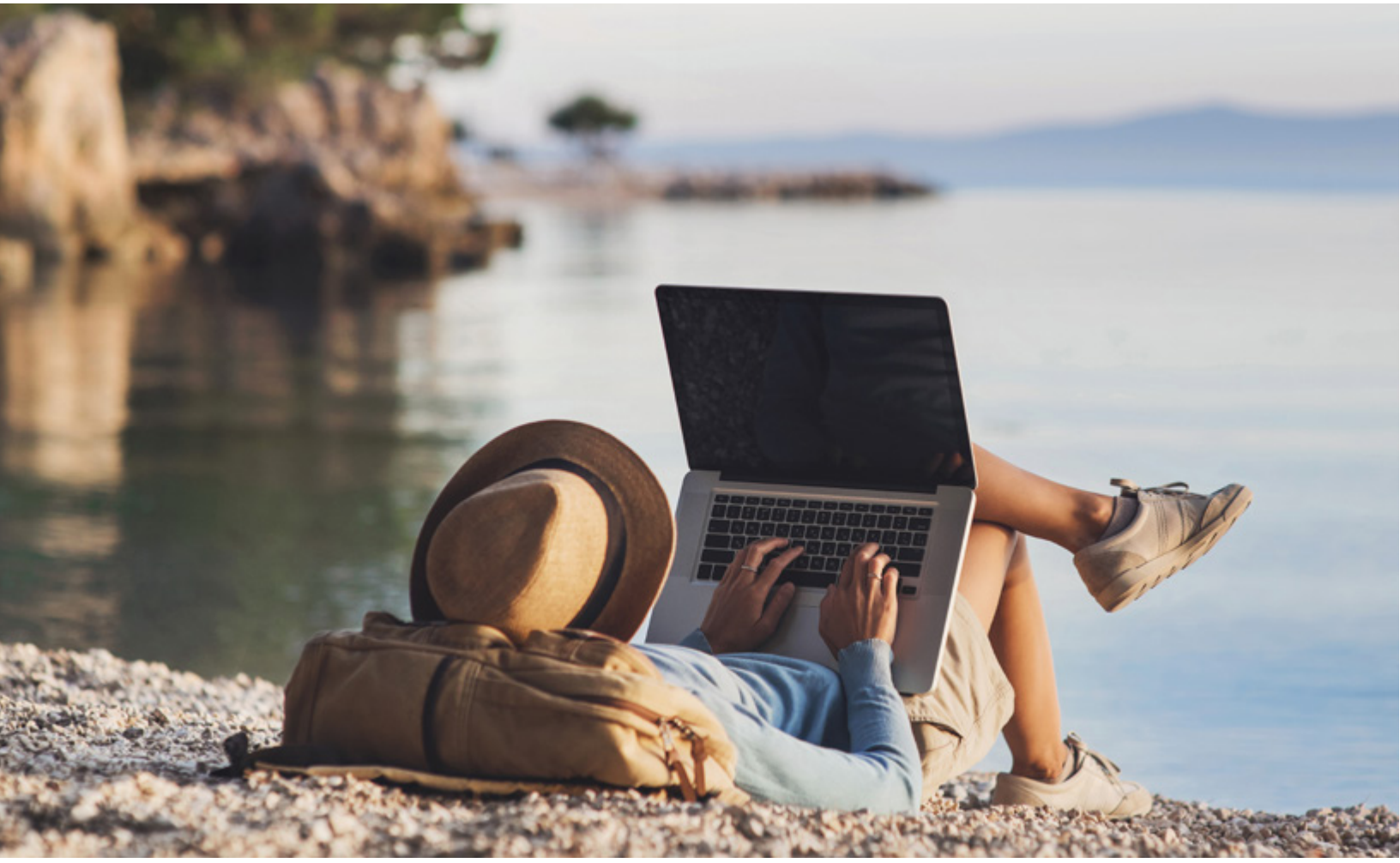
Medical Practice Cybersecurity

4 Sure Ways to Stop Cyberthieves



AdvancedMD

Medical practices are by and large filled with dedicated, highly skilled people focused on providing the finest healing, service and care possible for their patients. Many clinicians and staff go to extraordinary lengths to ensure their patients are safe and well attended.

