Closed Claim Review: Juries Get Good Medicine

By Stephanie Deupree, JD, BSN

Martha Mae Randolph, an active 74-year-old female with a history of esophageal stricture, GERD, and hiatal hernia presented to the office of general surgeon, Dr. Cameron Smith.[1] Approximately one year earlier, Dr. Smith had performed a robotic Nissen fundoplication with hiatal hernia repair. Although Mrs. Randolph initially reported relief from her symptoms related to GERD and the hiatal hernia after her surgery, over the last few months the symptoms had returned and, more recently, worsened.

Specifically, Mrs. Randolph had developed dysphagia, regurgitation, and odynophagia. These symptoms were increasing in frequency and severity. Eating had become very difficult. When she was able to eat, Mrs. Randolph experienced early satiety and nausea. All these issues led to unwanted and unneeded weight loss of 25 pounds within three months.

Dr. Smith ordered a battery of tests, including a barium swallow and endoscopy. The tests revealed esophagitis and a large recurrent paraesophageal hernia. Following the tests, Mrs. Randolph returned to see Dr. Smith. At that visit, Dr. Smith explained to Mrs. Randolph that she needed a revision surgery. Dr. Smith advised that he only performed this type of revision surgery with an open approach. Mrs. Randolph did not want an open procedure and expressed her desire for minimally invasive surgery. Due to Mrs. Randolph's strong preference for minimally invasive surgery, Dr. Smith referred her to Dr. David Cowen, a board-certified thoracic surgeon at a large metropolitan medical center known for his expertise with laparoscopic and robotic surgery.

Within a few weeks Mrs. Randolph had an appointment with Dr. Cowen. During the appointment with Mrs. Randolph, Dr. Cowen reviewed her symptoms along with the available diagnostic testing results. Dr. Cowen concluded that the patient needed surgery, but before scheduling revision surgery, he ordered a gastric emptying study and cardiac clearance.

Once these items were satisfactorily completed and revealed no problems, Mrs. Randolph, accompanied by her husband, returned to see Dr. Cowen. During the visit, Dr. Cowen explained to Mrs. Randolph that she was a candidate for laparoscopic revision surgery. He explained to Mrs. Randolph and her husband the difficulty of revision surgery, illustrating the anatomy and how he hoped to repair it. In addition, he gave handouts pertaining to hernias and the laparoscopic procedure. They had a lengthy discussion about the risks, benefits, and alternatives to surgery. Dr. Cowen advised the Randolphs of potential complications including damage to other organs, prolonged disability, and the risk of death. Nonetheless, Mrs. Randolph wanted to proceed with surgery. Dr. Cowen documented the informed consent process in great detail, and Mrs. Randolph was scheduled for surgery in one week.

The morning of surgery Dr. Cowen saw and examined Mrs. Randolph once again. She was given the opportunity to ask questions but declined. After the examination and discussion, Mrs. Randolph signed a detailed consent form for the surgery which outlined the significant risks and potential complications of the procedure including organ damage and death.

During the surgery, Dr. Cowen encountered significant scarring and severe fibrosis. While carefully dissecting to the esophagus, he faced significant fibrosis and unusually distorted anatomy all the way. When he reached the esophagus just under the pericardium, Dr. Cowen saw brisk bleeding coming from the hiatus. Believing there was a posterior heart injury, he immediately called for a stat cardiac surgery consultation.

Dr. Cowen did a quick laparotomy and placed his hand in the hiatus. Resuscitation efforts were initiated, blood products were administered, and the cardiac surgeon arrived within a few minutes. Upon arrival, the cardiac surgeon performed a median sternotomy which revealed an injury to the left atrium and pericardial tamponade. Despite the cardiac surgeon's efforts to repair the cardiac injury and the resuscitation efforts of the entire surgical team, Mrs. Randolph expired on the operating table. Dr. Cowen met with the Randolph family immediately after the surgery to explain what had happened and to offer his condolences.

Following Mrs. Randolph's death, her family decided to sue Dr. Cowen and his practice group. Years of litigation eventually led to a four-day jury trial. At trial, the Randolphs were able to paint a very sympathetic picture of a lady much loved by her family and community. Prior to her death Mrs. Randolph was still working part-time and was very involved in the lives of her children and grandchildren. Dr. Cowen's defense team never disputed any of this or maligned Mrs. Randolph in any way. In fact, the defense agreed that Mrs. Randolph was a lovely person by all accounts, and her death was a sad, unfortunate event.

