99MGMT
NINETY NINE HEALTHCARE MANAGEMENT

Sample HIPAA Security Risk Assessment for Small Physician Practices

Below are some common questions you may find in a security risk assessment for physician practices. You can start by reviewing these questions internally, but it is highly recommended that you get an assessment from an objective, experienced third party to ensure compliance.

	Risks found	Risk rating	Existing control measures applied	Recommended control measures
Information Storage & Access				
Do you store printed information in locked cabinets?				
Do you you store backups to the cloud?				
Do you collect handwritten or print documentation?				
Do you have a storage location for handwritten or print documentation?				
Do you use an EHR?				
How does your office access medical information?				
Networks				
Do you have a private wireless network connection with password to which all devices connect?				
What networks do you use to send and store information?				
How do you manage employee access to devices and networks?				
Office Devices				
What devices store information?				
What devices send information?				
Do the screens automatically shut off when not in use?				

Who has access to the devices?				
How do you physically protect your devices from theft?				
How does information travel from/between devices?				
Are all your devices encrypted?				
Are all your devices password protected?				
Security & Encryption				
Do you monitor and review third party connections to your network?				
Do you have a way to automatically log users out of databases or devices that have been idle?				
Do you have anti-malware and anti-ransomware software installed on all devices?				
Do you encrypt information while it's being sent?				
Do your data storage solutions encrypt information?				
Do you have a way to make sure that you install security updates to devices as soon as possible?				
Do you monitor potential unauthorized access to your systems and networks?				
Is your wireless connection encrypted or just the devices?				
How is your wireless connection protected from external threats?				
What are the physical security protections for your office, devices, and copies of printed materials?				
How do you secure passwords that can access information?				
Do you encrypt information as it travels between your devices and the database?				
Does the database encrypt the information?				

Patient Devices				
Do you have patients with medical devices that connect to the internet?				
Do you have patients using home/remote monitoring devices?				
Are connected patient devices encrypted?				
Do you use mobile devices for patients?				
People & Processes				
Do you create a unique user identification login and password for each employee?				
Do you have a way to make sure employees only access information they need for their jobs and nothing more?				
Do you have documented information security policies and procedures?				
Do you have a formal information classification procedure?				
Do you have formal acceptable use rules established for assets?				
Do you have formal processes in place for security policy maintenance and deviation?				
Do you have a process that addresses identification and measurement of potential risks, measures to reduce risk, and acceptance/transfer of residual risk post-mitigation steps?				
Do you provide formal information security training for employees?				
Do you provide periodic security reminders?				
Do you have a process to identify and respond to security risks/incidents?				