Company Details:

This report presents the findings from the simplified risk assessment of WebPT. WebPT is a cloud-based EMR system and practice management platform for rehabilitation therapists. The services offered by this company include but are not limited to, scheduling patients, completing proper documentation, billing patients, and tracking patient demographics and metrics. Rehab therapist companies contract with WebPT to reduce patient cancellations and appointment failures, improve care and clinic decision-making, help practices grow, and allow users to access patient records from anywhere.

Introduction

Purpose of the Risk Assessment:
The objective is to conduct a simplified risk assessment for WebPT. Evaluate the potential impact of these risks on operations and user trust, and develop strategies to mitigate or manage these risks effectively, ensuring the confidentiality, integrity, and availability of patient data.

Scope of the Risk Assessment:
The risk assessment encompasses the main components of WebPT, including the web application, user authentication mechanisms, and data storage.

Assumptions:
We assume that the current network security measures are correctly implemented, all employees have undergone basic security training, and our software is up to date at the start of this assessment.

Stakeholders and the Resources:
Will solicit and incorporate feedback from all stakeholders, including the IT department, end-users, and senior management as part of the review process. I will need access to authentication logs and incident report logs to get a better understanding of the likelihood analysis.

Identify and Analyze Risks

Asset	Risk	Risk Rating	Threat	Vulnerability
Patient data (PII & SPII)	Data breach	Likelihood: Very likely (3) Impact: Very impactful (3) Risk rating: 9 - High	Unauthorized access into the system	SFA (password-authentication)
Backup Systems	Service disruption	Likelihood: Very likely	DoS attacks	Lack of traffic filtering, rate

		Impact: Somewhat impactful (2) Risk rating: 6 - Medium		limiting, and use of IDS/IPS

Risk - Data breach:
WebPT has access to patient PII (i.e., name, phone number, home address) and SPII (i.e., credit card information, health records, and driver's license number). Therefore, there is a risk of unauthorized access to information such as these due to potential vulnerabilities in the system. This website only utilizes password authentication as a login method and WebPT does not implement the principle of separation of duties so all users have admin-level access to PII and SPII. The threats to this risk being realized are malicious hijacking of user accounts, malware injection, and malicious insider actions. The likelihood of this risk occurring is very likely and the impact is very impactful.

Risk - Service disruption:
In the past, WebPT has had occurrences of service disruptions that took multiple hours to amend which disrupted payment transactions as well as the work efficiency of the rehab therapists. Additionally, there is a potential for technical failures or cybersecurity attacks. The threats to this risk being realized are DoS attacks, malware injection, and insecure APIs. The likelihood of this risk occurring is very likely and the impact is somewhat impactful.

Risk Prioritization:
Prioritizing the risk of a data breach should be the org's main focus because a threat event could be expected to have severe adverse effects on organizational operations, customers, or other organizations. After addressing this risk, WebPT should focus on the risk of service disruption.

<u>Recommendations</u>

Risk Mitigation - Data breach:
WebPT should implement MFA and RBAC to address this risk. Currently, WebPT implements password-authentication which provides a weak protection against external threat actors looking to gain unauthorized access into the system. MFA makes it harder for hackers to access accounts, even if passwords are compromised. Additionally, MFA can help prevent phishing, account hijacking, and other cyber attacks. WebPT should also implement RBAC because it limits access to information to only what is needed for a job, reducing the risk of data breaches and unauthorized access. Currently, WebPT allows for rehab therapists and their administrative staff to all possess admin level access to patient data. Rehab therapists do not need access to patients' credit card information for example so the risk of a data breach is high.

Risk Mitigation - Service disruption:
WebPT should implement security controls such as traffic filtering, IDS/IPS, and rate limiting. Currently, WebPT may have weak controls in place to mitigate these service disruptions as they occur pretty frequently. Additionally, WebPT should update its incidence response plan that should help with detecting, containing, and mitigating DoS attacks, including communication protocols with stakeholders.

Communicate Findings

This comprehensive risk assessment has illuminated several key cybersecurity risks associated with WebPT, including vulnerabilities to account hijacking, phishing attacks, and DoS attacks, among others. The report has outlined targeted mitigation strategies and action plans designed to address these vulnerabilities, enhance the system's security posture, and protect sensitive patient data.

Implementing the recommended risk treatment strategies is imperative to mitigate the identified risks effectively. The implementation of MFA and RBAC will ensure that WebPT can reduce the risk of data breach by strengthening the risk posture of the organization. Senior management's commitment and support are crucial for the successful execution of these initiatives, which are fundamental to safeguarding WebPT’s reputation, customer trust, and operational continuity.

As the digital landscape and threat environment continue to evolve, WebPT must remain vigilant, responsive, and proactive in its risk management efforts. This risk assessment should serve as a living document, regularly updated to reflect new insights, technological advancements, and changes in business operations or objectives.