VILKAS
CYBERSECURITY

2026 Network & Web Application Penetration Test

Rules of Engagement

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

Ben Rollin
Founder & CEO

Table of Contents

Statement of Confidentiality

The contents of this document are proprietary and confidential information developed by Vilkas Cybersecurity & Risk LLC ("Vilkas"). This document may not be shared with vendors, business partners, or contractors without prior written consent from Vilkas. No portion of this document may be reproduced, distributed, or disclosed without the written consent of both Vilkas and the Client.

This document does not constitute legal advice. The services described herein are not intended to provide legal counsel and should not be interpreted as such. Clients requiring legal guidance should consult with qualified legal counsel.

Purpose and Objectives

This Rules of Engagement ("RoE") establishes the authorized parameters for External Penetration Test, Internal Penetration Test, and Web Application Security Assessment services conducted by Vilkas Cybersecurity & Risk LLC ("Vilkas") on behalf of Prysm Medical, Inc. ("Client"). This document defines the scope, constraints, communication protocols, and acceptance criteria for all testing activities.

Objectives:

- Identify vulnerabilities and misconfigurations in Client systems and applications
- Validate the effectiveness of existing security controls
- Demonstrate realistic exploitation impact and attack chains
- Provide actionable remediation guidance aligned with industry best practices
- Support applicable compliance requirements: Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA)

All testing will be conducted within the constraints defined in this RoE to ensure safe, controlled, and legally authorized activity.

Scope of Testing

External Penetration Test Scope Summary	
Scope Detail	• Up to 50 external IP addresses (~35 live hosts expected) • Vilkas to perform external reconnaissance and Open-Source Intelligence Gathering (OSINT) to map out the Client's external footprint ◦ This data will be presented to Client to confirm ownership before external testing commences
Assessment Details	• Open-Source Intelligence Gathering (OSINT) to profile Client's external footprint (e.g., domains, subdomains, public code repositories, leaked credentials). • In-depth analysis of any in-scope web applications exposed externally. • Thorough testing of in-scope API and web service endpoints. • Testing of all in-scope, externally exposed services for known and emerging vulnerabilities.
Vulnerability Analysis	Automated external vulnerability scanning with manual validation and analysis of results.
Penetration Testing	Manual and automated external penetration testing to validate exploitability, lateral movement, and potential impact, subject to the agreed Rules of Engagement.
Compliance Requirements	Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act (HIPAA)
Testing Time Window	Business hours unless otherwise specified in the Rules of Engagement.
Assessment Location	Remote
Information Disclosure	Blind
Evasive Technique	Hybrid-Evasive
Flags/Objectives	Client will define any specific flags, objectives, or success criteria to be captured during testing and specified in the agreed Rules of Engagement.
Role-based Testing	Testing will be performed from the perspective of an unauthenticated user on the internet; additional authenticated roles (e.g., customer or partner portals) may be included where explicitly in scope.
Sensitive/Fragile Hosts	Client will provide a listing of any sensitive or fragile URLs, code packages, or application stack elements that require special handling as specified in the agreed Rules of Engagement.

Internal Penetration Test Scope Summary	
Scope Detail	• Up to 1,000 internal hosts across the Client's corporate network environment • 1 Active Directory forest comprising 2 domains: 1 parent domain and 1 child domain • 1 Microsoft Entra ID and Microsoft 365 tenant connected to the on-premises environment • Testing will begin from an unauthenticated internal network position and transition to authenticated testing using a standard domain user account if an initial foothold is not achieved within the agreed testing window
Assessment Details	• Internal reconnaissance to map out the internal network, including accessible servers, workstations, network devices, services, and applications.

