9 • March 8, 2021

Weekly News and Compliance Strategies on Federal Regulations, Enforcement Actions and Audits

Contents

HCCA

Managing Editor
Nina Youngstrom
nina.youngstrom@hcca-info.org

Copy Editor
Bill Anholzer
bill.anholzer@hcca-info.org

OFAC Fines Add to Ransomware Peril; 'It's a Between-a-Rock-and-a-Hard-Place Thing'

Organizations have been warned by the U.S. Office of Foreign Assets Control (OFAC) that they may be fined if they pay ransom to "malicious cyber actors" to unlock their information systems. That complicates the decision whether to pay when attacked by ransomware and its variant, distributed denial of service (DDoS). Health systems should incorporate OFAC penalties into their prepayment due diligence and cybersecurity programs, attorneys said. They may pay the ransom anyway but will do it with their eyes open. This adds another dimension to ransomware at a time when the number of attacks is rising and cybercriminals may use artificial intelligence to make a bad situation worse.

In an Oct. 1 advisory,[1] OFAC stated that organizations are subject to fines if they paid ransom to people or entities on its "Specially Designated Nationals and Blocked Persons List (SDN List), other blocked persons, and those covered by comprehensive country or region embargoes (e.g., Cuba, the Crimea region of Ukraine, Iran, North Korea, and Syria)." That puts hospitals and health systems in a difficult position because they need to regain access to their protected health information (PHI) and business records immediately, especially if threat actors have hijacked their backup systems.

"It's a between-a-rock-and-a-hard-place thing," said Dave Summitt, chief information security officer at Moffitt Cancer Center in Tampa, Florida. "You may not have a choice to pay the ransom and make a recovery." But now hospitals must

continued on p. 5

Phasing Out IPO List May Not Slow Admissions; 'Because' Is Key Word for Medical Necessity

Orthopedic and spine surgeons at hospitals across the country are now making patient-status decisions for the first time on musculoskeletal procedures that CMS moved off the inpatient-only (IPO) list Jan. 1, although some procedures may continue to be performed mostly on inpatients. That was the first step in the process of eliminating the IPO list completely by 2024, putting all 1,740 procedures under the purview of Medicare's two-midnight rule.

CMS announced the sea change in the 2021 outpatient prospective payment system rule,[1] but hospitals already dipped their toes in the water when total knee arthroplasty (TKA) was pushed off the IPO list in 2018, and CMS did the same with total hip arthroplasty (THA) in 2020.

"Some hospitals are still doing every total knee replacement as inpatient," according to national data from the Program for Evaluating Payment Patterns Electronic Report, better known as PEPPER, said Ronald Hirsch, M.D., vice president of R1 RCM, at a Feb. 25 virtual presentation at Hughston Orthopedic Trauma, an acute-care hospital owned by a group of orthopedic surgeons. "I can't look at their charts to know if there is something special about their cases. Possibly they only

continued

treat morbidly obese or sleep apnea patients but I doubt that," Hirsch said. "I suspect it's due to ongoing confusion about how to interpret Medicare guidelines on who can be an inpatient."

There was no culture shock for surgeons at one hospital when CMS pushed musculoskeletal services off the IPO list. Val Kraus, vice president of case management, said his hospital, which he prefers not to identify, continues to admit most patients because they're overwhelmingly complex cases and typically cross two midnights. "We don't do a lot of simple orthopedic procedures," he said. "We have been working on beefing up the medical necessity piece."

Medicare typically pays much more for musculoskeletal procedures performed on inpatients versus outpatients, although the hospital uses "the same operating room, the same RN [registered nurse] and the same surgeon" in both settings, Hirsch said. For example, the MS-DRG for total joint replacement pays $12,137, while the ambulatory payment classification (APC) reimbursement is $10,970, and the ambulatory surgery center (ASC) payment is $7,962 (geographically adjusted for Columbus, Georgia/Alabama). The MS-DRG for lumbar fusion is $25,124, the APC is $10,970 and the ASC payment is $7,828. "Of course, don't change your plans" for patients because procedures are off the IPO list, Hirsch said. "You can't keep them longer for more money."

