Back It Up - The Importance of Proper System Backups

By Brian Johnson

We are a society that greatly depends on technology. Regardless of industry, all organizations rely on computers to conduct all manner of business operations. Additionally, your medical practice depends on computers and software to provide medical care to patients. Before computers, these processes were once conducted with pen, paper, charts and filing systems. Now everything is digital, and routine processes from scheduling and billing to medical record documentation are accomplished on computers. Without access to these systems, your practice will certainly be hampered. At best, you might be able to implement a temporary strategy using paper and manual processes to get by until your systems are restored. At worst, you will be unable to perform the most basic of patient care and business operations. For this reason, it's paramount that you ensure the availability of the systems that you depend on, a goal that can be obtained with a carefully planned backup strategy.

This article is focused on availability of systems and data. Availability is defined by

Merriam-Webster as "present or ready for immediate use." In the context of a computing system operated by a healthcare organization subject to HIPAA, availability is defined as having data or information that is “accessible and useable upon demand.”[1] In relation to your medical practice, it ensures that you have the information you need to care for your patients and perform business functions. Backups are your safety net when things go wrong. Computers fail for many reasons that range from technical failure and natural disasters to human error and criminal activity. Natural disasters such as fire, floods, hurricanes, and tornados can damage buildings and destroy computers. Electronic components often fail, especially hard drives. Human error can accidentally delete or corrupt data. We trust our employees, and no one likes to consider the possibility, but disgruntled employees have been known to sabotage systems. Even the theft of a server or laptop can disconnect you from the information you need to run your practice. Finally, cybercriminals are using ransomware to lock practices out of their data. Following any of these events, backups help facilitate availability and are used to recover systems and quickly restore data, bringing your system to a usable state.

Backups are duplicate copies of the critical data that run your practice and are a core component of any Business Continuity plan - your precompiled plan of action to ensure the business runs in the event of a disaster. If you don’t have a Business Continuity plan, please read on, as establishing your backup strategy is a good starting point. Your backup plan is essentially a ‘what, how, and where’ strategy to safeguard your data. When devising your backup plan, you first want to identify **what** systems and data you need to backup. These are the systems that you depend on to run your practice from both a patient care and a business aspect. Next decide **how** to back up each data set. Your documents and spreadsheets will require a different approach from your electronic health record (EHR) system. Even a cloud based EHR will require different backup strategies than an on-premises EHR system. Always contact your vendor for guidance on the best method of backup. The next step is to determine **where** to store your data. This is comprised of both a media type (i.e., disk or tape) and physical location.

The 3-2-1 backup rule is a robust, time-tested example of a backup strategy that is easily adaptable to many data types and technologies. This method was originally described by Peter Krogh, a professional photographer looking to safeguard his digital photo library.[2] The 3-2-1 strategy calls for 3 copies of your data, stored on 2 independent mediums, with 1 being off-site. The **three** copies of data are comprised of the original dataset plus two backups. In a perfect world you would only need your original dataset. However, the reality of technological failures and natural disasters puts your data at risk. By keeping **two** backup copies on independent mediums, you are increasing the probability that one will be available in your time of need. Furthermore, by keeping **one** copy offsite you are further increasing that probability and dramatically lowering your risk. Consider a situation where you have two copies of your backup. One is stored securely onsite, and the other is stored offsite. If you have a system failure such as a failed hard drive, you can restore from your local copy; however, if your building is destroyed by fire, you will rely on the offsite copy. We all know the adage of not keeping all your eggs in one basket; the same applies here.

An additional consideration is how often to make backups. This is determined by the rate at which your data changes and how much data you are willing to lose. For some practices this is one day, for others it's one week. You will need to determine your acceptable threshold and set your backup schedule accordingly.

Previously in this document, we identified backups as part of a Business Continuity plan. As a medical practice, you are obligated to have a data backup and disaster recovery plan to comply with HIPAA rules on contingency planning.[3] The HIPAA Security Rule addresses Administrative Safeguards (§ 164.308(a)(7)) that require a backup strategy for systems that store electronic protected health information (ePHI).[4] Following the 3-2-1 backup strategy will put you on good course for HIPAA compliance; however, there are a few additional items you will want to ensure. HIPAA requires written procedures related to your backup and recovery plan, encrypting backup media, and implementation of testing procedures.

