When a Vendor's Cybersecurity Problem Becomes Your Cybersecurity Problem

Several months ago, a medical practice was unable to access its cloud based EHR system early on a Friday afternoon. A support ticket was submitted to the EHR vendor requesting assistance for the problem. In the meantime, the practice activated its emergency procedures protocol and records of the patient visits for the rest of the day were kept on paper. When the office opened the following Monday morning, although the system was seemingly slow when staff initially logged on, by noon, the system appeared to be operating normally. Information from the paper records generated during the system outage was entered into the EHR system and, from all indications things seemed to be back to usual. The office manager who submitted the support ticket was curious however because, unlike support requests submitted in the past, the group had not received any response from the EHR company to the ticket that was submitted on Friday.

At the end of the week, the group received an email from its account representative attaching a letter from the CEO of the EHR company. Contained in the letter was a statement that the EHR vendor was investigating a security incident it experienced the prior week. The letter indicated that additional details would be provided after the company had concluded its investigation. A couple of weeks went by with no further mention from the EHR vendor about the incident. Approximately three weeks after the practice noticed the system problem, it received a letter from the EHR company stating that a data breach had occurred as a result of the incident and the practice's PHI was involved. The question then became who is going to provide notification of the breach to the practice's patients, the U.S. Department of Health and Human Services, and presuming the breach was a large one, the media?

With the growing reliance on an array of vendors, particularly for providing information technology services, the story above is becoming increasingly prevalent for medical practices of all sizes. According to a recent survey, organizations within the healthcare industry were the most common victim of attacks against third parties, i.e., their business associates, accounting for one third of these types of incidents last year.[1] Ransomware, and its particularly disruptive consequences, was the most common type of attack. These events can be catastrophic to the targeted vendor, with the disruptive effect significantly impacting the vendor's customers. In the increasingly common claims scenario above, the reason why the vendor did not respond to the support ticket was because, as is often the case, it was completely overwhelmed in responding to the incident. In many cases, because the immediate incident response has consumed all the vendors' capacity, the impacted vendor is, at least temporarily, unable to assist or even provide timely information to its medical practice customer. That can be a lonely and unsettling position for a healthcare organization who is completely dependent upon the vendor for the normal operation of the practice. It can also result in confusion for the medical practice in terms of what to do next.

Covered entities should be mindful of their obligations under HIPAA for notification in the event of a data breach. This includes a data breach occurring at or because of a medical practice's third-party business associate vendor.[2] Obligations for covering the cost of the data breach are increasingly common provisions in services agreements between covered entities and business associates. Regardless of the existence or nature of any such provision in a services agreement or business associate agreement, under the HIPAA Breach Notification Rule, the covered entity is ultimately responsible for ensuring that proper notification is made whether that notification is made (and paid for) by the business associate, or whether the covered entity must do that themselves. There may be additional breach notification obligations pursuant to state law.

In the scenario above, the medical provider was prudent in contacting SVMIC about the incident, who in turn notified Tokio Marine HCC, who writes and administers cybersecurity coverage for SVMIC policyholders.[3] Tokio Marine can begin to assist policyholders navigating these challenging scenarios by resourcing the necessary legal and technical assistance. While the availability of coverage is subject to the terms, conditions, and

limitations of the insurance policy based on the unique circumstances of each occurrence, it is prudent for insureds who receive notification about a security incident or data breach from a business associate vendor to promptly notify SVMIC about the incident. In the event the security incident is a data breach, significant costs and even liability may be involved. Even if the incident is determined, as a legal matter, not to be a data breach, the HIPAA covered entity medical provider is likely still required to take certain actions.[4] For a variety of legal and practical reasons, the earlier that notice is provided to SVMIC of these incidents, the better. In some cases, if notice of a potential claim is provided too late, coverage may be denied.

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

[1]. "33% of Third-Party Data Breaches in 2021 Targeted Healthcare Orgs," securitymagazine.com, https://www.securitymagazine.com/articles/96965-33-of-third-party-data-breaches-in-2021-targeted-healthcare-orgs.