This year's IPO change only applies to musculoskeletal procedures in CPT code range 20,000, which are orthopedic services, Hirsch said. CMS didn't touch the 60,000 list, which includes neurosurgery (e.g., some spine procedures). They're still on the IPO list, which means Medicare only pays hospitals when they're performed on inpatients. Medicare Advantage plans are not required to follow the IPO list and require many procedures to be performed in ambulatory surgery centers because the cost is lower.

Physicians Are Asked to Explain Their Decisions

Kraus said his hospital has completed education of the hospitalists and is moving on to the surgeons. Patient status orders give them four choices: inpatient, outpatient in a bed, observation and extended recovery. When physicians select inpatient, they must answer two questions, with an emphasis on the word "because," which helps supports medical necessity:

1. The patient needs to be in the hospital because (e.g., their oxygen saturation is below 90% and they need intensive monitoring and oxygen support they can't receive at home).
2. The patient is expected to cross two midnights because (e.g., this happened to the patient twice in the past three years, and both times it took three or four days for the patient's oxygen level to return to normal).

Kraus is wary of the use of the word "stable" in medical record documentation. Often physicians document "patients are stable and improving, expect one more day." Although stable is not the best word choice, physicians use it because the patient isn't deteriorating, he said. Unfortunately, auditors may interpret it to mean the patient didn't need to be in the hospital. When physicians use the word stable, Kraus recommends they explain that patients have to meet certain milestones before discharge, "and that's something surgeons often don't do." For example, physicians could elaborate that patients with a lot of intraoperative bleeding should have their hemoglobin and hematocrit at a certain level, adequate pain control and capacity to ambulate a certain distance.

Four Concepts Drive Patient Status Decisions

Hirsch described four basic concepts for physicians to apply when deciding how to status a patient having a procedure that's not on the IPO list:

1. **Complexity**. If complexity raises the patient's risk in the operating room (OR), physicians can

Report on Medicare Compliance (ISSN: 1094-3307) is published 45 times a year by the Health Care Compliance Association, 6462 City West Parkway, Eden Prairie, MN 55344. 888.580.8373, hcca-info.org.

Subscriptions to *RMC* include free electronic delivery in addition to the print copy, as well as a searchable database of *RMC* content and archives of past issues at compliancecosmos.org.

To order an annual subscription to **Report on Medicare Compliance** ($665 for HCCA members; $765 for nonmembers), call 888.580.8373 (major credit cards accepted) or order online at hcca-info.org.

Subscribers to this newsletter can receive 20 non-live Continuing Education Units (CEUs) per year toward certification by the Compliance Certification Board (CCB)®. Contact CCB at 888.580.8373.

admit the patient even if they plan to discharge the patient the next day, he said. For example, a patient may be admitted pre-op because of osteoporotic bone and extreme degree of deformity. "This surgery will be high risk, and admission is warranted because if you hit the bone wrong, it will shatter," he said. "Document your thought process preoperatively, and you can make the patient an inpatient." But don't get carried away. "We don't want every patient going into the OR with a note saying, 'This surgery will be difficult so I will make them inpatient.'"

2. **Surgical risk due to comorbid conditions**. Medicare says patients may be admitted for a procedure when they have medical comorbidities that raise risk if it's "real, delineated and attributed," Hirsch said. The physician must document the comorbidities before admission, and it depends on the comorbidity and the circumstances. A patient who has poorly controlled diabetes with A1C of 8% on insulin and chronic obstructive pulmonary disease and uses two inhalers probably should be admitted, but that's not the case for all diabetics. Class 2 and 3 of the American Society of Anesthesiologists (ASA) physical status classification for assessing the fitness of patients before surgery may not be a road map for inpatient versus outpatient settings, Hirsch said. ASA Class 3 is not "automatically inpatient," and ASA 2 isn't always outpatient.

   "Some surgeons say, 'I don't operate on people with a BMI over 40.' If you don't operate on high-risk people, you can't use that to justify admissions," he noted. Other comorbidities physicians can consider include dementia, BMI over 40, chronic arrythmia, chronic kidney disease stage 3 or more, hypertension on multiple medications and respiratory disease on chronic steroids.