Bottom line: when your systems are unavailable, you severely inhibit your ability to care for your patients. It is simply good practice to maintain backups to ensure continued operations of your medical practice. Disaster strikes in unforeseeable events and requires a robust strategy to ensure recovery. Follow the 3-2-1 backup strategy to ensure multiple copies of your backups are stored in multiple locations. Health organizations are further obligated to meet HIPAA requirements as prescribed in the Security Rule administrative safeguards. HIPAA is focused on patient care and ensuring medical records are available. However, you also depend on your computing system and the data therein to run the business aspects of your medical practice. Ensure that you are including both in your backup strategy. Always work with your information technology provider and system vendors to implement the best backup strategy for your specific systems. And finally, don't forget to test your backups.

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.

[1] HIPAA Privacy Rule, 45 C.F.R. § 164.304.

[2] Krogh, Peter. The DAM Book, Digital Asset Management for Photographers, Second Edition, O'Reilly Media, 2008

[3] HIPAA Rules on Contingency Planning (hipaajournal.com)

[4] HIPAA Security Series #2 - Administrative Safeguards (hhs.gov)

Proposed Medicare Payment Rate Drops for 2022

By Elizabeth Woodcock, MBA, FACMPE, CPC

The federal government's proposal for the Medicare Physician Fee Schedule in 2022 features an alarming payment cut of 3.75%. This is a result of the conversion factor shifting from its current rate of $34.89 to a proposed $33.58 based on the budget neutrality required by law. This news was certainly not welcome, particularly in light of the many sacrifices made by you and your colleagues in the past 18 months. The agency making the announcement – the Centers for Medicare & Medicaid Services (CMS) – has few options, as the formula is prescribed by law. There is already a movement afoot to request Congressional intervention; the precedent was set in December 2020 when federal legislators stepped in with a $3 billion aid package for the current year. A similar response is the best hope to reverse the proposed cuts, a feeling that reminds us of the 17 times that Congress had to intervene in the 2000s. The Medicare Access to Care and CHIP Reauthorization Act (MACRA) of 2015 was supposed to save you from these dreaded last-minute interventions. A silver lining could be that Congress realizes that MACRA didn't do the trick – and considers starting from scratch again to (finally) solve the payment problem

that has been plaguing medical practices for more than two decades.

The remainder of the proposed rule featured news that could represent opportunity:

- many telemedicine services would be reimbursed through December 31, 2023, providing a time cushion for the government to perhaps make the regulatory relaxations permanent
- delaying the “value pathways” that were proposed for the Merit-based Incentive Payment System in 2021, thus reducing the administrative burden of having to learn a new component of the government’s program
- boosting reimbursement for Medical Nutrition Therapy (MNT) and related services as rendered by nutritionists and dieticians in parity with the rate of 85% of the physician fee schedule enjoyed by other advanced practice providers, and extending the ability for any physician to refer for these services, not just the treating physician
- suspending the penalty for the Appropriate Use Criteria (AUC) program for another year

On the not-so-good-news front, the government confirmed that 2022 is the final year in which the “exceptional performance” bonuses for the Merit-based Incentive Payment System (MIPS) will apply. While touted to be a great financial opportunity, participating physicians who have attained perfect scores in the MIPS program have yet to even receive 2%. Even this paltry bonus, however, will no longer apply after 2022. Because the program runs in two-year cycles – what you are doing now influences your 2023 reimbursement -- this means that your participation this year (2021) is really just about avoiding the 9% penalty imposed on non-participants. Further, the program now shifts to 30% of your score being derived from the “cost” category, which is based on the government’s analysis of your claims and, if attributed, the claims of the patients for whom you care.

The government also announced changes to the definition of a shared (split) visit, direct billing by physician assistants, and limitations regarding the reporting of critical care services. These and other proposals are included in the just-released, 1,747-page rule.

With all these changes, it may be an opportune time to review your 2020 performance report to determine how the government is assessing you and your practice. The government just released the reports. (See below for how to access your report.) If your report deviates from expectations, take action by asking for a targeted review. There’s no cost to do so; requests for appeals will be received through October 1, 2021 at 8 pm EST.

