MEDCURITY

HIPAA COMPLIANCE: WHERE TO START

It is important for your healthcare organization to routinely assess security risks, and ensure that all employees have proper training in HIPAA compliance.

Start with a Security Risk Assessment

The crucial first step in your HIPAA compliance journey is the Security Risk Analysis (SRA). The risk analysis assesses the vulnerabilities, threats, and risks to your electronic Protected Health Information (ePHI) so you can address them and prevent potential breaches. You will document human risks involving improper training, technology risks involving possible cyber security issues, and more. On completion of the analysis, you'll be able to evaluate your organization's level of security risk.

The Medcurity platform takes the stress out of the Security Risk Analysis and allows organizations to conduct their assessment more efficiently and effectively than ever before. Our SRA helps you identify potential gaps your business needs to address to better safeguard your protected patient information. Performing regular SRAs is an essential piece of the HIPAA Security Rule and will be beneficial for your organization.

Develop Policies and Procedures

Once you've completed your SRA, you'll need to evaluate your Policies and Procedures. As you experience changes in personnel, buildings, and technology, your policies need to stay updated and relevant. It's important to establish comprehensive Policies and Procedures for your organization and inform all employees of their responsibilities in regards to these documents.

As you revise your current policies, keep these five things in mind:

1. Proper handling of Protected Health Information (PHI)
2. "Bring Your Own Device" (BYOD) policies
3. High-profile patients
4. Encryption
5. Physical security

MEDCURITY

1 PROPER HANDLING OF PROTECTED HEALTH INFORMATION (PHI):

Who will have access to PHI? Where will the data be stored? How will the data be backed up in case of viruses or cyber-attacks? How will your organization dispose of PHI securely? Clear answers to each of these questions must be laid out in your Policies and Procedures, and each employee must have a good understanding of what to do in any of these situations.

2 "BRING YOUR OWN DEVICE" (BYOD) POLICIES:

BYOD policies are becoming increasingly common in today's workplace. These policies deal with the devices owned by employees that are brought onsite, such as personal smartphones, laptops, or tablets. While allowing employees to bring their own technology can save your organization money, it also presents new security risks that must be addressed to protect the integrity of your data. It's up to your organization if you want to take this risk. If you do allow personal technology, you must have established precautions for the use of these devices. Whatever security measures you decide to enforce, it is critical that you train your employees on these required practices.

3 HIGH-PROFILE PATIENTS:

However large your organization, you may serve patients with a high reputation in the community. Strict requirements for the protection and confidentiality of these high-profile patients' information should be laid out in your Policies and Procedures. However, a "break the glass" policy should be in place to allow internal access for treatment, administrative, or other specific purposes. Frequent audits are necessary to determine who is accessing patient information and whether they have a legitimate "need to know."

4 ENCRYPTION:

With increased use of technology and cloud services, more and more organizations are utilizing data encryption to boost security. Your Policies and Procedures should contain requirements for device encryption to protect PHI.

5 PHYSICAL SECURITY:

This portion of the Policies and Procedures deals with protecting the physical locations of PHI. Your facility should have alarms, locks, and other security systems in place, and employee access to patient data should be limited to only authorized personnel.

MEDCURITY

Common Issues and Practical Strategies

The following are some common privacy and security issues organizations face and some practical strategies for solving the issues.

PHISHING EMAILS:

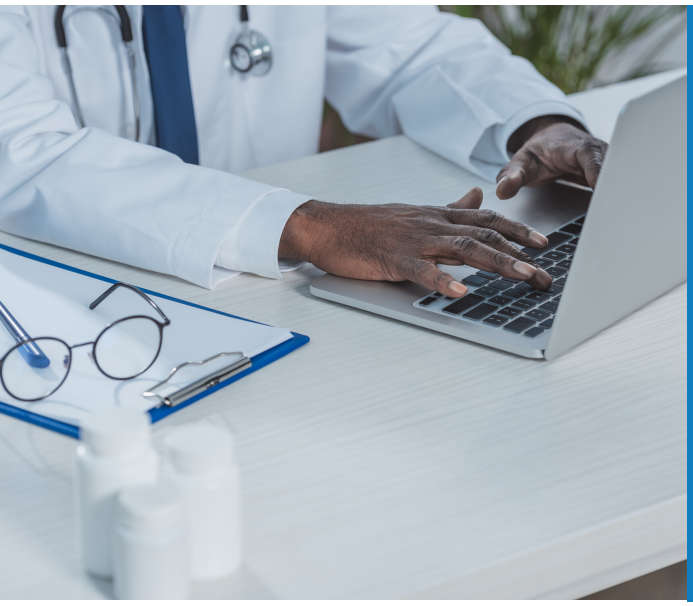
Cyber-attacks often occur when an employee unknowingly opens a phishing email, allowing a cybercriminal to bypass their organization's security system. To reduce security risks, employees should be properly trained on how to spot suspicious emails. The better informed your employees are on cyber-security threats, the safer your organization.

AUDITING AND MONITORING:

Smaller organizations may find it easier to monitor their fewer employees, but providers of all sizes need to conduct regular audits and random activity checks. These checks are a great way to catch and prevent suspicious employee activity and improve your overall security.

NOTICE OF PRIVACY PRACTICES:

Under the HITECH-HIPAA Omnibus Rule, a "Notice of Privacy Practices" is required on all covered entities' websites.



Your HIPAA Compliance Solution

HIPAA compliance isn't something organizations can afford to take lightly. At Medcurity, we have the knowledge and tools you need to **get the most out of your compliance efforts**. With our guided Security Risk Analysis software, customizable Policies and Procedures, Business Associate Agreement Management System, and Dark Web Monitoring, Medcurity helps you on every step of your journey to compliance. To see what this looks like, **go to medcurity.com and watch the free demo of our intuitive SRA**, which can be conducted and reviewed on your laptop, tablet, or smartphone.

Find out why Medcurity is the leading HIPAA compliance platform and begin your compliance journey today.

Contact Medcurity about HIPAA compliance software and services at **509-867-3645** or visit **medcurity.com** for more information.

CITATION: Primeau, Debra. "How Small Organizations Handle HIPAA Compliance" Journal of AHIMA88, no.4 (April 2017): 18-21.