   "Higher risk is relative," Hirsch said. For example, a 2017 study in the *Journal of Arthroplasty*[2] reported a higher risk of in-hospital post-operative complications (IHPC) in Type 2 diabetes patients after joint arthroplasty, and "IHPC may result in a higher risk of mortality in patients undergoing TKA." Diabetics are 4.5 times more likely to die, the study found. "It is a much bigger risk than nondiabetics, even if the absolute risk is small," Hirsch noted.

3. **Time needed to discharge**. "CMS knows your length of stay history, so don't change your standard practice," Hirsch said. For example, if surgeons keep multilevel cervical fusions two days, they can be inpatients. Sometimes physicians realize an outpatient who is expected to go home post-op day is not safe for discharge. "If you document why, you can admit them as inpatients," Hirsch said. Reasons include "drainage greater than expected," "swelling at site needs monitoring," and "patient hallucinating." Also, when patients recover faster than expected, CMS accepts a short stay as an admission under the two-midnight rule if it's documented. "It has to make sense," he said. "You can't admit to monitor a wound for two days and then say 'never mind' and discharge on day one."

4. **Discharge destination**. Another factor that supports inpatient admission is the patient's need for a skilled nursing facility admission or other post-acute care after discharge, whether or not there's a three-day qualifying stay. The qualifying stay requirement has been waived during the COVID-19 public health emergency.

Rachael Crenshaw, compliance officer and chief operating officer of Hughston Orthopedic Trauma, said the biggest challenge with physicians and the two-midnight rule is "their assessment is so intuitive" but not necessarily translated to paper. "It's an art. It's hard. Physicians are thinking clinically and forgetting about all the guardrails and rules. Our takeaway is to stratify more appropriately on the front end." For example, physicians identify patients with comorbid conditions, such as stroke, and whether they need more post-op monitoring.

Contact Hirsch at rhirsch@r1rcm.com and Henshaw at rcrenshaw@hughston.com. ✧

Endnotes

1. Medicare Program: Hospital Outpatient Prospective Payment and Ambulatory Surgical Center Payment Systems and Quality Reporting Programs; New Categories for Hospital Outpatient Department Prior Authorization Process; Clinical Laboratory Fee Schedule: Laboratory Date of Service Policy; Overall Hospital Quality Star Rating Methodology; Physician-Owned Hospitals; Notice of Closure of Two Teaching Hospitals and Opportunity To Apply for Available Slots, Radiation Oncology Model; and Reporting Requirements for Hospitals and Critical Access Hospitals (CAHs) To Report COVID–19 Therapeutic Inventory and Usage and To Report Acute Respiratory Illness During the Public Health Emergency (PHE) for Coronavirus Disease 2019 (COVID–19), 85 Fed. Reg. 85,866 (December 29, 2020), https://bit.ly/3v2tktF.
2. Maria A. Martínez-Huedo et al., "Effect of Type 2 Diabetes on In-Hospital Postoperative Complications and Mortality After Primary Total Hip and Knee Arthroplasty," *Journal of Arthroplasty* 32, no. 12 (December 2017), http://bit.ly/3bfxczg.

Medical Group Pays $373,715 to Settle CMP Case on Supervision

Children's Hospital Los Angeles Medical Group has agreed to pay $373,715 to settle allegations it billed for radiology services performed by residents without "appropriate" supervision, according to a civil monetary penalty settlement with the HHS Office of Inspector General (OIG). This is the latest in a series of settlements with providers for submitting claims for services that were performed by residents without the physical presence of the teaching physicians.

Teaching physician billing "is still very much a live issue," said attorney David Vernon, with Hooper, Lundy & Bookman in Washington, D.C. "Going back to the OIG Physicians at Teaching Hospitals audits 25 years ago, it has gotten the government's attention for many years as an area of potential fraud." Meanwhile, as with everything since the COVID-19 pandemic, CMS has given teaching physicians the flexibility to supervise residents virtually.

