

# WHERE DOES YOUR BUSINESS STAND IN THE FIGHT AGAINST CYBER CRIME?

## WHY DOES MY ORGANIZATION NEED TO WORRY ABOUT CYBERSECURITY AND HIPAA COMPLIANCE?

95% Of Data Breaches Are Due To Human Error<sup>1</sup>



59% of individuals admitted to mostly or always using the same password, despite 91% knowing it's a security risk.<sup>2</sup>



With protected health information (PHI) bringing in top dollar on the dark web, storing and accessing patient data puts your organization at a higher risk of suffering a cyber-attack.

Protecting patient data is your organization's responsibility. If you fail to properly protect that data, you are in violation of HIPAA regulations. Failure to comply often comes with hefty fines and penalties.



## HEALTHCARE SECURITY CHECK-UP

Review the top 11 security and compliance measures recommended for healthcare organizations below to see where your organization stands in the fight against cyber crime!

1. Do you conduct an annual HIPAA Security Risk Assessment and work to remedy any deficiencies?

☐ Yes ☐ No

2. Do all staff members take an annual structured HIPAA Security and Privacy Training course with a compliance quiz and documented proof?

☐ Yes ☐ No

3. Are all staff members trained on how to spot phishing emails?

☐ Yes ☐ No

4. Do you perform Network Vulnerability Scans on a regular basis (at least annually)?

☐ Yes ☐ No

5. Do you have Business Associate Agreements in place with all appropriate vendors?

☐ Yes ☐ No

6. Do you have any additional assurances that all your Business Associates are compliant with HIPAA?

☐ Yes ☐ No

7. Are all computer systems in your office encrypted?

☐ Yes ☐ No

8. Do you have a documented incident response procedure that addresses what steps are taken in the event of an incident?

☐ Yes ☐ No

9. Is there a process implemented to periodically check on the access and activity within systems that store electronic protected health information?

☐ Yes ☐ No

10. Do you have Cyber Insurance Coverage that can help offset the expenses, reputational damage, and workload related to a breach?

☐ Yes ☐ No

11. Do you have the appropriate documentation required by the HIPAA Security and Privacy Rules including termination procedures, disaster recovery plans and disposal procedures?

☐ Yes ☐ No

## HOW DID YOU DO?

Count up the total number of security measures you marked "Yes" to having in place, then use the key below to see the security state of your organization.

**8-11** You're well on your way to implementing a strong culture of HIPAA compliance & cybersecurity - Great job!

**5-7** You're off to a great start, but there's room for improvement!

**< 5** Now is the time to seek assistance and start working on your HIPAA compliance and cybersecurity!

Remember, whether you scored a 2/11 or 11/11, HIPAA compliance and cybersecurity are ongoing processes. Make sure you're actively working towards both!

## LET'S WORK TOWARDS PROTECTING YOUR ORGANIZATION, TOGETHER!

### Not sure how to get started?

Contact us today to learn more about [PHIshMD](#) and how we can help you mitigate your HIPAA compliance and top cybersecurity pain points.

[info@hipaasecurenow.com](mailto:info@hipaasecurenow.com)

877-275-4545