# When “Country Tough” Isn’t Tough Enough

**By Judy King Reneau, JD, BSN**

When Dr. Fabian Starr[1] arrived for work that day in summer 2014, he was asked to examine Mr. Chet Stetson, a 58-year-old male who presented to the office to discuss liposuction. Dr. Starr, a plastic surgeon, worked at Fabulous New You, a free-standing office that advertises esthetic treatments and cosmetic surgical procedures that can be done under local anesthesia. Mr. Stetson, a widower who had recently remarried, explained to Dr. Starr that he had always been overweight and in high school had weighed as much as 320 lbs. He still “loved to eat” but had recently lost a significant amount of weight. Despite the weight loss, he was still unhappy with the way he looked, especially his big belly and “love handles.” He had heard the catchy advertisements by Fabulous New You and was interested in a particular liposuction procedure that promised to give him a thinner, more youthful shape. Dr. Starr examined Mr. Stetson and determined that the problem was not excess abdominal fat, but rather loose skin left behind after his weight loss. Dr. Starr counseled *against* having the liposuction procedure, but instead recommended a different surgery that would remove the loose skin around his middle.

This other procedure, though more invasive, would provide the thinner silhouette Mr. Stetson was seeking.

Dr. Starr remembers discussing the details of the more invasive procedure with Mr. Stetson, including the necessity of arranging for a driver to take him home afterwards. Mr. Stetson signed a form which indicated that if he took sedatives, he absolutely must have a driver. Dr. Starr recalls that Mr. Stetson assured him that he was "country tough" and would not need sedatives, and therefore, he could drive himself home. The visit ended with the understanding that Dr. Starr would use only local anesthetics, and Mr. Stetson would not be sedated in any way. Based on this understanding, Dr. Starr decided to move forward with the surgery. Later, with the benefit of hindsight, Dr. Starr realized that he should not have agreed to perform the procedure with the expectation that only local anesthetics would be used. It was against his medical judgment and an assurance he should not have made.

On the morning of the scheduled procedure, Mr. Stetson arrived without a driver. He confirmed to the staff that he intended to decline any sedative-like medication during the surgery. In fact, he refused the pre-operative Valium that was offered to him. The surgery went forward starting at 9:15 a.m. utilizing tumescent solution containing Lidocaine and Epinephrine.

Approximately an hour into the surgery, Mr. Stetson experienced some pain and anxiety. In response to this, Dr. Starr ordered that a dose of Versed syrup be given. It is alleged that a second dose of Versed syrup may have been given during the surgery but was not charted. When the surgery was over around noon, the patient was moved to the holding area to recover. The staff arranged to have lunch delivered, and he ate his lunch without incident. During this time, it was noted that Mr. Stetson emphasized to the staff that he needed to leave the office right away to beat the traffic he would encounter on the way to his home in a rural part of the state 90 miles away.

Dr. Starr looked in on Mr. Stetson a couple times while he was eating his lunch. He advised him that he should not drive so soon after surgery. The doctor offered to call him a cab, have a staff person drive him home, or make other arrangements to see that he got safely home. Mr. Stetson declined all these offers, commenting that he was "tough enough" to drive. The staff noted a short time later that Mr. Stetson had left the facility when no one was watching. No discharge order was written, and no AMA (Against Medical Advice) form was completed. It would have been helpful if Mr. Stetson had been asked to sign an AMA form, acknowledging his failure to follow medical advice and the risks of such behavior, at the point when he declined the offers for assistance in getting home safely.

During his drive back home, shortly after 3:00 p.m., Mr. Stetson recalled that he suffered a sharp pain in his abdomen, causing him to black out. His vehicle rolled over and wrecked, causing multiple orthopedic and spine injuries. His injuries included multiple acute bilateral rib fractures, acute dehisced incision, comminuted acute C2 fracture, acute right shoulder dislocation with anterior glenoid fracture, acute C1 ring fracture, acute right-sided