The settlement, which was obtained through the Freedom of Information Act, stemmed from a self-disclosure to OIG by Children's Hospital Los Angeles Medical Group. OIG alleged the medical group knowingly submitted claims to Medicaid for services it knew were fraudulent. From Feb. 1, 2013, through March 31, 2018, the medical group billed Medicaid for radiology services performed by a physician that allegedly "were not provided as claimed because the radiology images were reviewed and the radiology reports were prepared by residents without appropriate supervision and review" by the physician.

Children's Hospital Los Angeles Medical Group didn't admit liability in the settlement and said in a statement that it's "committed to engaging in fair and equitable billing for professional services. In the unlikely event that inaccurate billing should occur through a reporting error, the Group's policy is to move quickly to disclose it and work closely with the appropriate agencies to address the matter in the most collaborative manner possible." Otherwise, it declined to provide any details about the self-disclosure.

In the Medicare arena, a number of hospitals have settled cases over teaching physician billing. Last year, University of California Los Angeles (UCLA) Health System agreed to pay $241,033 to settle a civil monetary penalty case over a teaching physician's billing. According to the settlement, OIG alleged that UCLA Health System submitted claims to Medicare and TRICARE for services provided by a physician when allegedly the services were actually provided by "international fellows or Accreditation Council for Graduate Medical Education residents and domestic fellows, outside [the physician's] physical presence and without his supervision" between Jan. 1, 2014, and Feb. 5, 2018. The settlement stemmed from a self-disclosure.

CMS Has Relaxed Documentation Standards

Medicare allows teaching physicians to bill for services furnished in teaching settings through the Medicare Physician Fee Schedule (MPFS), including evaluation and management (E/M) services, performed by the residents they supervise, even though their hospitals already receive graduate medical education payments. To receive separate E/M reimbursement, teaching physicians must document "that you performed the service or were physically present during the critical or key portions of the service furnished by the resident and your participation in the management of the patient," according to a March 2018 *MLN Booklet*.[1]

In the past couple of years, CMS has relaxed documentation requirements for physical presence. Teaching physicians are now free to let residents and nurses document most of their E/M services, as long as their physical presence is noted in the medical records, according to the 2019 MPFS rule. A year later, the MPFS rule said physicians, physician assistants and advanced practice registered nurses who perform and bill for their professional services only have to verify, rather than re-document, information in the chart from the members of the medical team, including residents and nurses.

With radiology, Medicare pays teaching physicians for interpreting diagnostic radiology and other diagnostic tests if the interpretation was performed or reviewed by physicians other than the resident. "The documentation has to indicate the physician reviewed the resident's interpretation," Vernon said. The physician can't take the resident's word for it.

CMS OKs Virtual Supervision of Test Interpretations

The public health emergency (PHE) has opened the door to the use of telehealth for supervision in phases. Starting March 31, 2020, as part of the first COVID-19 interim final rule with comment (IFC), Medicare paid physicians for radiology test interpretations performed by a resident when the teaching physician is present through interactive telecommunications technology, Vernon said. CMS updated the requirement in its May 8 IFC and then again in the 2021 MPFS,[2] which states that "physician fee schedule payment may also be made for the interpretation of diagnostic radiology and other diagnostic tests if the interpretation is performed by a resident when the teaching physician is present through audio/video real-time communications technology. The medical records must document the

extent of the teaching physician's participation in the interpretation or review of the diagnostic radiology or diagnostic test."

Vernon said while the MPFS change applies to all teaching settings during the PHE, the use of virtual supervision is permanent for residency training sites that are located outside of a metropolitan statistical area "to bolster rural training opportunities and rural area health care access."