That is, until it comes to cybersecurity – the security of patients' personal healthcare information, or PHI as it is known in industry parlance, stored in the electronic medical record systems of most practices and hospitals. Unfortunately, the healthcare industry historically leads in the number of security breaches per year where sensitive personal customer or patient data is lost to cyberthieves. A recent Protenus report found that healthcare cyber breaches now account for 34% of all incidents worldwide, and have jumped 151% over the past ten years, reaching a pace of one breach per day in 2017.

While you may have dodged the hacker's bullet thus far, the fact is that most practices are significantly behind in implementing more sure ways to stop cyberthieves. Unfortunately, neglecting the cybersecurity of your patient data is a ticking time bomb, equivalent to hanging out a big cyber sign saying, "Patients for Sale."

Healthcare cyber breaches now account for 34% of all incidents worldwide

Why Do Cyberthieves Pick On Us?

Many practices wonder why they are singled out for these cyber attacks.

The answer is twofold: Not only does your industry lag behind the latest security measures, making for an easier score, but you also have the misfortune of having a large target painted on your patient data because it sits at the top of a hacker's value chain of illegal information sold on the so-called "dark web."

For example, a recent Trustwave report found that a healthcare record may be valued at up to $250 per record on the black market, compared to $5.40 for the next highest value record (a payment card). That's because the medical record is the most comprehensive profile of a person's identity that exists today. A patient's EHR record contains all of their demographic information - names, social security number, historical information of where they live, where they worked, the names and ages of their relatives, and financial information like credit cards and bank numbers. This is in addition to highly sensitive medical information, including every visit they've made to the doctor and every diagnosis received.

The truth is you can cancel credit cards and change social security numbers, but personal health information is immutable. With this information, hackers can potentially blackmail you for a lifetime.

Understand the Risks

Many administrators are unaware of the magnitude of the risks, legal and financial, their practice could face from a cyber breach. A breach of any size is more than a passing problem. It's a major risk that can be potentially devastating for a group practice.

Legal Risks
Legally, cyber breaches are monitored and governed by the Office of Civil Rights, OCR, an office of the Department of Health and Human Services that oversees overall HIPAA compliance. Any breach of more than 500 patient records must be reported to OCR, and can result in substantial fines and even criminal charges.

Even a small breach can result in large fines if compliance is especially weak or lacking. For example, in June 2017, Catholic Health Care Services of the Archdiocese of Philadelphia (CHCS) settled for $650,000 over the loss of only 412 patient records – a fine of more than $1,500 each. The settlement was a punitive measure in response to the entity's lack of cyber protection policies and risk management plans.

Cost of Repair
Beyond reporting and paying fines, laws also require remediation with patients, which can include notifications, credit repair and monitoring services, legal fees and other measures. A recent study estimates this cost at $148 per record. A loss of 1,000 records, for example, can result in an additional $148,000 in cost of repair above and beyond fines paid.

Loss of Credibility
Perhaps worst of all is the loss of credibility and trust practices suffer with patients whose personal information has been compromised. No dollar figure can capture the sentiment of patients who lose confidence in their providers as a result of a cyber hack.

What You Can Do:

4 Sure Ways to Stop Medical Practice Cyberthieves

While no system is completely impervious to hacking, implementing these four proven approaches will vastly improve your defense against cyber criminals, and will put you in a very strong position for dealing with OCR and quick recovery in the unfortunate event of a breach or audit. Discuss these options with your physician decision makers and help them understand the magnitude of the challenge and what can practically be done to protect the practice.

#1. Know Where You Are Now – Perform a Security Risk Analysis

As a minimum, obtain a reliable checklist that is comprehensive and HIPAA-centered, and complete a self-assessment. This is best done by designating a security officer in your practice to conduct the analysis, as this is one of the first positions OCR will look to verify in the event of a breach or audit. This could be you as administrator, or someone else in the practice who has the skills and interest.