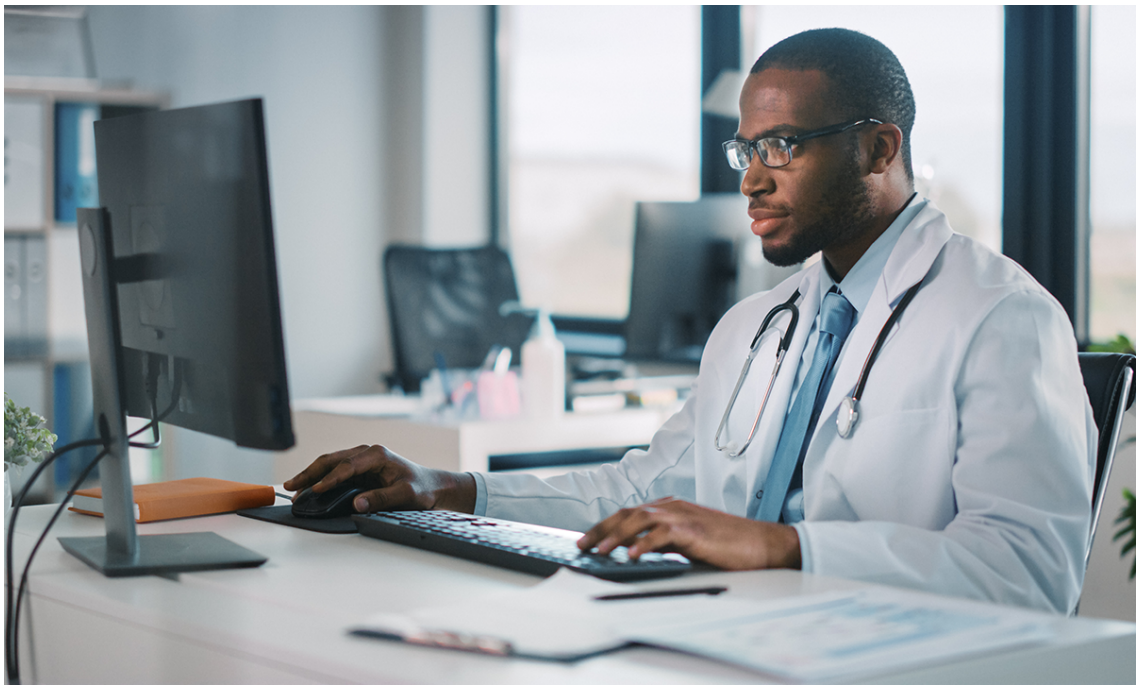
pneumothorax, right vertebral artery dissection, and transverse process fractures of L2 and L5. He was transported by Life Flight to Benevolent Hospital and admitted into the intensive care unit. After approximately one week of treatment, Mr. Stetson was discharged to a rehabilitation hospital where he received therapy for approximately two weeks. He was then discharged in the care of his wife.

Mr. Stetson sought representation from a well-known plaintiff's attorney. Suit was filed demanding a large amount of compensatory and punitive damages (for alleged grossly negligent and reckless medical care). Dr. Starr, in kind, was represented by experienced defense counsel. After three and a half years the case went to trial, and the jury found in Mr. Stetson's favor. A large compensatory damage award was handed down, and the jury determined that punitive damages were warranted with the amount to be determined at a separate hearing. However, before the punitive damages phase of the trial, a confidential settlement was reached that resolved the case.

It is well known that it is foolhardy to drive yourself home after surgery. This is true even if the patient sees himself as "country tough." In this scenario, the practice would have been wise to cancel the procedure when they realized that the patient did not bring someone to drive him home. The surgery should have been rescheduled for a time when he could arrange for a driver to be with him. While they could not control the fact that the patient left without their knowledge, they could control whether the procedure went forward at all that day.