Contact Vernon at dvernon@health-law.com. ✧

Endnotes

1. CMS, "Guidelines for Teaching Physicians, Interns, and Residents," *MLN Booklet*, ICN 006347, March 2018, https://go.cms.gov/2PEcUHx.
2. Medicare Program; CY 2021 Payment Policies Under the Physician Fee Schedule and Other Changes to Part B Payment Policies; Medicare Shared Savings Program Requirements; Medicaid Promoting Interoperability Program Requirements for Eligible Professionals; Quality Payment Program; Coverage of Opioid Use Disorder Services Furnished by Opioid Treatment Programs; Medicare Enrollment of Opioid Treatment Programs; Electronic Prescribing for Controlled Substances for a Covered Part D Drug; Payment for Office/Outpatient Evaluation and Management Services; Hospital IQR Program; Establish New Code Categories; Medicare Diabetes Prevention Program (MDPP) Expanded Model Emergency Policy; Coding and Payment for Virtual Check-in Services Interim Final Rule Policy; Coding and Payment for Personal Protective Equipment (PPE) Interim Final Rule Policy; Regulatory Revisions in Response to the Public Health Emergency (PHE) for COVID–19; and Finalization of Certain Provisions from the March 31st, May 8th and September 2nd Interim Final Rules in Response to the PHE for COVID–19, 85 Fed. Reg. 84,472 (December 28, 2020), https://bit.ly/398n6hu.

OFAC Fines Add to Ransomware Peril

continued from page 1

consider the risks in the advisory from OFAC, which is part of the Treasury Department, and "pull OFAC into their overall cyber preparedness and response plan," said David Rybicki, former deputy assistant attorney general. "Treasury wants to send a message you can face liability and will expect internal controls that are OFAC specific and pressure tested," said Rybicki, now an attorney with K&L Gates in Washington, D.C.

The OFAC advisory said there was a 37% increase in ransomware attacks from 2018 to 2019. "Our systems detect a ransomware attempt probably every week, three to four times," Summitt said. They're costing organizations a fortune, whether or not they pay the ransom. A cyberattack cost Universal Health Services, a huge hospital chain, $67 million in pre-tax losses, according to CyberScoop.[2] A Sept. 27 breach led to delayed billing, diversion of ambulances to competitors and spending on labor to restore connectivity.

The OFAC advisory said it could levy civil penalties on organizations for violations based on strict liability, which means they can be fined even if they didn't know they were engaging in a transaction with a person or entity on the SDN List.

'The Government Views You as the Perpetrator'

"You can have a situation where you are the victim and the government views you as the perpetrator," said attorney Christopher Swift, who investigated and prosecuted sanctions cases at the Treasury Department before he joined Foley & Lardner. In the eyes of OFAC, "it's kind of like paying a terrorist group." OFAC said it's concerned that ransomware payments to cybercriminal organizations, such as Russia-based Evil Corp, "could be used to fund activities adverse to the national security and foreign policy objectives of the United States."

Organizations invite sanctions when they rush to pay ransom without investigating the hacker. "There is a knee-jerk reaction to 'get my stuff back as soon as possible because of HIPAA,' and that can sometimes lead people to make decisions before they know what they're dealing with," Swift said. "Make sure senior leaders know about the sanctions risk. When you have tabletop exercises or standard operating procedures to deal with ransomware, a sanctions assessment should be baked into that cake."

Whether to pay a ransom is always a torturous question. Hospitals don't want to encourage cybercriminals, and there's a risk they won't get the decryption key even if they pay. Sometimes hospitals say no and just rely on their backup systems, although the cybercriminals could post the PHI on the internet in retaliation. Whatever the calculation, the potential OFAC sanctions take hospitals into dangerous territory.

"It's important to recognize that the OFAC guidance doesn't stand for the proposition that some have attributed, which is you can never pay ransom payments," said former federal prosecutor Robert Trusiak, an attorney in Buffalo, New York. "You can in certain circumstances. But you need to appreciate, despite the fact that everyone is running around with their hair on fire because you don't have access and the threat actor is threatening to publish your PHI in 96 hours if you don't pay, that you need to do work items as it relates to ensuring you're not dealing with a terrorist organization."

That's where a forensic investigation comes in, Swift said. That will help hospitals figure out if the threat actor is a sanctioned entity. There are clues, such as the

cryptocurrency wallet address, the type of malware used and whether the ransom demand suggests English is not the threat actor's first language. "All of these things go into the analysis of what flavor risk you have," he said.

