Practice Scenario: TechHealth Medical Clinic

Company Background

TechHealth Medical Clinic is a mid-sized healthcare provider with 3 locations serving 15,000 patients annually. The clinic recently transitioned from paper records to a cloud-based Electronic Health Records (EHR) system hosted by a third-party vendor, MediCloud Solutions.

Current Environment:
- 45 staff members (physicians, nurses, administrative staff)
- Patient data includes: medical histories, insurance information, Social Security numbers, payment card data
- Staff access EHR system remotely using personal devices (BYOD policy)
- No formal cybersecurity training program in place
- Annual HIPAA compliance audit scheduled in 90 days
- Recent media coverage of healthcare data breaches has patients asking questions about data security
- EHR system credentials shared among nurses during shift changes

Your Task

As the newly hired GRC Analyst (this is your first week), you've been asked to create a risk register identifying the top cybersecurity and compliance risks facing TechHealth. The CEO wants to understand which risks require immediate attention before the HIPAA audit.

Instructions:
1. Identify at least 4-5 distinct risks based on the scenario above
2. Document each risk in the Risk Register tab using the cause-and-effect format
3. Assess the control effectiveness (most will be "Open" given the scenario details)
4. Rate the Impact and Likelihood for each risk
5. Recommend appropriate risk response strategies
6. Prioritize which risks need immediate attention (Red) vs. can be monitored (Green/Yellow)

Tip: Look for risks related to: access controls, third-party vendors, employee training, remote access, data classification, incident response, and

Risk Identification Hints (refer to these if you get stuck)

Risk Category	Questions to Consider
Access Control	What happens if unauthorized staff access patient records they shouldn't see? How are admin privileges managed?
Third-Party Risk	What if MediCloud Solutions experiences a data breach? What controls does TechHealth have over vendor security?
Remote Access	What risks arise from staff using personal devices to access sensitive patient data? Are devices encrypted?
Training & Awareness	What could happen if staff fall for phishing emails? How would untrained staff handle a suspected breach?
Incident Response	Does TechHealth have a plan for responding to a ransomware attack? What about breach notification requirements?
Data Classification	Are all staff aware of which data is PHI? What happens if patient data is accidentally emailed to wrong recipient?

Portfolio Tip

Portfolio Tip

When sharing your completed risk register on LinkedIn:
1. Write a 3-4 sentence post: "I completed a risk assessment for a healthcare organization transitioning to cloud EHR. Here are my top 3 priority risks and why..."
2. Include a screenshot of your completed register (redact company name)
3. Mention you used NIST 800-30 framework
4. Tag 2-3 GRC professionals and ask: "What would you prioritize differently?"

This shows: analytical thinking, framework knowledge, and communication skills—exactly what hiring managers look for.