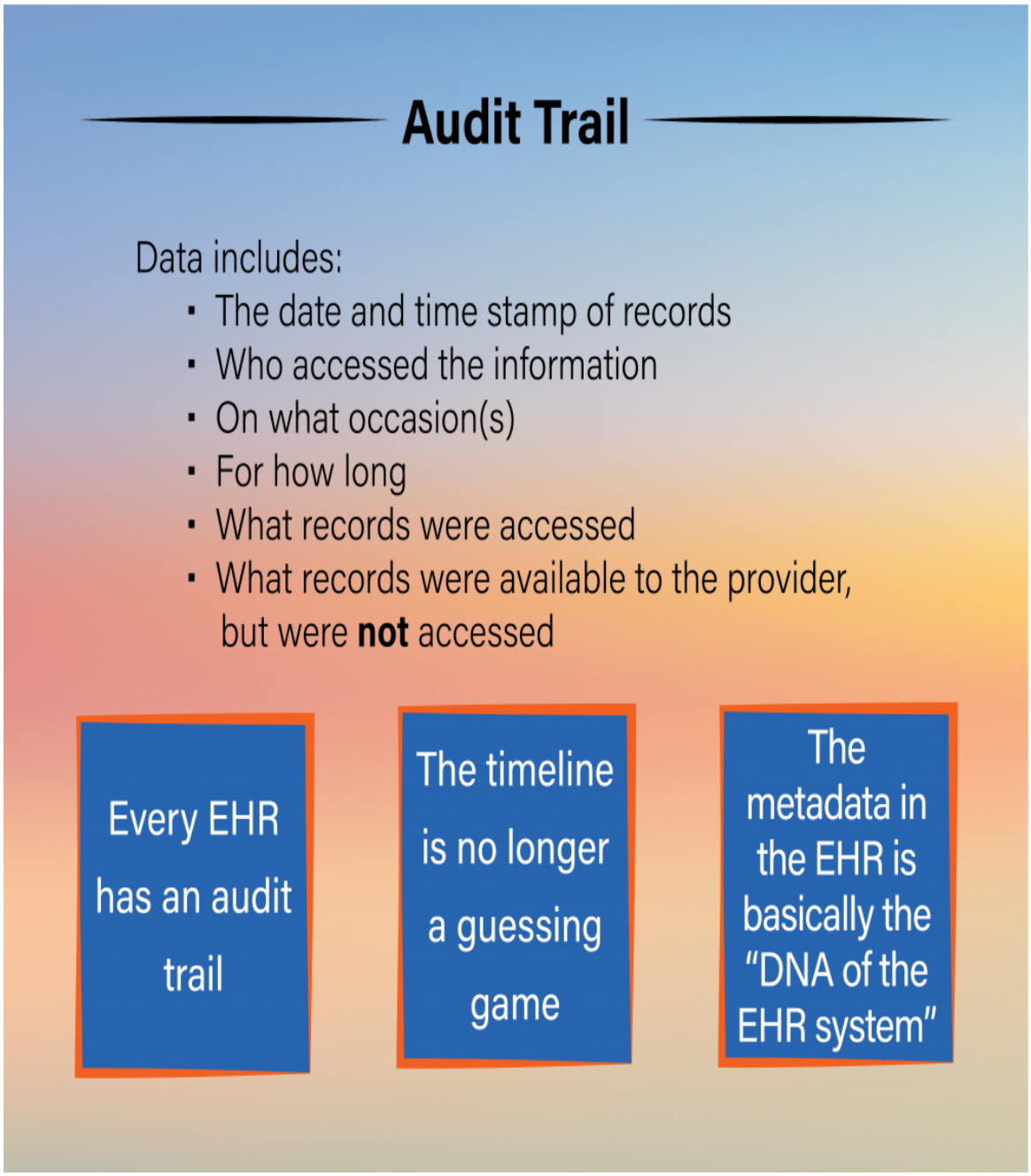
[1] Names have been changed.

# Risk Matters: EHR Tips



**By Jeffrey A. Woods, JD**

Every EHR system has an audit trail. The timeline is no longer a guessing game. Gone are the days of using handwriting experts to try to determine when and by whom an entry was made in a patient's chart. Forensic IT experts can now review the metadata contained within the EHR to determine everything that occurred in the electronic chart, outlined in the graphic below.