HIPAA and OFAC: Carrot and the Stick

Whether hospitals pay the ransom depends on several factors, Rybicki said. They include the nature of the breach, patient and financial considerations, whether information was backed up, and whether the cybercriminal is on the SDN List. "There are a lot of covered entities that make the calculation they need to pay based on the gravity of the situation," Rybicki said. "But management would need to undertake a highly fact-specific analysis before acting."

The OFAC part is a prepayment due diligence matter for hospitals and other organizations, he said. "They need to determine using outside counsel and third-party vendors whether paying the ransom creates exposure," Rybicki said. OFAC will take into consideration the due diligence and internal controls if an organization unwittingly makes a ransomware payment to an entity on the SDN List.

Summitt is skeptical that the Treasury Department will fine a health care organization for paying ransom in the service of patients, and some of the attorneys agreed the OFAC advisory may be intended to motivate more effective cybersecurity programs. Trusiak thinks the federal government and New York state's Department of Financial Services, which on Feb. 4 published an OFAC-like framework,[3] are pursuing a carrot-and-stick approach to better cybersecurity, Trusiak said. The carrot is the HIPAA safe harbor enacted by Congress late last year in an amendment to the Health Information Technology for Economic and Clinical Health Act,[4] which was signed into law Jan. 5. It requires the HHS Office for Civil Rights to consider recognized security practices of covered entities when calculating fines for violations of HIPAA privacy and security rules. Penalties may be reduced if security practices have been in place for the previous 12 months. The provision is retroactive to Dec. 13, 2016, the signing of the 21st Century Cures Act.

The stick is the OFAC penalties. "Cybersecurity and ransom payments are quickly devolving into a Hobson's choice for providers," Trusiak said. You either pay the ransom and "risk being victimized twice, by the state or federal government or both, or don't pay and risk having your doors shuttered." He thinks implementing a zero-trust solution avoids the Hobson's choice. Zero trust, as the name implies, prevents people, internally and externally, from connecting to the network unless they have specifically been given permission through authentication. "A zero-trust solution right now is the best approach to hardening the cybersecurity environment," Trusiak said.

Sometimes You Can Just Say No

Sometimes ransomware attacks pose little threat and health care entities don't have to make risk calculations about OFAC, said Gina Bertolini, an attorney with K&L Gates in Research Triangle Park, North Carolina. She recently helped a provider in this position after an employee clicked on a phishing email from a hacker posing as a DHL carrier with a shipping update. The hackers unleashed malware, which remained in the provider's computer system undetected for months. The hackers were able to tap into and exfiltrate data, but it wasn't extensive enough to disrupt the provider's business, Bertolini said. Eventually, some employees noticed unusual activity and reported it. Although it took some time for the provider to find the ransom note, it didn't pay the threat actor, she said. After a forensic analysis, the provider determined the threat actor hadn't permanently removed anything, Bertolini said. "We had backups of everything," she noted. "Most of the records they accessed were business records." Because a small percent had PHI, the provider reported the breach to the HHS Office for Civil Rights and to patients. "They did everything right once they discovered it," she noted, including improving education and upgrading information technology tools.

Bertolini suggested health systems build ransomware protections and the OFAC due diligence process into their enterprise-wide HIPAA privacy and security program. "HIPAA has standards and specifications with built-in flexibilities for covered entities to determine for themselves how to protect the integrity of their PHI," she said. They should use that flexibility to determine what tools they need to prevent attacks and how to proceed if they have one. "A robust security compliance program integrates the OFAC guidance on ransomware," she noted.

Bad Actors Demand Ransom to Stop DDoS

There's more than one kind of ransomware attack; DDoS is another threat in this vein, Summitt said. Threat actors set up robocalls at such a high volume they jam phone lines, preventing people at hospitals from calling out and vice versa, which only stop when hospitals pays a ransom or when they take extra steps working with their telecom company, he said. Moffitt works closely with its telecom company to help prevent these events and has reported some to the FBI.