As there was no question as to the cause of Mrs. Randolph's injury and death, when it was time for the defense team to present their proof, they focused on the standard of care. First, Dr. Cowen testified in his own defense, going through his informed consent discussion and process. He also testified about the surgery with the use of anatomical exhibits to help the jury understand what he saw and did. Dr. Cowen's testimony showed him to be a caring and conscientious physician who had grieved the unfortunate loss of his patient, whom he had been trying to help.

Second, two fully supportive medical experts testified at trial that Dr. Cowen complied with the standard of care throughout his treatment. The experts were able to explain to the jury the complexity of the surgery and how the injury could occur in the absence of any negligence. Their ability to walk the jury through the science and evidence was markedly different from the plaintiff's expert, who struggled to articulate his opinions in a clear and concise manner.

At the conclusion of the trial, the medical proof as presented by Dr. Cowen and the defense experts, along with Dr. Cowen's well-documented informed consent process, carried the day. The jury returned a defense verdict despite the very sympathetic nature of the case. Taking the time to document every step of the way through treatment ultimately helped Dr. Cowen prevail. The defense was able to show the jury all of Dr. Cowen's documentation, including office notes, history and physical note, operative report, and consent form. These documents showed not only that Mrs. Randolph had been fully

apprised of the significant risks associated with the surgery, but also that she understood and willingly chose to proceed with the surgery knowing the possible outcomes. Certainly, Dr. Cowen and everyone else involved would have preferred a very different outcome. This case illustrates the importance of providing and documenting thorough informed consent, especially in the event of a bad outcome.

[1] The names of all involved parties have been changed.

Don’t Take the Bait in 2021

By Brian Johnson

2020 was a difficult year, unprecedented in many ways. As organizations across all industries scrambled to implement work-from-home strategies, healthcare organizations faced the COVID-19 pandemic head on. Hospitals and medical practices focused on caring for patients, but sadly cybercriminals pounced on the opportunity to attack. Among all industries, healthcare saw one of the largest increases with a 42% rise in hacking incidents[1]. IBM reported, in the X-Force Threat Intelligence Index 2021, that across all industries, phishing emails provided the initial entry point 33% of the time.[2] Based on its ease of use and high success rate, phishing is a longtime favorite of cybercriminals who are financially motivated, attacking those who they perceive as most likely to pay a ransom. Knowing that healthcare facilities rely on their information systems to treat patients and that any down time could negatively impact patient care, cyber criminals ramped up their ransomware attacks hoping for a big payday during the pandemic. Given this trend, it is important to understand phishing emails and the threat they impose on healthcare. This article will break down the anatomy of a phish, discuss common traits, identify the red flags and methods to identify a phish, and discuss defense and mitigation of phishing attacks.

In its simplest form, a phish is any attack that is delivered via email. The objective of the attack will vary, but the most common include ransomware, credential theft, fraud, and theft of intellectual property. For you to be duped, the cybercriminals need to develop a relevant and realistic email to pique your interest. Phishing emails are as much psychological as they are technical in nature. Security professionals use the term “social engineering” to describe the tactics used by phishing. These tactics rely on your human nature and social tendencies, tricking you into divulging sensitive information, clicking malicious links, downloading malware, and unknowingly enabling fraud.

Phishing emails impersonate brands, companies, people, and processes you trust. Next, they play on emotional triggers that manipulate your social tendencies that include authority, urgency, fear, duty, and a desire to be helpful. For example, cybercriminals often impersonate a CEO, CFO, or other important figure in your organization. For some, a rightly worded email from the “CEO” will induce several emotional triggers.

To help identify a phish, examine the **To** and **From** addresses of an email. Sometimes the email is not even addressed to you, other times you might be included in a long list of recipients that have no relation. Examining the **From** address can help uncover impersonation attempts. For example, you probably know your CEO’s email address because it follows a common naming convention particular to your company. Emails that come from any other addresses pretending to be your CEO, such as CEOname@gmail.com, are a phish.

Misspellings, grammatical errors, and spelling variations are other phish red flags. The cybercriminals behind phishing emails are often operating in a foreign country where English is not the primary language, and this will often come through in the message. Spelling variations such as using an S instead of Z are also clues about the person behind the email.

Phishing emails often contain malicious hyperlinks and attachments. Hyperlinks can lead to fake login pages where cybercriminals harvest your username and password, or potentially lead to a website that downloads malware, such as a backdoor or ransomware, to your computer. Attachments can also contain malware designed to compromise your computer. It is very easy for a cybercriminal to create a hyperlink that displays one address but goes to another. Hovering the cursor over a hyperlink will always show the true destination address. Look for identity and brand mismatches. For example, if an email says, “Elizabeth has shared a file with you,” and it is branded with a Dropbox logo with a hyperlink displaying www.dropbox.com, when hovering over the hyperlink, it will display a Dropbox address. Conversely, a phishing link will display and unrelated address with no resemblance to Dropbox.