Because every keystroke in an EHR is recorded with a time and date stamp, amendments, supplementation, corrections, and addendums should not be made after an adverse event or the assertion of a claim or filing of lawsuit. Doing so will likely be viewed suspiciously and as self-serving. If a correction to the EHR is needed for continuity of care purposes, and there is no claim or lawsuit pending or threatened, these corrections should be made

in the same manner as with paper charts:

- Clearly identifying that it is a correction or supplementation
- Articulating the reason necessitating the change
- Specifying the date and initials or e-signature of the person who made the change

If a claim or lawsuit is pending/threatened, or possible, contact an SVMIC Claims Attorney or your defense attorney to discuss whether correcting the record is advisable at that time.

Additionally, EHR documentation should be performed contemporaneous with the event or as close thereto as possible. The audit trail will reveal the time differential between the event taking place and the recording of the event. If a significant amount of time is allowed to elapse, the accuracy of the provider's documentation may be called into question.

Finally, keep in mind that if a provider shares his or her login information with a staff member or permits someone else to sign an EHR electronically using e-signature, it will appear from the audit trail that it was the provider who accessed the EHR or signed the record. This could be problematic in a claim where the record is in question, and it could also be a violation of third-party payer contracts.

# Security Risk Analysis: Step One of an Effective Cybersecurity Program

**By Loretta Verbeck, MS, FACMPE, CHC**

Cybersecurity is a topic that physicians and their staff cannot ignore. Ransomware, data breaches, distributed denial of service (DDoS) attacks, and email fraud are just a few of the cybersecurity issues that can cause financial and reputational damage to any organization. In healthcare, the impact of a cyber-attack goes beyond financial and reputational damage. It can also disrupt the ability to provide patient care. This is why healthcare organizations must implement an effective cybersecurity program.

The HIPAA Security Rule requires covered entities, which includes nearly all healthcare organizations, to protect the confidentiality, integrity, and availability of all electronic protected health information (ePHI) that is created, received, maintained, or transmitted by the entity. The Rule includes administrative, physical, and technical standards and implementation specifications that are either required or addressable. At a minimum, HIPAA covered entities must conduct a risk analysis by assessing their current risks, security measures already in place, and any remaining gaps that need to be addressed.

The first standard under administrative safeguards is the security management process which includes risk analysis and risk management. These two implementation specifications are required by the Security Rule and, if conducted and implemented appropriately, can reduce the risk of a successful cyber-attack. Unfortunately, based on findings from the 2016-2017 HIPAA Audits Industry Report, released in December 2020, "most covered entities and business associates failed to implement the HIPAA Security Rule requirements for risk analysis and risk management." Lack of an accurate and thorough risk analysis is also one of the most cited deficiencies in enforcement action taken by the Department of Health and Human Services (HHS).

The Security Rule does not require a specific risk analysis methodology, but guidance has been developed by the Centers for Medicare and Medicaid Services (CMS) in large part based on the National Institute of Standards and Technology (NIST) 800 Series of Special Publications (SP), specifically, SP 800-30 - Risk Management Guide for Information Technology Systems. Depending on the size of the practice, the complexity of systems containing ePHI, and the technical expertise of the workforce, it may be necessary to outsource the risk analysis process. There are a number of third-party vendors that can assist covered entities with this process. However, even if the risk analysis is performed by a third-party, the covered entity is ultimately responsible for ensuring that it is accurate and thorough.

The following steps are summarized from the CMS guidance to help medical practices conduct their own internal risk analysis or determine if an outsourced risk analysis is sufficient to meet the Security Rule criteria.

1. **Identify the Scope & Gather Data**

   The scope of an accurate and thorough risk analysis must include **all** ePHI that is created, received, maintained, or transmitted. This means thinking beyond the electronic health record and billing system to develop a proper ePHI inventory. There are many places and systems that are overlooked by practices when conducting a risk analysis. That is why it is important to include the entire organization in the process. This can be accomplished by interviewing workforce members, using surveys to inquire how ePHI is being shared internally and externally, and identifying systems and devices used to create, send, or receive ePHI.

Some examples of systems that could be left out of a risk analysis are telephone systems using voice over internet protocol (VoIP), email applications, mobile devices used by workforce members, portable storage devices, and cloud storage. The scope and method of gathering data must be documented regardless of the size of the organization. If the organization is large, with several departments or facilities, the scope must be enterprise-wide.