Hackers also have been calling physicians and other clinicians, pretending to be from the Department of Justice or state of Florida medical or

continued on p. 8

Checklist: Preparing for Downtime Caused by a Cybersecurity Event

The Technical Resources, Assistance Center, and Information Exchange in the HHS Office of the Assistant Secretary for Preparedness and Response, better known as ASPR, created this checklist to help organizations prepare for a cyberattack.[1]

HOSPITAL DOWNTIME PREPAREDNESS CHECKLIST

Early preparation and proactive planning for a possible cyber emergency across the hospital or facility will increase effective ***continuity of operations*** and ensure patient safety.

- ❒ Establish a downtime planning team to oversee preparation efforts, manage ongoing activities, update plans, reinforce training; include IT experts, front-line professionals, hospital operations staff.
- ❒ Schedule regular processes for reviewing, updating, approving downtime procedures, forms, back-up medical equipment; ensure new/updated forms are compliant, approved by appropriate leads.
- ❒ Plan for extended downtime disruptions to healthcare operations and patient care (e.g., affected IT systems prompt closing of services). Pre-define criteria for altering services, facility operations.
- ❒ Establish a "knowledge center" or web-based IC system to store cyber event related information (e.g., status updates, tasks, IT service requests). Ensure staff know how to use the system, understand limitations (e.g., user can only log in as one role though they work at different facilities).
- ❒ Ensure computers have necessary downtime software and are tested regularly.
- ❒ Plan for impacted shared drives impacting operations. Consider options for secondary access to critical information (e.g., hospital policies, patient information, employee schedules, on call schedules, staff, and vendor contact information).
- ❒ Identify secure and convenient area(s) in the hospital to setup paper-based downtime workstations for organizing administrative records, patient charts, and orders. Ensure it is large enough to accommodate several portable workstations and follow facility security requirements.
- ❒ Develop a comprehensive list of all biomedical equipment, their location, and interdependencies. Have downtime procedures documented for all equipment. If report-back to the EHR is disrupted, have a downtime procedure workflow in place.

  Have offline.
- ❒ Plan a workaround for verifying/documenting health insurance; collecting payment if financial systems are down (e.g., payroll systems, cash payments, procurement cards). Develop downtime ordering and billing workflow instructions (e.g., use of barcodes, hardcopy list of billable supplies, procedure, and process codes).
- ❒ Inventory older clinical equipment that does not require Internet connectivity or systems access. Assess their condition, document location, and log with other downtime documentation.
- ❒ Prepare for use of dictation. Create instruction cards for staff unfamiliar with the process and for consistency in dictation style. Maintain a cache of handheld devices, decide who will control them; identify where to submit devices for transcription.
- ❒ Have color coded paper on-hand to easily identify STAT lab orders, and to prevent non-critical orders from being submitted as high-priority due to lab backlogs during downtime.
- ❒ Publish and regularly update a repository of nursing station, office, pneumatic tube station numbers.
- ❒ Ensure adequate supplies of folders, binders, hole punchers, labels for paper charts; avoid having to prepare/procure items during an emergency. Have thumb drives and/or CDs needed to create files.
- ❒ Be prepared to move copiers/scanners. Map their location/capacity (numbers, color/non color). Ensure adequate paper and toner supplies. Have printing instructions available at workstations for printing medical orders and other information not normally in "printable" format (i.e., how to take a screenshot, reformat documents for print, send jobs to proper printer).

Endnotes

1. Office of the Assistant Secretary for Preparedness and Response, "Hospital Downtime Preparedness Checklist," HHS, accessed March 4, 2021, https://bit.ly/2O6grOe.

pharmacy licensing agency. They tried to elicit personal information from some clinicians. "Sometimes it was to do prescription fraud," Summitt said. "It was really scary for the providers." They have been educated to contact Moffitt's cyber team when they receive these calls. "The overwhelming majority of the time, you hang up on the caller."

What lies ahead sends shivers down the spine. "Machine learning and artificial intelligence are starting to take off, and the bad actors are starting to take advantage of it," Summitt said. For example, they potentially can use deep fake video and audio to mimic the CEO and request a wire transfer or sensitive business/patient information. That's harder to prevent or expose than business email compromise, where hackers pose in email as CEOs or other executives.