When examining an email, you want to review all the red flags and establish an overall context for the message. Knowbe4 provides a convenient one-page printout that shows all the red flags.[3] When looking at context, ask yourself the following questions: Do I know this person? Is the email address correct? Does the tone of the message make sense? Where do the hyperlinks go? Does the attachment align with the subject of the message? If something feels wrong, follow your gut, and do a little more investigating. Never reply to the email because you might be talking to the cybercriminal directly. Often, someone replies to a compromised email account asking if the attachment is legit, and the cybercriminal kindly replies, “yes.” The best option is to call the individual using a number you have on file, not a number contained in the message.

Now that you are familiar with the composition of a phish and the tactics used by cybercriminals, it is time to develop a plan to mitigate and defend against phishing attacks. First, bring awareness to your team. Let them know what phishing is and that the organization is a target. Next, educate your employees on the red flags and how to recognize phishing emails. The best way to recognize a phish is to experience them firsthand, but in a safe environment. Knowbe4 has an image library comprised of real phishing emails.[4] Look at their examples and see if you can recognize the red flags. Many organizations test their employees using a paid solution that sends safe phishing emails and tracks the results. Paying for a solution might not appeal to you, but most solutions offer a free test or trial period. Lastly, encourage your employees to report suspicious emails. Many email solutions now have built-in features to report suspicious emails. If your email solutions do not offer a reporting feature, encourage your employees to ask for help when an email does not feel right. This could be forwarding it to your information technology department or another employee for a second opinion.

Phishing continues to be a favorite attack vector for cybercriminals and is predicted to

increase over the next several years. Assess your current situation and determine your organization's ability to detect and combat phishing emails. Do not delay, start implementation of awareness training to avoid becoming the next attack statistic. SVMIC members have access to educational content that covers phishing and other cybersecurity topics at **vantage.svmic.com**.

[1] HIPAA Journal, https://www.hipaajournal.com/2020-saw-major-increase-in-healthcare-hacking-incidents-and-insider-breaches

[2] IBM X-Force Threat Intelligence Index 2021, https://www.ibm.com/security/data-breach/threat-intelligence

[3] KnowBe4 Red Flags Printout, https://www.knowbe4.com/hubfs/Social-Engineering-Red-Flags.pdf

[4] KnowBe4 Phishing Examples, https://www.knowbe4.com/covid-gallery-phishing-examples

Open Notes Mandate Starts Now

By Elizabeth Woodcock, MBA, FACMPE, CPC

In May 2020, the Office of the National Coordinator for Health Information Technology (ONC) published the *21st Century Cures Act: Interoperability, Information Blocking, and the ONC Health IT Certification Program Final Rule*, which is designed to provide patients and providers secure access to health information. This implementation ruling follows the 2016 passage of the law titled – "21st Century Cures Act." The law – and subsequent ruling about its application -- contained many terms, but one key provision – electronic health information (EHI) blocking – was scheduled to launch last fall. With only days until the new standards went into effect, the US Department of Health and Human Services (HHS) extended the mandate to April 5, 2021, citing challenges related to COVID.

That day has come, and it's time to gear up for compliance with the new rules.

The so-called "open notes" mandate dictates that physicians must be able to make eight types of clinical notes data available to patients upon request (see SIDEBAR). Clinical notes are defined as "Composed of both structured (i.e., obtained via pick-list and/or check the box) and unstructured (free text) data. A clinical note may include the history, Review

of Systems (ROS), physical data, assessment, diagnosis, plan of care and evaluation of plan, patient teaching and other relevant data points." Clinical notes are one of 16 data classes in the United States Core Data for Interoperability (USCDI) Version One. (See https://www.healthit.gov/isa/united-states-core-data-interoperability-uscdi.) The USCDI list identifies the data elements that must be incorporated in the response to a patient's request to use, access, or exchange the information. If the data elements were not captured, they do not have to be reported.

The government's latest efforts build upon the requirement to allow access to patient records mandated under the 2000 HIPAA Privacy Rule. HIPAA established a patient's right to access, inspect and obtain a copy of their health records. The government subsequently passed the 2009 HITECH Act that launched the EHR Incentive Program to encourage adoption. Further, the Act directed HHS to adopt certification standards for electronic health record systems, including methods for access. For participating physicians, the program's "meaningful use" criteria necessitated granting records' access to patients.

Although physicians could purchase portals to comply with the program's meaningful use measures, EHR vendors were not required to extend the functionality to support data exchange or interoperability. Indeed, the blocking of the capability was so ubiquitous that "gag clauses" were often integrated in EHR system contracts. So, patients could garner access to these closed ecosystems but little more. Vendors were not the only ones blocking information, however. The ruling names three categories of "actors" subject to the new rules: certified health IT developers, health information exchanges and health information networks (HIEs/HINs), and health care providers.