[2]. Obligations of HIPAA covered entity providers and organizations relating to their business associate vendors was the subject of a January 2022 Sentinel article.

[3]. For more information, including general information pertaining to limitations and notification obligations, about the privacy and cybersecurity aspects of coverage provided through SVMIC, please see the September 2021 Sentinel article, "Know Your Policy: Your Coverage and Responsibilities under the Cybersecurity Policy."

[4]. Obligations of HIPAA covered entity providers and organizations pertaining to security incidents was the subject of a November 2021 Sentinel article.

Risk Matters: Tracking Procedures

Missed diagnosis is a top claim received at SVMIC. The tracking of lab and diagnostic test results, as well as referred patients and missed or canceled appointments, is essential to avoid delays in diagnosis and/or treatment. A patient may fall through the cracks if an abnormal test result is misplaced or filed away without taking appropriate action, or when a patient fails to keep a recommended appointment either with the referred physician or your practice. If a patient suffers consequences from not receiving the lab test that you ordered or from not seeing the consultant to whom he/she was referred, you could be named in a medical malpractice lawsuit. This Risk Matters advice focuses on the delivery of test results.

A consistent method for notifying patients of **all** test results and instructing them to call the office if they have not received the results within the expected time frame should be established. These instructions to the patients, as well as actual patient notification, should be documented in the medical record. Although instructing the patient to call for test results does not absolve the doctor of the duty to inform the patient, it does act as another safety net to ensure that important test results do not get overlooked and is a legitimate means of vesting the patient in his/her own healthcare. The more layers of redundancy that can be built into a system, the better.

It should be noted that, irrespective of a facility's statutory responsibility to report test results, (e.g., mammograms), the physician is not alleviated of responsibility to ensure the patient has been notified of **all** test results as outlined above. Likewise, when an *unsolicited* test result is received regarding an established patient of the practice, it should be handled the same way as one that was personally ordered. The patient needs to be notified that the provider is in receipt of the report in error and has or will notify the ordering physician. Do not automatically assume "normal" results do not require action, as occasionally results within normal range of the laboratory may not be the expected result for the patient. Rather, attempt to contact the ordering physician. Additionally, the testing facility needs to be contacted and notified that the provider is not the ordering physician, and the result should be delivered to the physician who ordered the test. If the patient is not known to the provider, there is still a limited duty of care owed to the patient. Much of this obligation would be minimized by confirming with the ordering physician (if possible) that he or she received and addressed the test result. In any event, the testing facility should be notified that the provider is in receipt of the report in error, and it should be delivered to the ordering physician. *If the report indicates a panic value or grave condition* and the provider is not able to confirm that the ordering physician is in receipt of the report, an attempt should be made to contact the patient. In both cases, this notification includes contacting the patient and arranging for any appropriate follow-up care.

