AdvancedMD

BOOST

EHR SECURITY

5 features to look for

Since 2009, more than 120 million people have had their healthcare records compromised, and the problem is growing. From cybercriminals vying for your patients' most valuable information to a natural disaster that could wipe out your records, keeping your patient and practice data secure is increasingly challenging.

Choosing an EHR system that has the ability to keep your health records secure is more important than ever. This guide will help you learn the 5 key features you need in an EHR system to ensure top-level security.

Confidence in your EHR security and data recovery will help you and your patients feel safe in an era of growing threats.

Healthcare data breaches are growing. Are you ready?

Since 2009, more than 120 million people have had their healthcare records compromised, and the problem is only growing.[1] In 2014, 42 percent of all major data breaches happened within the healthcare industry[2], and security experts are already calling 2015 the year of the healthcare hack.[3] The potential economic costs of these breaches are anticipated to be as high as $6 billion.[4]

Cybersecurity threats are a top concern for many healthcare organizations. Today's cybercriminals recognize that your independent physician practice is a treasure trove of personal and highly sensitive information, and they're working hard to get their hands on it.

Beyond cybersecurity, your practice—if unprepared—is also vulnerable to everyday risks, like power outages, floods, fires, or even a natural disaster. If you have paper records or records stored on local servers, you are at risk. An unanticipated event could easily result in permanent data loss, crippling your practice and hindering patient care.

"In 2014, 42% of all major data breaches happened within the healthcare industry."

Are your records secure from cyber threats?

In February 2015, Anthem experienced a major healthcare data breach that affected nearly 80 million people. Anthem's cyberattack follows Premera Blue Cross' records breach, which affected 11 million people.[5] Unfortunately, these major security breaches weren't isolated incidents, but are instead part of a growing trend within the healthcare industry. Since 2010, cybercriminal attacks on healthcare systems have risen a startling 125 percent.[6]

Today's healthcare organizations are faced with mounting cybersecurity threats, including identity theft, malware, and other inadvertent or deliberate data breaches that put patient data and practice records at risk. In fact, research shows that the number one cause of a healthcare data breach is a cyberattack, followed by a lost or stolen computing device.[7]

"Since 2010, cybercriminal attacks on healthcare systems have risen a startling 125 percent."

Cybercriminals recognize that your practice contains financially lucrative patient data, while also recognizing the overwhelming task you have to keep that data secure. Unlike large hospitals, small practices often don't have the IT resources to protect their data. That's why having a secure EHR software system is so vital.

Would your EHR be secure in a natural disaster?

No one expects that a natural disaster will strike, destroying everything in its path—but it happens and it can wreak havoc on your private practice if you're unprepared. Just ask the many healthcare providers who were hindered by Hurricane Sandy or the tornados that ripped through Joplin, Missouri in 2011.

But beyond a natural disaster, a seemingly simple event—like a power outage or flood—can quickly turn catastrophic. If your practice is unprepared, you are at risk of losing invaluable patient medical records and practice information. And once this information is lost, it's nearly impossible to restore if you are using paper records or a client/server system. No matter the size, a disaster can have a long-lasting personal and economic toll on your organization and patients.

Could you access your patient data?

It is clear that a medical data breach could greatly impact your practice, but it would also harm your patients—and, just like you, they're worried about it.

Research shows that 45 percent of patients are "very concerned" about a security breach involving their personal health information.[8] And when they're worried, they're less likely to share their personal health information with you, including sensitive information such as substance abuse and mental health illness. In fact, 25 percent of patients already withhold personal health information due to data security concerns, and 54 percent say they are likely to change providers in the result of a data breach.[9]

In an editorial published in the April 2015 JAMA issue, David Blumenthal, M.D., and Deven McGraw, J.D., say patient trust is gradually diminishing, which has several negative implications for everyone. They write: "The stakes associated with the privacy and security of personal health information are huge. Threats to the safety of healthcare data need much more focused attention than they have received in the past from both public and private stakeholders."[10] Patient concerns are real—from becoming a victim of identity theft to maintaining personal privacy, it is your special responsibility to keep their information out of harm's way.

Is your EHR wired for security?

One of the primary threats to your practice is simply not planning or preparing for an unanticipated event. A majority of healthcare organizations agree that preventing a data breach, loss or theft is vital, yet studies indicate that only 33 percent have sufficient technologies and resources in place to prevent or quickly detect a data breach.[11]

Are you doing enough to ensure your EHR system information is safe? If you're backing up your data on a local server, the answer is no and you are at risk.

EHR security:
5 features to look for

Although there is a lot of concern about cybersecurity, the good news is that the right EHR can help protect your independent physician practice from a breach or data loss.