How To Obtain Your 2020 Quality Payment Program Report:

- Sign in to **qpp.cms.gov**
- Select “Performance Feedback” from the home page
- Select your organization (Practice, APM Entity, Virtual Group); note that practice

representatives can access both individual and group feedback through the practice organization.
- You must have a HARP account to view your performance. To register for an account, see the “Register for a HARP Account and Connect to an Organization” documents in the **QPP Access User Guide**

Risk Matters: EHR Duplication

By Jeffrey A. Woods, JD

EHR Duplication: Native Form vs. Printed Copy

Physicians' offices receive a large number of requests for copies of medical records from patients, their representatives, insurance carriers, attorneys, and other providers. Prior to the advent of electronic health records, someone in the office would respond to such requests by physically removing the pages from the medical records folder and placing them on a photocopier. Once the copies had been made, the duplicate set would be forwarded to the party making the request. Assuming that each page was copied (front and back), there was little room for error. In other words, the copies that the requesting party received were an exact duplicate of the physician's records. That is sometimes not the case with today's EHR systems.

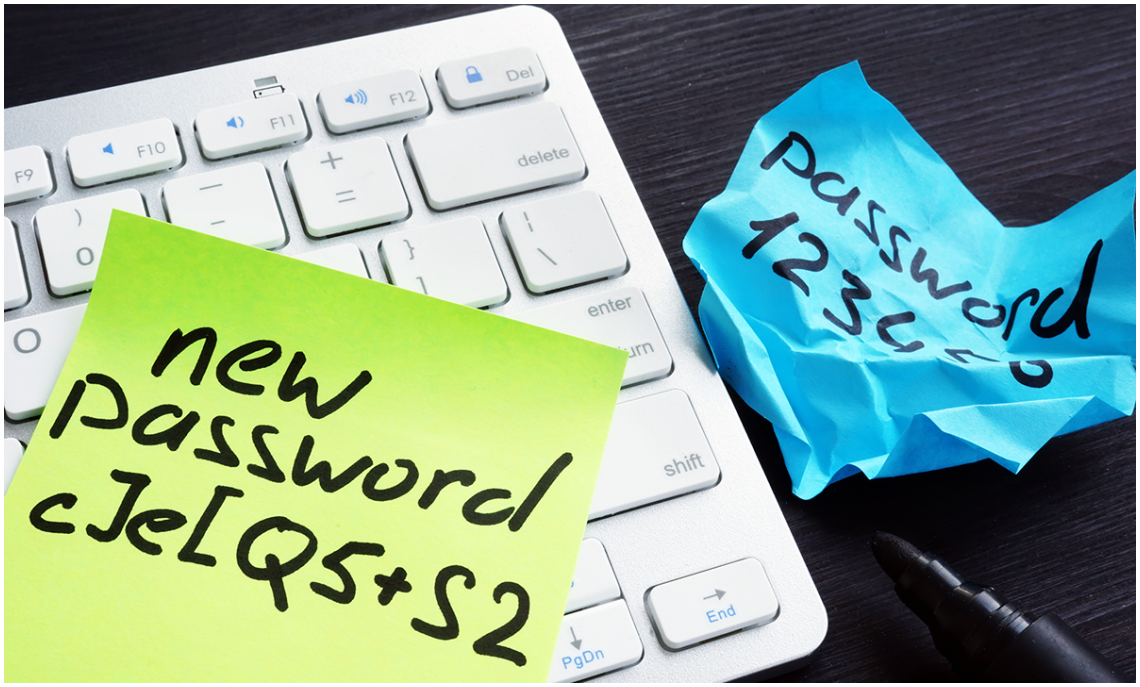
Physicians and other healthcare providers make entries in the EHR based upon the information they are visualizing on the screen in front of them. "Physicians Notes," "Nurses Notes," etc. are in certain familiar locations depending on the system and format being used. Some healthcare providers assume that if a hard copy of the electronic

medical records was printed, the image on the paper would appear the same way it does on the screen. However, this is not necessarily true in all cases. Some EHRs omit large portions of data when a hard copy is printed.

Because a printout of the EHR can sometimes differ significantly from the image that is on the monitor screen being viewed by the provider (native format), this can create problems and cause a record to be suspect when a patient or his/her representative or attorney requests a hard copy printout of the medical record. Practitioners and staff should be familiar with what information is and **is not** printable from the EHR. If a patient, representative, or attorney requests copies of the EHR, the hard copy should be reviewed to ensure it is complete and any discrepancies noted prior to forwarding the information to the patient, representative, or attorney.

Members with concerns regarding providing copies of records to patients or their attorney are encouraged to contact the SVMIC Claims Department at ContactSVMIC@svmic.com or 800.342.2239.