	• In-depth analysis of the Client's Active Directory and relevant internal identity infrastructure from both unauthenticated and authenticated perspectives. • Testing from the perspective of an unauthenticated internal user (e.g., rogue device or intruder) and, where appropriate, a standard domain user if Vilkas is unable to obtain a foothold via unauthenticated testing. • Attempts to bypass or evade endpoint and network security controls in accordance with the agreed Rules of Engagement.
Vulnerability Analysis	Automated internal vulnerability scanning with manual validation and analysis of results.
Penetration Testing	Manual and automated internal penetration testing to validate exploitability, lateral movement, and potential impact, subject to the agreed Rules of Engagement.
Compliance Requirements	Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS)
Testing Time Window	Business hours unless otherwise specified in the Rules of Engagement.
Assessment Location	Remote
Information Disclosure	Semi-Blind
Evasive Technique	Hybrid-Evasive
Flags/Objectives	Client will define any specific flags, objectives, or success criteria to be captured during testing and specified in the agreed Rules of Engagement.
Role-based Testing	Testing will be performed from the perspective of an unauthenticated user on the internal network and a standard domain user.
Sensitive/Fragile Hosts	Client will provide Vilkas with a listing of any sensitive or fragile hosts as specified in Rules of Engagement.

Web Application Security Assessment (WASA) Scope Summary	
Scope Detail	• PrysmConnect Patient Portal and associated REST API ◦ 1 externally accessible web application and its supporting API endpoints ◦ Approximately 150 API endpoints • Testing of 3 user roles: Patient, Provider, and Billing
Assessment Details	• Testing will begin from the perspective of an unauthenticated remote user originating from the public internet or internal network, as applicable to the application's deployment. • Role-based testing will be performed for in-scope application roles (for example, standard user, administrator, and any additional claims-based roles) to validate authorization and access controls. • The assessment will evaluate the application, its supporting software stack, and interconnected components (such as databases, proxies, and load balancers) for vulnerabilities and misconfigurations.
Compliance Requirements	Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS)
Vulnerability Analysis	Automated vulnerability scanning with manual validation and analysis of results.
Penetration Testing	Manual and automated penetration testing to validate exploitability, lateral movement, and potential impact, subject to the agreed Rules of Engagement.
Testing Time Window	Business hours unless otherwise specified in the Rules of Engagement.
Assessment Location	Remote

Information Disclosure	Semi-Blind
Evasive Technique	Non-Evasive
Flags/Objectives	Client will define any specific flags, objectives, or success criteria to be captured during testing and specified in the agreed Rules of Engagement.
Role-based Testing (WASA)	Up to 3 roles in a staging environment that mirrors production.
Sensitive/Fragile Hosts	Client will provide Vilkas with a listing of any sensitive or fragile URLs, code packages, or application stack elements.

In-Scope Assets

Use the table(s) in Appendix A to add additional resources if needed.

External Penetration Test

Resource(s)	
198.51.100.0/27	203.0.113.0/28
192.0.2.50/32	192.0.2.51/32
prysmmedical.example.com	vpn.prysmmedical.example.com
mail.prysmmedical.example.com	remote.prysmmedical.example.com
securefile.prysmmedical.example.com	benefits.prysmmedical.example.com
connect.prysmmedical.example.com	community.prysmmedical.example.com

Internal Penetration Test

Resource(s)	
10.20.10.0/24	10.20.20.0/24
10.20.30.0/24	10.20.40.0/24
10.10.10.0/24	10.10.20.0/24
10.10.30.0/24	10.10.40.0/24
10.10.50.0/24	10.10.60.0/24
ad.prysmmedical.example.com	clinical.ad.prysmmedical.example.com

Web Application Security Assessment

Resource(s)	
staging.portal.prysmmedical.example.com	OpenAPI specification: https://staging-api.prysmmedical.example.com/openapi.json
REST API base URL: https://staging-api.prysmmedical.example.com/v1	

Out of Scope / Exclusions

List assets, networks, or systems that are excluded from testing for each assessment type. Insert additional rows as needed.