The are 5 key features to look for in an EHR system to ensure that your patients' information and your practice data is safe.

Interoperability | Patient portal | Cloud platform | Data backup | Data encryption

Interoperability for secure document exchange

Your EHR should have secure document exchange so you can interface lab and imaging results to automatically flow to the patient chart. This will give you the ability to receive and share health information electronically. This is called "interoperability" and will allow your EHR software to coordinate care across settings.

Electronically receiving and exchanging orders, results, referrals, consults, medical histories, and summaries is critical to patient care and you want to be sure that information is secure. Safe, effective document exchange can help you manage transition of care when you share patient clinical information with outside entities such as a new hospital, next provider of care and health information exchanges.

Processes that submits health data to registries must also have world-class security. When you electronically transmit health-related data to immunization, public health registries and cancer registries you need to know that the document exchange isn't vulnerable to hacks.

Secure patient portal

Choose an EHR that lets you securely communicate with both staff and patients. A powerful EHR allows you to collaborate with staff through secure interoffice messaging and to communicate with patients through the secure patient portal.

Find an EHR system that has unified messaging, a secure communications platform built into the EHR that allows your staff to easily communicate so the patient has a seamless, consistent experience from check-in to checkout.

Cloud platform

When your EHR data is stored on the cloud, you can access your records anytime and from anywhere, allowing on-call staff round-the-clock access.

This on-demand access means you never need to fear a data loss and your practice will be up and running in no time in the case of a natural disaster or damage to your medical office. Beyond enhanced security and anytime/anywhere access, the cloud ensures that your practice is up-to-date and compliant with the ever-changing and overwhelming regulatory environment.

Hourly data backup

Cloud-based EHR systems include automatic, hourly data backups, which mean you don't have to spend your valuable time with tedious manual updates. Every backup is verified to restore correctly and additional secure copies are storied every night. EHR systems with automated processes and security procedures also ensure that you're complying with stringent HIPPA regulatory and security requirements.

Furthermore, your electronic data should be stored in a state-of-the-art datacenter facility with several layers of security measures, such as biometric access, 24-hour monitoring, locked server cages, firewall protections, and NSA-approved procedures and policies.

Data encryption

An EHR system that encrypts your data will keep it safe from cybersecurity threats. Encryption is one of the most technologically advanced security systems, similar to those trusted by financial institutions to keep their data secure. Encryption will safeguard your electronic data transfers, prohibit unauthorized patient record access, and log all user activity, while also offering privacy tools for specific user roles.

Conclusion

No one expects that their data will be stolen by cybercriminals or lost during a natural disaster, but it happens. As the old adage goes, hope for the best and prepare for the worst.

The good news: Choosing the latest in EHR technology will ensure your information is secure. When shopping for a new EHR, or replacing your current system, make sure to check its key security features and capabilities. Knowing your EHR system has the ability to keep your records secure will help you and your patients feel safe and help you remain independent and profitable in an era of growing cybersecurity threats.

Choose a secure EHR

AdvancedMD is one of the world's largest providers of cloud software, including a Certified complete electronic health record. Our system can replace five or more systems with an all-in-one EHR and practice management solution that allows you to optimize schedules, simplify check-in and checkout, document patient encounters, prescribe and order, capture and pursue revenue, measure financial performance and practice on the go.

Request a demo

Visit advancedmd.com to see how integrated AdvancedMD EHR and practice management capabilities can work for you and your practice.

References

1. "*2015 is already the year of the health-care hack — and it's only going to get worse.*" The Washington Post, March 20, 2015.

2. Experian's 2015 Data Breach Industry Forecast.

3. "*2015 is already the year of the health-care hack — and it's only going to get worse.*" The Washington Post, March 20, 2015.

4. "*Hackers Sell Health Insurance Credentials, Bank Accounts, SSNs and Counterfeit Documents, for over $1,000 Per Dossier.*" Dell SecureWorks, July 2013.

5. "*22 New Breaches Affect 116,000 Patients.*" Health Information Privacy/Security Alert, June 2015.

6. "*Fifth Annual Benchmark Study on Patient Privacy & Data Security.*" Ponemon Institute, May 2015.

7. "*Fifth Annual Benchmark Study on Patient Privacy & Data Security.*" Ponemon Institute, May 2015.

8. "*HIPPA Breaches: Minimizing Risks and Patient Fears – Industry View 2015.*" Software Advice.

9. "*HIPPA Breaches: Minimizing Risks and Patient Fears – Industry View 2015.*" Software Advice.

10. "*Keeping Personal Health Information Safe.*" Journal of the American Medical Association (JAMA), April 2015.

11. "*Fifth Annual Benchmark Study on Patient Privacy & Data Security,*" Ponemon Institute, May 2015.