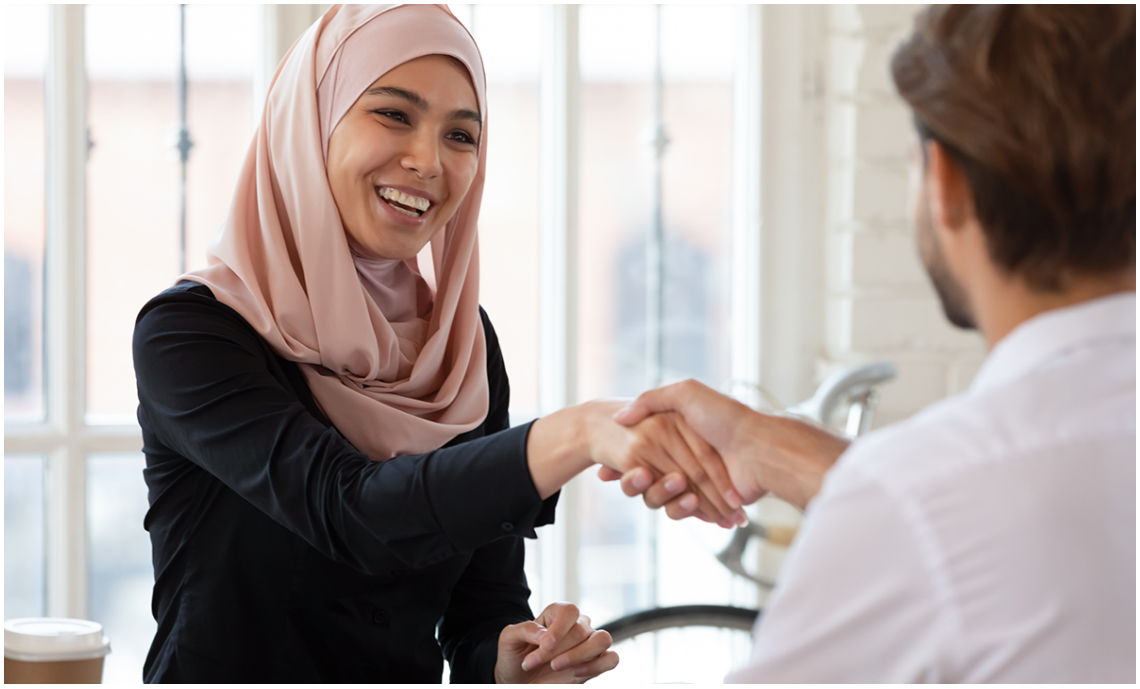
Practices can make use of electronic patient portals for notification of normal, non-sensitive test results for those patients who have signed a written consent or electronically agreed to receive information via the portal. However, it is not reasonable to assume all patients are able or choose to use the portal. Practices should verify that patients have accessed the portal before utilizing this as the sole vehicle of notification of normal non-sensitive results. Patients who do not use the portal should be notified of normal test results through another mechanism. It is not acceptable, from a risk or customer service perspective, to advise patients that the only method of normal test notification available will be through the portal.

Practices should be familiar with the general requirements of the U.S. Department of Health and Human Services Office of the National Coordinator for Health Information Technology's (ONC) Cures Act Final Rule, also known as the ONC Information Blocking rule, which became effective in 2021. Among other aspects of compliance with the regulation, practices should have documented procedures pertaining to how both in-house and outside lab results are made available to patients and when an exception to access may apply. While clinicians are not required to make in-house test results immediately available, they are required to promptly respond to a patient's request for access. Medical practices should be mindful that outside lab results may be immediately posted to a patient's EHR and implement a policy requiring prompt review of posted results as well as personal communication with any patient with an abnormal result, sensitive information or a result requiring immediate action.

The required follow-up *for non-adherent patients* or to communicate test results is not clearly defined. However, there is an expectation that the physician has superior medical knowledge and therefore owes a duty to the patient to thoroughly explain the results of the tests and any recommended treatment course. Follow-up should be appropriate for the

individual patient's specific circumstances. The reasonableness of the effort to contact the patient will depend on the clinical importance of the test results, the severity of the patient's medical condition, and the risk associated with failing to notify the patient of the results.

New HR Checklists to Streamline Your Practice



Human resources consume a tremendous amount of time for the average practice. The paperwork alone is overwhelming for many practice executives, especially coupled with other duties and management responsibilities. The Great Resignation has brought the need for a strong recruitment and retention plan to the forefront of practice management. A single, unintentional misstep can not only cost a practice a good employee, but it can result in an HR nightmare with accusations of discrimination, bullying, or worse. The key to avoiding such accusations is a consistent approach to the hiring, training, and evaluation of all employees. Checklists are a great way to ensure all employees, either current or potential, are treated equally. SVMIC is pleased to share with our members and their practice leaders our newly developed HR Toolkit.