Under the ONC's new ruling, which was opposed by EHR system vendors, "actors" are prohibited from information blocking practices that have become the norm; instead, systems, networks and providers must open their doors to clinical data sharing.

To comply, data exchange must be performed on a standard information highway – HL7 FHIR (Release 4) – and transacted at no cost to the patient. Because this data standard supports smartphone apps, many experts expect a proliferation of companies to focus on this new access point.

Of course, this translates into patients' ability to access their records, including your clinical notes. The new rule focuses on your response to patients' requests, not broad availability. For example, HHS professes:

> *While the information blocking regulations do not require actors [to include health care providers] to proactively make electronic health information (EHI) available, once a request to access, exchange or use EHI is made, actors must timely respond to the request (for example, from a patient for their test results). Delays or other unnecessary impediments could implicate the information blocking provisions. In practice, this could mean a patient would be able to access EHI such as test results in parallel to the availability of the test results to the ordering clinician.*

For more information, see: https://www.healthit.gov/curesrule/resources/information-blocking-faqs.

The government has outlined exceptions, including prevention of risk or harm to patients, privacy and security, and infeasibility. However, "routinely time-delaying" data availability does not fall under the exception, according to the Final Rule.

While it may be frustrating to learn about another complex rule with which to comply, the ruling will benefit some physicians. Vendors can no longer charge excessive fees for restricting access to patients' data, for example, a significant challenge that often occurs when physician practices decide to switch electronic health record (EHR) systems. Further, vendors are prohibited from implementing tactics that delay access to data. Experts surmise that the ruling will also extend to prohibit the all-too-common practice of vendors requiring expensive upgrades to add on patient-facing communication platforms such as patient portals. In sum, there may be corollary benefits to physicians.

The government's new stance on access to data is not going away. The ruling is consistent with the government's overall health care technology strategic plan, just released in the fall. (https://www.healthit.gov/topic/2020-2025-federal-health-it-strategic-plan) Accessibility of health information is a key principle of the new plan; it may be an opportune time to determine if and how the "open notes" mandate will impact your practice.

Required Patient Data Available for Clinical Notes:

- Consultation note
- Discharge summary note
- History and physical
- Imaging narrative
- Laboratory report narrative
- Pathology report narrative
- Procedure note
- Progress note

Risk Matters: Informed Consent

By Jeffrey A. Woods, JD

Last month, we discussed the importance of the informed consent discussion to prevent malpractice claims. As a follow-up, remember that it is the discussion that takes place between the provider and the patient (or patient's legal representative) that constitutes the basis for the consent to be "informed." The consent form that is signed by the patient or representative is merely evidence memorializing that the discussion took place, and the patient/representative understood the information discussed. Accordingly, be sure the details of all discussions relative to obtaining informed consent are documented in the medical record. Relying solely on boilerplate, fill-in-the-blank hospital or generic consent forms that are not procedure-specific will most likely not capture all of the details of the conversation.

Getting Paid for Vaccine Administration

By Elizabeth Woodcock, MBA, FACMPE, CPC

The Centers for Medicare & Medicaid Services more than doubled the reimbursement for COVID vaccines as of March 15, 2021; the payment rate is now approximately $40 per dose. For up-to-date information on payment rates for Medicare, see COVID-19 Vaccines and Monoclonal Antibodies | CMS . If your practice is offering COVID vaccines, you can bill for the shot administration. The process is seamless, but let's review some tips to ensure that you are getting paid for your hard work:

Submit a single claim per patient – or a roster bill to Medicare for five or more patients. For more information about roster billing for the vaccine, see https://www.cms.gov/medicare/covid-19/medicare-billing-covid-19-vaccine-shot-administration. For more information about billing for the vaccine for non-Medicare patients, query the payer's website.

If the vaccine was free to you, charge only the administration.

For Medicare Advantage patients, submit your claims to your Medicare contractor as Original Medicare under Part B coverage using the patient's Medicare Beneficiary Identifier (MBI). If the patient doesn't have the MBI, gather the patient's name, birthdate, and social security number; use this handy guide to query for the MBI. https://www.cms.gov/Medicare/New-Medicare-Card/Providers/MACs-Provider-Portals-by-State.pdf

To get paid for uninsured patients at the Medicare rate; submit the claim for the vaccine administration to: https://www.hrsa.gov/CovidUninsuredClaim.

If you're having issues with scheduling in your practice management system, download free vaccine scheduling software here: https://www.blockitnow.com/covid.