If your practice is inexperienced in this area, a better option might be to hire an outside security company to perform a HIPAA security risk analysis, coordinated by your designated security officer.

Include your technology vendors in your review. It's important to understand the security measures and potential holes built into practice management, EHR and billing software packages, and vendors' plans to address issues.

#2. Create a Risk Management Plan

Document risks that come out of the security risk analysis, determine how they'll be handled, and track progress of remediation efforts.

This step is crucially important, first because without a plan, nothing changes. A good plan, faithfully implemented and updated, vastly improves your chances of thwarting a cyber attack. Beyond that, OCR fines and punishments have historically been most harsh against organizations with weak or non-existent plans in place.

#3. Control External Vectors

In security lingo, a vector is a pathway used by hackers to infiltrate a target system. These can be external to the organization, or from within. We'll first address external vectors.

Move to a Cloud-based System
This point can't be overemphasized. Cybersecurity is a complex, moving target. Continuous updates are necessary to stay a step ahead of the criminals who continue to improve their level of sophistication daily.

Leading cloud-based EHR/PM/Billing system vendors have invested millions of dollars protecting PHI, and many have dedicated security teams. It is virtually impossible for a small or midsized practice to invest sufficiently to protect data in an on-premise system.

Sign Business Partner Agreements
HIPAA requires that any business partners you engage with (e.g. technology vendors, service providers, etc.) sign an approved business partner agreement certifying their security compliance. This is another key component of your plan that OCR will look for in the event of a breach or audit.

Plug Endpoint Holes
While the heavy lifting of system security will be handled in the cloud, there are "endpoint" pieces of technology that must also be secured. First and foremost, all laptops and other access devices must use encrypted drives, and no PHI leaves the facility unencrypted (e.g. thumb drive, etc.). Other endpoint measures include things like changing default passwords on routers and Wi-Fi access points, and securing kiosks and monitoring devices open to the public.

#4. Control Internal Vectors

The key internal vector for system breach are your people. In practical terms, you are only as safe as your least committed, least well-trained employee or provider. That includes your physicians, by the way. They could turn out to be your biggest challenge. Research shows that of 1,138 breach incidents between 2009 and 2017, or 53 percent originated internally. Here's what you can do:

Thoroughly Screen Employees
This starts with background checks on all new hires prior to starting. Interviews should probe for understanding of and commitment to protecting sensitive personal patient information.

Detailed, Ongoing Training
Employees must be thoroughly trained on types of cyber attacks, how to recognize them, and what to do when they encounter suspicious items.

For example, The most common type of cyber attacks are phishing attacks, which infiltrate systems through fraudulent emails or direction to fake websites. According to an American Medical Association and Accenture survey of 1,300 U.S. physicians, 83 percent had experienced a cyber attack, and more than half of these came in the form of a phishing email.

Employees and clinicians must be trained in anti-phishing education, including things like taking caution when opening unknown emails, never downloading unverified files or visiting unknown websites, verifying email recipients, and never sending unencrypted PHI over email. Other minimum training includes choosing strong passwords, and limiting the release of PHI per the "minimum necessary" principle.

Constant Policy Review
Even with ongoing training in place, security policies must be continually highlighted and promoted to help ensure internal compliance. Reminding employees and providers of proper computer and email use, for example, can help ensure that security stays top of mind.

Listen
Employees are often on the front lines of cyber attack attempts. Create a strong feedback loop where they have the opportunity to ask questions, relate experiences, and share success that can help others throughout the organization.

No Patients For Sale From My Practice

Cyber criminal activity is at an all-time high, and is growing worldwide at an accelerated pace. Fortunately, the good guys have developed strong counter measures and the ability to stay a few steps ahead. The key is to understand the risks, create a strong plan, engage the right experts and technology, and constantly train and upgrade employees' knowledge of what to look for and what to do. Now is the time to put a stake in the ground and protect your practice, and especially your patients. Their PHI should never be for sale from your practice.

AdvancedMD

(800) 825-0224
advancedmd.com