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)

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.