2. **Identify Potential Threats & Vulnerabilities**

   Once an ePHI inventory has been developed, the next step is to identify the potential threats and vulnerabilities to the confidentiality, integrity, and availability of that ePHI. A threat is the potential for a specific vulnerability to be triggered or exploited. Threats can be natural (floods, earthquakes, tornados), human (intentional or unintentional actions by people), or environmental (power failure, pollution, chemicals). A vulnerability is a flaw or weakness in systems or processes that could result in a security breach or a violation of a security policy if triggered or exploited. Threats and vulnerabilities must be documented.

3. **Assess Current Security Measures**

   Even when a risk analysis is being conducted for the first time, it is likely that the practice has some security measures already in place. In this step, current security measures should be documented. Security measures can be technical (automatic logoff, encryption) or non-technical (policies and procedures). Security measures will vary with the size of the organization. The goal of this step in the risk analysis process is to minimize or eliminate risks to ePHI.

4. **Determining Level of Risk**

   Using the ePHI inventory, along with identified threats and vulnerabilities, and security measures already in place, the practice can now determine the level of risk to ePHI. The level of risk is determined by the threat's likelihood of occurrence and the impact on ePHI should the threat occur. The purpose of determining the risk level of each threat is to prioritize efforts to reduce risks to a reasonable level.

Each threat should be given a likelihood of occurrence. This can be as simple as rating each threat as low, medium, or high. Next, determine the impact to the confidentiality, integrity, or availability of ePHI if the threat does occur. For example, if the practice is in a flood zone, the likelihood that a flood (threat) could occur is high. The impact on ePHI if the practice does not have an offsite backup (vulnerability/lack of security measure) will also be high. The combination of high likelihood and high impact results in high risk. On the other hand, if the practice has an offsite backup that can be restored if systems storing ePHI are damaged in a flood, the impact to ePHI would be low. The combination of high likelihood and low impact results in a low level of risk.

5. **Identify Security Measures and Finalize Documentation**

   Now that risk levels have been assigned, it is time to determine the actions that must take place to reduce risks to reasonable and appropriate levels. When choosing safeguards, practices should consider the regulatory requirements of the Security Rule's standards and implementation specifications and any existing security policies and procedures. Once safeguards have been identified, documentation of the results can be finalized.

The Security Rule does not require a specific format for documentation, but it should be done in a way that is useful for the practice. For example, a spreadsheet that lists the risk analysis process, results of each step, and initial identification of security measures would serve the purpose of documenting the risk analysis and provide a starting point for the risk management process.

Following the Security Rule requirement to conduct a risk analysis is the first step of an effective cybersecurity program because it puts the spotlight on areas that pose the most significant risks to your practice. Once the risks are identified, action can be taken to reduce those risks to a reasonable and appropriate level through the risk management process.

Several resources are available to assist healthcare organizations with the risk analysis process. HHS provides guidance and tools that include a series of papers designed to provide insight into the Security Rule requirements, guidance on specific risks such as remote use, mobile devices, and ransomware, and a link to the Security Risk Assessment (SRA) Tool. This tool provides healthcare providers with a step-by-step guide through the risk analysis process.

If you have questions about cybersecurity or access to the resources available exclusively to SVMIC policyholders, call 800-342-2239 or email ContactSVMIC@svmic.com.

Individuals in your organization such as your administrator, privacy or security officer, or information technology professional may benefit from this article and the other available resources to SVMIC policyholders and staff through their Vantage® account. If someone in

your organization needs a Vantage account, he/she can sign up here.

**If you experience a cybersecurity incident**, contact SVMIC as soon as possible by calling 800-342-2239 and ask to speak to the Claims department.

# Personnel Management During a Labor Shortage

**By Elizabeth Woodcock, MBA, FACMPE, CPC**

Labor shortages are creating havoc for many businesses in the United States, and medical practices are not immune. Although there may be some relief when the federal government's bonus checks end this fall, the problem will not come to a screeching halt. Indeed, experts believe that the growth of the ambulatory sector – 22,000 of the 23,000 jobs added in health care in May alone -- will propel even more challenges. Moreover, the workload burden has been unrelenting, causing some employees to migrate out of healthcare altogether to other, less stressful – and often higher-paying jobs. Regardless of how you slice it, the labor shortage is a reality.