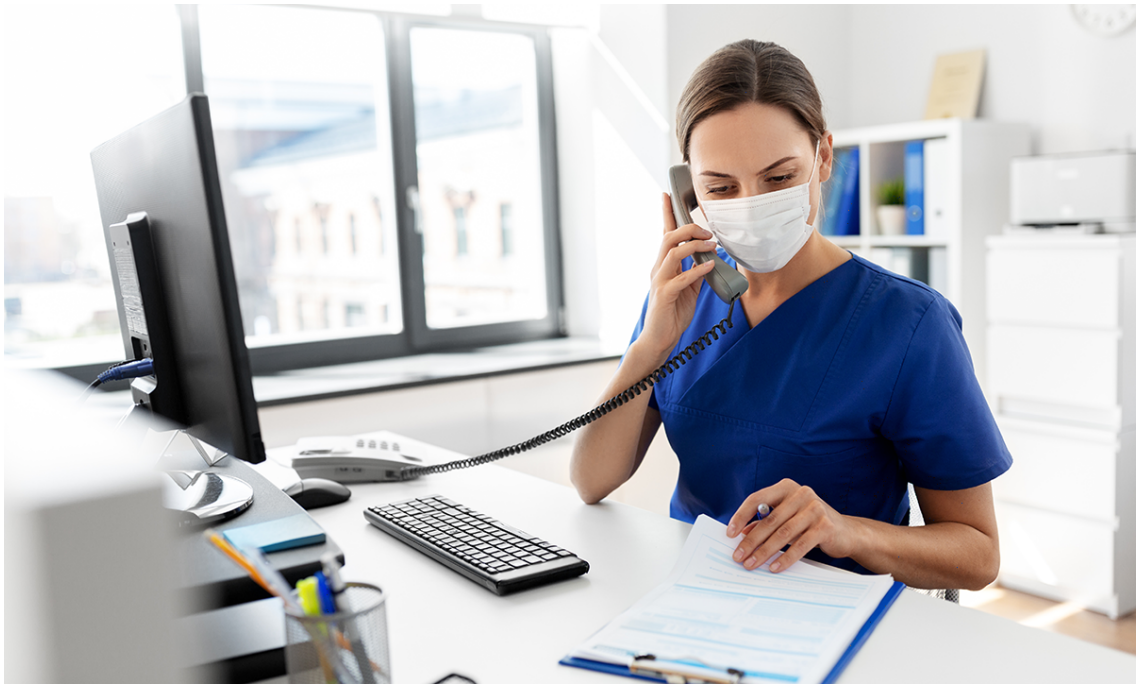
The SVMIC Human Resources Toolkit provides an “at-a-glance” view of the key steps in an employee’s life cycle with handy, easy-to-use checklists to support each stage. Beginning with the recruitment and hiring process and continuing through onboarding, the toolkit offers suggestions for improving retention. If needed, for those unfortunate situations, a performance improvement plan and a termination checklist are also available. The toolkit is

designed to be used in its entirety for every employee, or individual sections may be downloaded for use as needed. When you already have a full plate, this is a great resource to ensure nothing falls through the cracks.

Members and their staff can access the HR toolkit on the Vantage® Resources page at this link.

The HR Toolkit is one of the many ways SVMIC can help with your HR challenges. Our Medical Practice Services Consultants are available to assist with those tough HR questions. Additionally, we can perform an assessment of your practice's culture to help you keep those great employees once you find them. A variety of educational topics are also available to supplement your professional development efforts with your team. Reach out to us at ContactSVMIC@svmic.com or 800.342.2239 and ask for Medical Practice Services.

Leveraging Human Behavior Insights to Benefit Your Practice



Behavioral science is a growing field of science, rooted in economics as a means of understanding decision-making. People do not always make rational decisions that align with the beliefs of economists. Indeed, traditional economists had historically opined that all human determinations are made based on price and quality. Researchers are now challenging that notion.

At the most basic level, think about a pair of shoes that your child asks you to purchase; the shoes are $400(!). You think that the price is way too high, especially when you learn that the shoes will not even be worn. Your child is simply focused on the “coolness” factor that the shoes provide.