External Penetration Test

Resource(s)	
prysmmedical.example.com - third-party hosted website	careers.prysmmedical.example.com - third-party applicant-tracking platform

Internal Penetration Test

Resource(s)	
10.20.50.0/24	biomedical and IoT devices
10.20.60.0/24	medical imaging/laboratory systems
10.20.70.0/24	building management, environmental controls, badge access, and surveillance systems
10.20.80.0/24	guest wireless and unmanaged personal devices

Web Application Security Assessment

Resource(s)	
portal.prysmmedical.example.com – production URL	api.prysmmedical.example.com – production API

Sensitive or Fragile Systems

The following systems require special handling due to stability concerns, business criticality, or regulatory constraints:

System	Constraint	Handling
LEGACYBILL01.ad.prysmmedical.example.com (10.20.30.45)	Fragile legacy billing integration server	No automated vulnerability scanning. Manual validation only. Must coordinate testing during the approved maintenance window.
STG-DB01.ad.prysmmedical.example.com (10.20.30.60)	PrysmConnect staging database containing production-like schemas	Access only synthetic test records. Do not modify database configuration, perform bulk extraction, or retain complete database records in evidence.
HL7GATEWAY01.ad.prysmmedical.example.com (10.20.30.46)	Legacy clinical interface engine supporting HL7 message exchange with laboratory and billing systems	No automated vulnerability scanning.

Authentication, Access and Test Accounts

Client will provide the following access to support testing activities:

Access Type	Details	Delivery Method
Standard Domain User Account	vilkas2026	Secure portal
Patient web application user	patient.test@prysmmedical.example.com	Secure portal
Provider web application user	provider.test@prysmmedical.example.com	Secure portal
Billing web application user	billing.test@prysmmedical.example.com	Secure portal

All credentials and access details will be securely destroyed within 30 days of engagement completion, per Data Handling below.

Rules, Constraints, and Prohibited Actions

This section defines what Vilkas is authorized to do, what is off-limits, and how any sensitive data encountered will be handled. All activity remains subject to the scope defined above unless modified in writing by both parties.

Authorized Activities

Vilkas is authorized to perform the following against in-scope assets:

- Host discovery
- Vulnerability scanning (authenticated and unauthenticated)
- Manual penetration testing and exploitation of identified vulnerabilities
- Privilege escalation and lateral movement within scope
- Bypassing or evading security controls to demonstrate attack paths
- Offline password cracking
- Post-exploitation activities

Prohibited Activities

The following are prohibited unless explicitly authorized in writing by the Client:

- Denial-of-service (DoS) or distributed denial-of-service (DDoS) attacks
- Destructive testing, data corruption, or modification/deletion of production data
- Accessing, exfiltrating, or disclosing PII, PHI, or PCI data beyond what is necessary to demonstrate vulnerability impact
- Testing of out-of-scope systems or networks
- Social engineering campaigns
- Physical intrusion or facility access attempts

Data Handling

- Access to sensitive data (PII, PHI, PCI, confidential business information) will be minimized to what is necessary to demonstrate impact
- Any sensitive data encountered will be handled per the Client's data classification and retention policies
- No sensitive data will be removed from Client systems
- Credentials obtained during testing will be securely stored, encrypted, and destroyed within 30 days of engagement completion
- Screenshots and evidence will be redacted as necessary to protect sensitive information

Testing Schedule and Windows

Key Milestone Dates

Add or remove test-type columns to match the assessments authorized under this engagement:

Milestone	External Penetration Test	Internal Penetration Test	Web Application Security Assessment
Testing Window (Start – End)	01/12/2026-01/16/2026	01/12/2026-01/23/2026	01/12/2026-01/16/2026
Authorized Testing Days & Hours	Any	Mon–Fri, 8:00 AM–6:00 PM ET	Any
24x7x365 Scanning & Testing Authorized	Yes	No	Yes
Blackout / Restricted Dates	N/A	N/A	N/A
Kickoff Meeting	01/07/2026	01/07/2026	01/07/2026
Status / Midpoint Review	N/A	N/A	N/A
Draft Report Delivery	2/2/2026	2/2/2026	2/2/2026

Dates are subject to confirmation. Any changes will follow the change management process outlined in the SOW.

Emergency Stop ("Kill Switch")

If testing must be paused or stopped immediately, Client or Vilkas may invoke emergency stop procedures via phone or email to designated contacts.

