VILKAS
CYBERSECURITY

Scoping Questionnaire

DOCUMENT DATE July 21, 2026

PREPARED FOR

Prysm Medical, Inc.

1000 Example Plaza
Suite 600
Raleigh, NC 27601

Elena Marlowe
Chief Information Security Officer

PREPARED BY

Vilkas Cybersecurity & Risk LLC

7901 4th St N
Suite 300
St Petersburg, FL 33702

Engagement Overview

Organization	Prysm Medical, Inc.
Billing address	1000 Example Plaza, Suite 600, Raleigh, NC 27601
Primary point of contact	Elena Marlowe, Chief Information Security Officer (919) 555-0142 elena.marlowe@prysmmedical.example.com
Secondary point of contact	Daniel Kim, IT Infrastructure Manager (919) 555-0176 daniel.kim@prysmmedical.example.com
Desired start date	2026-01-05
Required completion date	2026-02-06
Compliance requirements	Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS)
Special reporting requirements	Attestation Letter, Executive Level Presentation
Selected services	External Penetration Test (EPT), Internal Penetration Test (IPT), Web Application Security Assessment (WASA)
Additional details	Testing must avoid disruption to clinical operations.

Post-remediation testing: Post-remediation testing to confirm the effectiveness of the Client's corrective actions and updated security controls is included in all test scopes.

External Penetration Test (EPT) — Scope Summary

Performed from the perspective of an unauthenticated attacker on the internet to identify vulnerabilities and misconfigurations in the Client's internet-facing infrastructure, services, and applications. This assessment focuses on gaining initial access, demonstrating realistic attack paths, and evaluating the potential business impact of a compromise originating from the public internet.

Approximate live host count	35
Testing Parameters	
Assessment location	Remote
Testing time window	Business hours
Information disclosure	Blind
Evasive technique	Hybrid-Evasive

Internal Penetration Test (IPT) — Scope Summary

Performed from the perspective of an intruder or malicious insider on the Client's internal network. The objective is to determine the level of access an attacker may achieve once inside, including lateral movement, privilege escalation, and access to sensitive systems and data, given the Client's current security controls and configurations.

Approximate live host count	1000
Is Active Directory in scope?	Yes
Active Directory domains	2
Approximate user account count	1250
Approximate computer count	900
Network segmentation checks required?	No
Testing Parameters	
Assessment location	Remote
Testing time window	Business hours
Information disclosure	Semi-Blind
Evasive technique	Hybrid-Evasive

Web Application Security Assessment (WASA) — Scope Summary

Evaluates the security of in-scope web applications and their supporting components from both unauthenticated and authenticated perspectives. Testing focuses on application-layer vulnerabilities, configuration weaknesses, and business logic flaws, and includes scenario-based evaluation of role-based access controls (RBAC) for the Client's defined user roles.

Applications in scope	1
Application 1	
Description	PrysmConnect is a patient portal for managing appointments, secure messages, documents, and billing information. It includes role-based access for patients, providers, and billing staff.
Roles in scope for testing	3
API endpoints	150
Testing environment	Staging
Testing Parameters	
Assessment location	Remote
Testing time window	Business hours
Information disclosure	Semi-Blind
Evasive technique	Non-Evasive