White Paper

From EHR HIPAA Compliance to Total HIPAA Compliance

securityMETRICS®

Electronic health record (EHR) systems are transforming the collection and standardization of patient medical information today. Having the ability to bring a patient's complete medical history into a single, electronic record easily accessed by literally thousands of providers and support staff, including physicians, nurses, therapists, clinical support, and billing departments is a major advance to the medical industry.

Never before has it been so easy for healthcare practitioners to access patient information.

Unfortunately, many organizations don't realize just because their EHR system is compliant with Health Insurance Portability Accountability Act (HIPAA) security standards, their workplace as a whole may not be compliant.

EHR security is just one small step towards HIPAA compliance.

The goal of this white paper is to provide HIPAA guidance by breaking down the compliance process into simple steps. The first step is to understand what your organization is and is not currently doing for HIPAA compliance. From there you can make HIPAA more manageable by breaking up the work into bite-sized, daily tasks. Finally, you should remember to search for and protect your patient data in all your systems and devices.

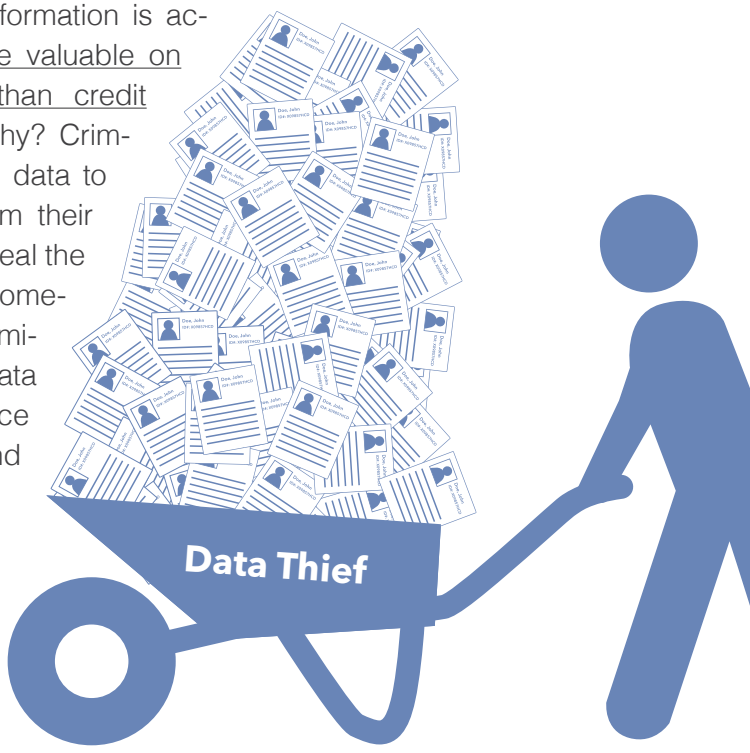
Your EHR: A Gold Mine

While EHR systems provide a more seamless flow of information within the digital health care infrastructure, they also offer quick access to confidential patient medical information.

Last year, medical and healthcare entities accounted for 42.5% of reported data breaches, such as the Anthem hack with millions of employee and customer information stolen.

Attackers are increasingly targeting electronic personal healthcare information (ePHI) instead of credit card data because many healthcare organizations tend to rely on outdated, poorly protected computer systems to manage their data.

Personal medical information is actually 10 times more valuable on the black market than credit card information. Why? Criminals don't just steal data to purchase things from their favorite store, they steal the data to take over someone's identity. Criminals use patient data to commit insurance fraud, tax fraud, and purchase drugs.



HIPAA Compliance Protects You and Your Patients

Every healthcare organization under HIPAA is responsible for the protection of its patients' data, regardless of whether or not organizations use an EHR vendor to process or store their patient records. Even if your EHR vendor claims you don't have to worry about HIPAA compliance – don't believe everything you hear. Even cloud-based EHR systems do not fully cover an organization's HIPAA compliance.

Just think of all the places patient data is gathered or stored that don't involve your EHR system, such as PHI stored at the front desk, file cabinets, folders, workstations, ticketing systems, telephone recordings, etc.

HIPAA compliance involves compliance with 75 specific security controls. These requirements include but aren't limited to:

- An annual HIPAA risk analysis (to identify organizational risk to patient data, as well as plan for remediation of those risks)
- Compliance with specific HIPAA Security Rule administrative, physical, and technical safeguards
- Development of specific policies and procedures
- Annual employee training

In our ever-changing digital environment, it's critical that today's healthcare organizations regularly assess their security programs as a whole to ensure they have the policies, procedures and security measures in place to better protect patient information and avoid costly violation fees.

3 Crucial Steps to Reach HIPAA Compliance

Step One: Understand Your Current Security State

The ongoing responsibility of managing patient data throughout an organization requires an organized, well-thought-out approach to risk management. No matter how small or established a practice, it's critical for healthcare entities to understand what they are, what they are not, and what they should be doing in the future to protect patient data.

While some EHR systems and their related equipment have security features built into or provided as part of a service, they are not always configured or enabled properly.