Communication and Escalation

The following individuals serve as points of contact for this engagement, including emergency-stop coordination:

Team	Role	Name	Phone	Email
Vilkas	Project Manager	Maya Bennett	+1 813-555-0112	maya.bennett@vilkascyber.example.com
Vilkas	Primary Technical Contact	Ethan Cole	+1 813-555-0136	ethan.cole@vilkascyber.example.com
Vilkas	Account Executive	Laura Mitchell	+1 813-555-0174	laura.mitchell@vilkascyber.example.com
Client	Primary Point of Contact	Elena Marlowe	+1 919-555-0142	elena.marlowe@prysmmedical.example.com
Client	Secondary / Technical Contact	Daniel Kim	+1 919-555-0176	daniel.kim@prysmmedical.example.com
Client	Emergency Stop Contact	Rachel Foster	+1 919-555-0108	rachel.foster@prysmmedical.example.com

Communication Protocols

Status Updates:

- Frequency: As needed
- Method: Email/Slack
- Scheduled check-ins: N/A

Critical-Severity Findings

- Vilkas will immediately notify Client via email upon discovery of critical vulnerabilities requiring urgent attention
- Notification within 2 hours of discovery

Incident Handling

- If testing causes unintended service disruption, performance degradation, or system instability, Vilkas will immediately notify Client and cease related activities
- Client will notify Vilkas immediately if testing is detected by monitoring systems or if suspicious activity is observed

Physical/Virtual Testing Device

- Vilkas will provide a custom physical penetration testing device (Proxmox server running custom Linux and Windows VMs) for internal and wireless testing or a custom Linux virtual machine for internal testing as applicable
- Device will be shipped to Client facility or remote hands as coordinated
- Client will connect device to internal network per Vilkas instructions
- The following security controls are in place for physical devices, with the relevant controls also applied to provided custom virtual machines:
- Tamper-evident shipping packaging
- Full disk encryption (LUKS) for virtual machine storage
- Boot-level protection
- Remote wipe capabilities
- Communications over an encrypted peer-to-peer mesh via NetBird, which uses WireGuard-based encryption
- SSH key-based authentication to testing virtual machines. Root SSH login disabled
- Up-to-date base operating system and virtual machine images
- Up-to-date network infrastructure; routine vulnerability scanning and penetration testing against infrastructure and devices
- Strict access control and client device network isolation
- No internet-facing services; all traffic inside encrypted mesh
- NetBird access revoked, VM data securely wiped, and devices re-imaged before reuse

Monitoring, Detection and Incident Response Notification

Client Security Operations Center (SOC) / Monitoring:

- Client SOC/MSSP awareness level: Blind
- Detection validation: Testing will assess SOC/MSSP detection capabilities

Incident Response Coordination:

- If Client incident response team detects suspected malicious activity that may be related to authorized testing, they will contact Vilkas immediately before taking containment actions
- Vilkas will confirm whether activity is part of authorized testing within 1 hour of notification
- If testing triggers automated incident response (e.g., account lockouts, IP blocks), Client and Vilkas will coordinate resumption of testing

Third-Party Notifications

- Client is responsible for notifying third-party monitoring providers (SOC, MSSP, MDR) in accordance with contractual obligations
- Client has confirmed that notifications are not required

Acceptance and Approvals

By signing below, both parties acknowledge that they have read, understood, and agree to the terms and conditions set forth in this Rules of Engagement document. Testing activities will not commence until this document has been signed by authorized representatives of both parties.

Vilkas Cybersecurity & Risk LLC

By: _____

Date: _____

Name: Ben Rollin
Title: Founder & CEO

Prysm Medical, Inc.

By: _____

Date: _____

Name: Elena Marlowe
Title: Chief Information Security Officer

Appendix A

Use the table(s) below to record additional resources that must carry over into testing authorization (or were identified after proposal scope charts were finalized).

External Penetration Test

Resource(s)	

Internal Penetration Test

Resource(s)	

Web Application Security Assessment

Resource(s)	