To prevent ransomware attacks, Moffitt uses a "defense in depth" strategy. It starts with user education (e.g., on phishing) because 65% to 95% of ransomware attacks occur through an email. Also, "we isolate all attachments and have them checked before we release them to users" and check incoming links. Another layer is workstation protection. "If [users] download a malicious user file, we don't allow it to propagate," Summitt said. Moffitt also does a lot of monitoring. If something is triggered, hopefully Moffitt's response is quick enough to remove the malware before it moves from computer to computer. "You don't rely on one control," he explained. "We probably have four layers of defense at Moffitt before a ransomware event can take hold." Other layers include the firewall, anti-virus software and patching. "There is no single bullet in defending against ransomware" because "it's high risk, high probability," Summitt said.

Attorney Jennifer Urban, with Foley & Lardner in Chicago, encourages organizations to work with the FBI and other law enforcement agencies when they're hit with ransomware attacks. Even organizations with the best cybersecurity will be victims of cybercrime.

"There's no foolproof security solution," Urban said. Organizations should focus on a risk-based method, she said. "You do your due diligence on the front end" and mitigate on the back end with security controls.

Contact Summit at dave.summitt@moffitt.org, Bertolini at gina.bertolini@klgates.com, Rybicki at david.rybicki@klgates.com, Trusiak at robert@trusiaklaw.com, Swift at cswift@foley.com and Urban at jurban@foley.com. ✧

Endnotes

1. U.S. Department of the Treasury, "Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments," advisory, October 1, 2020, https://bit.ly/3kL666e.
2. Sean Lyngaas, "Universal Health Services reports $67 million in losses after apparent ransomware attack," CyberScoop, March 1, 2021, http://bit.ly/3sO0dZ4.
3. New York state Department of Financial Services, "Cyber Insurance Risk Framework," Insurance Circular Letter No. 2, 23 NYCRR 500, February 4, 2021, http://on.ny.gov/3e9lvfG.
4. To amend the Health Information Technology for Economic and Clinical Health Act to require the Secretary of Health and Human Services to consider certain recognized security practices of covered entities and business associates when making certain determinations, and for other purposes, H.R. 7898, 116 Cong. (2020), http://bit.ly/2Lm9KG1.

NEWS BRIEFS

◆ **Hospital outpatient departments with "affirmation" rates of 90% or better in the prior authorization process for outpatient procedures will be "exempt from submitting prior authorization requests for dates of service beginning May 1, 2021," CMS said in updated answers to frequently asked questions[1] on the hospital outpatient prior authorization process.** Their Medicare administrative contractors (MACs) will send hospitals a notice of exemption in the mail or through the MAC provider portal. Not only are the hospitals with a 90% compliance rate off the hook for the five procedures subject to prior authorization, but they're exempt for two procedures that join the prior authorization process in July, said Ronald Hirsch, M.D., vice president of R1 RCM. "This is quite surprising in that these two procedures are not cosmetic-like, as with the other procedures, and the reimbursement is markedly higher," he said. "But hospitals would be wise to be sure to obtain all the required documentation as if prior authorization was needed since these surgeries will be subject to biannual chart audits."

◆ **California physician Ashok Kumar paid $215,228 to settle false claims allegations that he received kickbacks for referring patients to Memorial Hospital of Gardena, the U.S. Attorney's Office for the Central District of California said March 3.**[2] The lawsuit was set in motion by a whistleblower, Dr. Joshua Luke, the former CEO of Memorial Hospital of Gardena. The lawsuit alleged the hospital, which hired Kumar as a medical director, paid him compensation that was above fair market value and attempted to incentivize his patient referrals, the U.S. attorney's office said. Kumar didn't admit liability in the settlement.

Endnotes

1. CMS, "Prior Authorization Process for Certain Hospital Outpatient Department (OPD) Services Frequently Asked Questions (FAQs)," March 1, 2021, https://go.cms.gov/30nvB5N.
2. Department of Justice, U.S. Attorney's Office for the Central District of California, "South Bay Doctor Settles Federal Lawsuit Alleging He Accepted Illegal Kickbacks for Patient Referrals to Gardena Hospital," news release, March 3, 2021, http://bit.ly/3kMvbOc.