As the guardian of patient health information, it is up to each healthcare organization to learn and understand the basic features of their IT assets and medical devices, what security mechanisms are in place, and how to use them.

There are a number of actions you can take to make sure that your EHR systems and IT assets are secure, such as integrating

- Data Loss Prevention (DLP) tools: a piece of software or strategy to ensure users don't send sensitive information (such as PHI) outside the network.
- Intrusion Detection Systems/Intrusion Prevention Systems (IDS/IPS): a monitoring system to monitor network security appliances and report malicious activity.
- File Integrity Monitoring (FIM): a way of checking software, systems, and applications in order to warn of potential malicious activity.
- Role-Based Access Control (RBAC): the act of restricting users' access to systems based on their role within the organization.

To know which programs to integrate, ask 3rd party HIPAA compliance experts on best practices for data protection.

Many solutions available on the market today can empower healthcare professionals to implement first class security and HIPAA compliance programs that help with correct documentation on security practices, processes and policies, and better protect against data theft.

However, creating adequate safeguards does not happen overnight. The process requires you to:

1. Realize what HIPAA compliance fully entails by speaking with 3rd party compliance experts.
2. Understand your organization's risks and vulnerabilities by performing a HIPAA risk analysis.
3. Coordinate responsibilities in your organization and with third parties.
4. Have ongoing re-evaluation of your organization's approach for altered processes.
5. Hold regular security training.

Step Two: Make HIPAA Manageable

While it may seem overwhelming and time-consuming at first (especially because HIPAA compliance is so complex), the biggest obstacle to overcome is actually getting the entire process started. Begin by carving out a regular, weekly routine – perhaps starting at about 30 minutes per week when your staff members who are responsible for HIPAA compliance can meet to discuss the privacy and security of patient data.

Here are some specific actions an entity should take when working to protect patient information:

Staff Requirements

- Have a designated HIPAA-assigned compliance officer or team member.

- Clearly and specifically lay out the roles of everyone in your organization involved with HIPAA compliance responsibilities.
- Ensure that access to ePHI is restricted based on an individual's job roles and/or responsibilities.
- Require user authentication, such as passwords or PIN numbers that limit access to patient information to authorized-only individuals.
- Implement workstation security, which ensures computer terminals that can access individual health records cannot be used by unauthorized persons.

Technology Requirements

- Conduct an annual HIPAA security risk analysis (specifically required under HIPAA rules). This can involve regularly engaging with a trusted provider that can remotely monitor and maintain your network and devices to ensure ongoing security.
- Mitigate and address any risks identified during your HIPAA risk analysis, including deficient security, administrative and physical controls, access to environments where ePHI is stored, and a disaster recovery plan.
- Encrypt patient information using an encryption key known or made available only to authorized individuals.
- Incorporate audit trails, which record who accessed your information, what changes were made, and when they were made, providing an additional layer of security.

Step Three: Protect Your Entire Organization

Privacy and security concerns are key when it comes to HIPAA, but it's also important to be sure your enterprise as a whole is protected. It's critical to ensure ***all*** systems where ePHI resides are protected. The following are the most common areas where ePHI is stored (intentionally and unintentionally):

- EHR
- Database
- Server
- Security appliances
- Email system (in-office and doctor-to-doctor emails)
- Data warehouse
- File shares
- Ticketing systems
- Tablets/smart phones/mobile devices

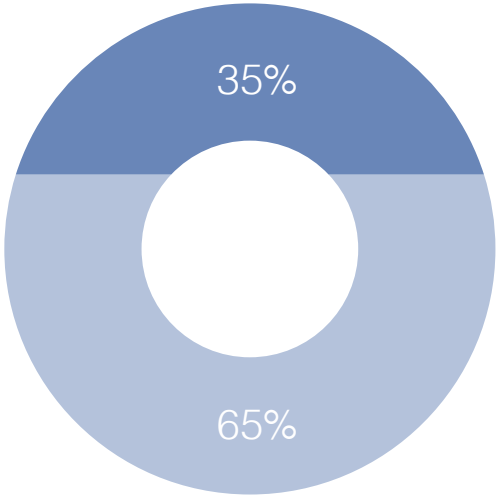
If this data is not properly secured, organizations are placing themselves and their patients at serious risk.

Failure to perform a thorough HIPAA risk analysis can have numerous negative repercussions, including:

- Increased chance of personal health information theft

- Fines and penalties from HIPAA violations (up to $50,000 per day)
- Potential for civil lawsuits ($1,000 per record)
- Loss of patient trust and business (40% choosing new health providers)

In October 2014, NueMD conducted a survey of more than 1,100 healthcare professionals to gauge their knowledge of HIPAA and preparedness for an audit. The results showed that only 35% said their business had conducted a mandatory HIPAA risk analysis.



Conclusion

Moving forward, the healthcare industry will need to continue to address the increasing threat of organizational data breaches. For organizations that have not already worked through a HIPAA compliance program, there are many options available that can be adopted with relative ease and low expense to further safeguard valuable data.

Without thorough implementation, most covered entities and business associates would fail a HIPAA audit. Without a background in security, there are many security aspects you might never consider. If you haven't already, start HIPAA compliance now and protect your patient's data.