

# HIPAA IT Security Risk Assessment

Is your organization doing all it can to safeguard confidential patient information?

**Doing nothing could be considered willful neglect.**

A HIPAA Security Risk Analysis is required by law. We can conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by your organization.

## WHAT ARE THE RISKS?

- Increased exposure to data breaches
- Increased exposure to data loss
- Greater risk of downtime due to security incidents
- Monetary and Civil Penalties

In addition to civil financial penalties, a HIPAA violation can result in criminal charges being filed against the individual(s) responsible for a breach of PHI. Criminal penalties for HIPAA violations are divided into three separate tiers, with the term – and an accompanying fine – decided by a judge based on the facts of each individual case.

## WHAT DO WE OFFER?

### PEACE OF MIND WITH:

- Up to 20 hours of on-site interviews with key staff members
- An independent third party to review your environment
- Review of all HIPAA IT Security Policies and Procedures
- Gap Analysis of policies and actual performance
- A thorough assessment of the IT security configuration at the hospital and connected facilities
- A software tool that searches devices for vulnerabilities
- HIPAA IT Risk Assessment document, including results of a network penetration and vulnerability test, meeting the requirements of the HITECH Act and Meaningful Use requirements
- Three Quarterly updates, including up to two hours of off-site technical review per quarter

If you don't know the answers to these questions, call for a HIPAA Risk Assessment.

- When was your last annual risk analysis?
- Do all systems require a password?
- Do all systems require users to reset passwords every 90 - 120 days?
- Do systems timeout after a certain time of inactivity?
- Are all laptops encrypted?
- Is a Business Associate Agreement with **every** vendor that may access ePHI in place? Can I present them on demand?
- Do all new employees attend HIPAA training?
- Are all PCs patched?



**Call for a Free Consultation**

**Shannon Williams,**  
**MBA, PMP, CPHIMS**  
VP, Business Systems  
[swilliams@qhr.com](mailto:swilliams@qhr.com)  
479-879-7003

[Learn More](#)



**QUORUM** | HEALTH RESOURCES®

[QHR.COM](http://QHR.COM)