Although you could rely on luck to get you through this challenge, consider taking proactive steps to mitigate the risk of an inadequate labor force:

***Show Your Appreciation***. There are no words for the turmoil you and your practice have endured over the past 18 months, but there is also no doubt that the pandemic touched

the personal lives of *everyone* on your team. Show support for your team with a gesture like bringing a light breakfast to snack on, accompanied by a sign that reads: “thanks for all you do;” give everyone on your team a handwritten note: “I appreciate you, and everything you do for our patients.” Consider adding a gift card for a major retailer or gas station -- or offer a gift certificate for a movie theater with a bag of popcorn. Encourage your colleagues to take action as well; make sure your team knows they are appreciated.

***Engage with Your Team***. Make a list of all your employees and commit to spending at least 10 minutes with each of them in the next 30 to 60 days. Ask each member of your team: “How are you?” (Yes, just this simple question demonstrates your engagement and can stand out during this tumultuous time.) Follow it with: “What can we do to make you be more successful at your job?” You will be amazed at the suggestions – and your team will appreciate being asked.

***Review Compensation***. The labor shortage is not the only influence on staff; as more health care organizations embrace a virtual delivery platform, there is a significant shift in the employment market. Employees can work for anyone – anywhere in the world. Your employees may be bombarded by offers from your local hospital, community health center, or nursing home, but they may also be receiving offers from organizations based in California, Alaska, or other far-flung places. It is an opportune time to make sure that you’re paying competitively. As many employees may focus solely on the hourly rate, it also pays to document the benefits you offer – and even attach a dollar value. Consider listing your full compensation package, to include health insurance, disability benefits, leave, and so forth. It might also be time to add a benefit such as childcare or tuition reimbursement, a payroll-deduction emergency savings account, and an extra health day (or two) for mental health or to make up preventive care skipped during the pandemic.

***Proactively Recruit***. Do not wait until a position opens if you find great talent. Turnover is bound to happen, and it’s a much better investment to pay an extra few months’ salary – rather than wait for someone to resign and scramble. Consider looking in unexpected places – maybe you’ve had an interaction in a retail setting with someone who went above and beyond from a customer service perspective; or recruit back a former employee who decided to stay at home, compelling him or her with a flexible, part-time schedule. Part-timers can be a huge win for your practice, as there are often days of the week that demand higher resources (e.g., Mondays) that might be perfect for a part-timer – and your virtual business, if applicable, could accommodate someone working from home.

Attrition does not have to be negative, but it certainly needs to be managed. Conduct exit interviews to learn from departing staff members what could have been done to improve the work environment. Most importantly, set a plan in motion now to avoid getting shocked by the resignations that may be coming across your desk in the near future.

# Breaking News: COVID-19 Public Health Emergency Extended for 90 Days


**By Elizabeth Woodcock, MBA, FACMPE, CPC**

On July 19, 2021, Xavier Becerra renewed the Public Health Emergency for 90 days starting July 20. The move by the Secretary of Health & Human Services signals the federal government's intention to extend regulatory relaxations associated with telemedicine delivery and reimbursement into the fall. The Biden administration has stated that the PHE will not expire before the end of the year and that a minimum of 60 days' notice will be given prior to its conclusion. While the renewal clears the deck for Medicare delivery and reimbursement for another 90 days, several key payers have signaled a long-term commitment to telemedicine. Cigna, for example, announced that payment for telemedicine will be at the same rate as an in-person visit. However, in reading the fine print from Cigna, United, Aetna, and other payers, there are statements about payment for "certain" services, only if the plan offers coverage, and deferring to state law. In other

words, telemedicine is here to stay, but don't be surprised about the checkerboard of payment policies that is under construction.

---

*The contents of The Sentinel are intended for educational/informational purposes only and do not constitute legal advice. Policyholders are urged to consult with their personal attorney for legal advice, as specific legal requirements may vary from state to state and/or change over time.*