The field of behavioral science is centered on understanding seemingly irrational human behavior - and may have some important findings that can be translated into your medical practice.

Take the opportunity to consider these observations and tactics to benefit your practice:

Waiting feels like forever (literally). A recent meta-analysis concluded that, on average, a minute of waiting time feels like three minutes. Consider designing systems to keep your patients informed and perhaps even entertained. Train staff to fill in dead space during phone calls, or when they escort the patient down the hall. Talking about the weather is always a great default (and yes, many staff need training on how to make small talk). Message or call patients back at the end of the day to report that their message is in process, or their records are being reviewed. The uncertainty breeds insecurity, which often translates into more work (i.e., patients leaving a multitude of messages trying to get a response). If you cannot close the loop on messages every day, at a minimum, make it a priority on Friday afternoons. Give patients a tablet to gather information while they are waiting, ideally linked directly with your EHR system to reduce the staff's burden of re-keying the information. The dead time in the exam room can be supported by a poster or LCD screen conveying patient education; soft, white noise; or coloring pages. Look for other ways to reduce waiting times – or the perception of them.

Recency bias is real. Not surprisingly, researchers have proven that the last information we hear is what we remember. Our brains cannot contain everything, so we take short cuts. Translate that into practice for staff meetings – always close with the key points verbally and bullet the takeaways on index cards; for patients – always repeat the key points of the plan to conclude an encounter; and reiterate the date and time of the follow-up appointment at the end (over the phone or in person).

The community exerts influence. During the pandemic, we were restricted from being with other people; new research has demonstrated the negative impact of loneliness. Consider group visits: 98961 and 98962, for example, provide a community setting for patients – and the opportunity to leverage your non-physician clinical support team's time for billable services. Some commercial payers recommend using the standard office E/M codes – 99211-99215 for group visits, making denials unlikely. Another idea to leverage your community is to ask patients to be your "spokespeople" – reach out to a local high school or college and ask a teacher to sponsor a film project. Seek permission from patients who are willing to share their stories on film. Photographs can also be a compelling medium.

Use basic, non-verbal cues. In Japan, each train station stop has a unique "jingle" when the train pulls up to the stop. In healthcare, many children's hospitals have embraced non-verbal design elements such as the "butterfly" elevator. But cues do not need to be limited to trains or children's hospitals. Consider sound, light, colors, shapes, or symbols to promote a patient-centered design in your practice. Design elements may include a large red carpet in front of check-out, or a series of circles that lead a patient to the lab. Paint the exam room doors a different color for each pod, or use a theme for each (e.g., mountain, river). For a large facility, associate a color with each floor. If patients are registering at a central station on the ground floor, give the patient a green folder, clipboard, or form for the second floor, for example, and carry that theme through the clinic on that floor. Dimmer lighting has been proven to create a calm environment for patients; remove bright lights as the standard for your exam room, and instead rely on an exam lamp when needed.

Get a foot in the door. Every medical practice is challenged with staff recruitment and retention today; consider that behavioral science reveals the benefit of getting a foot in the door. This is why, for example, many companies offer free trials to get us hooked as customers. Instead of conducting phone interviews, therefore, consider bringing in top candidates who have compelling resumes to interview after an initial screening. Offer a mug, charger, or other small gift emblazoned with your logo, as a thank you for interviewing. If you like the candidate, shoot a text to a current employee during the interview to stop by the room to welcome the candidate. Send an email to the candidate thanking them for interviewing. A mug or a bit of kindness is not going to make up for a sizable salary difference, but if your candidate is deciding between two similar offers, your small gestures will certainly be a positive influence.

A multitude of ideas exists to harness human behavior to your practice's benefit. Start with a few of these – and challenge yourself and your staff to come up with more ideas. Researchers in behavioral science are not only thought-provoking, but they are also inspiring – and some of their findings may have a big impact on your practice.