Weak Password Allows Major Cyber Extortion



By Justin Joy, JD, CIPP

After arriving at the office on a Tuesday morning following a holiday weekend, a medical assistant at an ophthalmology practice* logged into her workstation to pull up the clinic schedule for the day. For an unknown reason, the assistant received an error message on her computer screen when she attempted to access the schedule. Around the same time, a physician was attempting to pull up a diagnostic test stored on the practice's picture archiving and communication system (PACS) server. Similar to the problem experienced by the medical assistant, the physician was also unable to access the imaging of her patient performed the Friday before the holiday weekend. Both the medical assistant and the physician contacted the practice's administrator about the unexplained problems they were experiencing with the group's system. The practice administrator then placed a call to the help desk at the group's third-party IT vendor about the two problems.

Upon receiving the report of the two problems, a technician employed by the vendor, a local IT managed service provider (MSP) firm, promptly accessed the practice's computer

system using a remote access tool. The technician attempted to access the server hosting the practice's data to troubleshoot the problem. In viewing the files contained on the server, the tech immediately noticed that all of the files had time stamps indicating that they had been changed within the past 72 hours and the filenames had been appended with text that did not appear to be correlated to the data. Upon further investigation, the MSP tech discovered a text file containing a note demanding a ransom payment be made in cryptocurrency of 5 bitcoin (which, at the time of the attack, was the equivalent of over $50,000) in order to regain access to the data. The note indicated the group had less than 36 hours remaining to pay the ransom or else the ransom would double. The note also indicated that if the ransom was not subsequently paid in 72 hours, the data would become permanently inaccessible.

The technician, along with the owner of the MSP firm, contacted the practice administrator to report the findings. The MSP owner stated to the practice administrator that the group appeared to have been hit with a ransomware attack, and all the practice's data stored on the impacted servers had been encrypted and rendered inaccessible. The practice administrator immediately contacted SVMIC thereafter to provide notice of the incident. The SVMIC claims attorney taking the call then contacted SVMIC's third-party cyberliability insurer, Tokio Marine,[1] about the incident.

Tokio Marine promptly contacted a law firm to request that they advise the insured medical practice. Following a couple of initial telephone calls with the practice administrator, the retained law firm contacted a digital forensic investigation firm which focused on responding to data security incidents and requested that they assist in the incident response. Specifically, the digital forensic investigation firm was requested to immediately confirm that the medical practice's system was not subject to ongoing or persistent compromise. Once there was some assurance that the attacker had been fully eradicated from the system, the digital forensic investigation firm began an investigation to determine the initial point of entry the adversary exploited to attack the network and took steps to determine whether any protected health information (PHI) had been accessed or stolen ("exfiltrated") by the attacker. Additionally, the investigation/cyber incident response firm was requested to contact the adversary to begin ransom demand negotiations in the event it was necessary to pay the ransom in order to attempt to restore the practice's data.

In the meantime, while the practice administrator, the group's retained legal counsel, and the investigation firm were looking into the matter, the practice's waiting room continued to fill up for the day. Many patients were turned away, as no records could be accessed. For patients with more acute conditions who needed to be seen that day, they were examined, with the findings recorded on paper and stored in a secure file drawer. One patient presented who needed a medication refill urgently. A nurse had to spend an hour looking for the key to the drawer where one physician's paper prescription pad was stored because the practice's electronic prescribing system was not functional due to the ransomware attack. No billing for any of the services provided that day could be entered into the system, as the practice's financial management system was also inaccessible.

While the group's MSP firm was very cooperative in the efforts, by the end of the day on Tuesday, it was unclear whether the medical practice had a full and viable backup of its data. As a result, the investigation firm proceeded to engage in negotiations with the adversary in the event that the ransom payment was necessary in order to attempt to recover the data. The MSP had required all user passwords to be reset shortly after the ransomware attack was discovered. The investigation firm was able to provide some preliminary assurance that it appeared the immediate threat had been eradicated from the group's system. However, as the cyber incident response firm made clear from the outset, a payment of any amount of ransom was no guarantee that any of the data would be retrievable.

On Wednesday morning, following some negotiation with the adversary by the incident response firm, the ransom demand had been reduced slightly, to 3.5 bitcoin, or around $35,000. Fortunately, the MSP was able to confirm that a backup of the practice's data had completed at approximately 2:00 AM on the preceding Saturday morning, just about three hours before the attacker began encrypting the practice's data. It was also with relief that the MSP confirmed that the malicious software had not encrypted the data on the backup system. New hard drives were inserted into the workstations and servers that had been identified as impacted, and the MSP began restoring the practice's data from the backup. The old hard drives were preserved for evidence. The MSP provided an estimated recovery time of all systems no earlier than mid-day on Friday.

For the remainder of the week, as the practice's systems were restored piece by piece, patient care capacity was significantly reduced, with many patients continuing to be turned away. It was not until after noon on Friday that the practice had regained full access to all its data from the rebuilt systems and recovered data. It took the practice another full week to input the medical record information that was recorded on paper while the systems were down, and it was another two weeks until all the billing information had been brought up to date.

Within about a week and a half after the attack, the forensic investigation firm had completed its initial investigation. It determined that the adversary had accessed the practice's network by way of its Windows Remote Desktop Protocol. The user account, which had administrator-level privileges, and which was compromised to access the system remotely, had a weak password that had not been changed in at least two years. Additionally, multi-factor authentication was not enabled for the user account. Fortunately, however, there was sufficient evidence from the investigation indicating that the attacker was only in the system long enough, about 30 minutes, to install and launch the malicious software that encrypted the practice's data over the long holiday weekend. Based on the evidence examined, there was no indication that the adversary viewed, accessed or exfiltrated any of the practice's PHI as a result of the incident.

Lessons Learned

While estimates vary considerably, by any annual measure—whether it is dozens or

hundreds of attacks—ransomware is an undeniable threat to healthcare entities, as covered in a recent SVMIC newsletter article. Under the framework of the ransomware guidance from the U.S. Department of Health and Human Services (HHS) addressing ransomware in the context of HIPAA, it is generally believed that many, if not most, ransomware attacks do not result in reportable HIPAA breaches. As a result, the actual number of attacks against healthcare entities is unknown.

Taking proper preventative steps is the most effective means of avoiding ransomware attacks in the first place. In this claim scenario, the practice suffered a ransomware attack due to a weak remote access account password, which was likely acquired from a darkweb site or easily guessed. The extended period of time since the password was last changed (if ever) makes a weak password even more vulnerable. Additionally, the practice had not implemented multifactor authentication (MFA) to the Internet-facing account. MFA is not readily and conveniently available for all systems, but it is something that should be explored for an additional layer of protection. Finally, while not a specific issue in the investigation, it was not clear whether the practice had evaluated if every user needed to have administrator-level privileges. Limiting levels of access can, in some cases, help prevent the installation of malicious software.

One positive takeaway from this claim is that the practice had a viable and fresh backup. When a practice is hit by a ransomware attack, there are usually two options: #1, recover your data from a backup; or #2, pay the ransom and cross your fingers that you get a valid decryption utility from the hacker. Unfortunately, in many instances, a viable recent backup is not available, eliminating the preferable option. There are a number of reasons why a viable backup may not be available, not the least of which is that the backup system is not segregated from the network and the backup data is also encrypted by the same malicious software impacting the other data. It is important that groups work with their IT staff or their outside MSP vendor to configure their backup systems to be resilient against ransomware while also reliably and frequently backing up the practice's critical data. Backup system resiliency and comprehensiveness should be periodically evaluated.

Another positive outcome from this otherwise unfortunate claim is that the digital forensic examination was able to determine with a reasonable degree of certainty that there was not any improper access or exfiltration of PHI or other sensitive data. For a variety of reasons, there are some instances where such a reassuring finding cannot be made. In those cases, where either there is an indication that data has likely or actually been accessed or acquired, or there is insufficient evidence to reach a point where a determination can be reasonably made that such access or acquisition was unlikely, notification to patients, HHS, and in some instances, the media, may be necessary. Additionally, it is becoming increasingly common that ransomware actors are extorting victims twice: first by demanding a ransom to be paid, purportedly in exchange for a decryption utility; and then, even in cases where a good backup is available, demanding a ransom be paid or else the adversary will disclose sensitive data that it claims to have stolen from the practice's system.

Healthcare entities of all sizes are prime targets for ransomware attacks. The threat has increased in recent years and shows no signs of abating. As this claim scenario demonstrates, even with a relatively good outcome—where no ransom had to be paid, and no notification was required—ransomware attacks are extremely challenging, disruptive, and costly to healthcare groups. Preventative measures are the best first step to take to avoid ransomware attacks. Groups should also be ready to quickly respond in the event they become a victim.

* Several facts about this claim have been changed to anonymize the individuals and entities involved, but the consequences of ransomware attacks, as presented here, are real.

[1]. For more information about resources available from Tokio Marine HCC and its role in cyber liability claims, see these articles from May 2021 and June 2021.
