Third Party Memorandum

Statement regarding the penetration test of MijnNoorderlicht patient portal

Date · 3 September 2026 Reference · TPM-2026-0147 Refers to report · CS-2026-0147, v1.1

To: whom it may concern
Re: Noorderlicht Zorggroep B.V. — penetration test MijnNoorderlicht

Purpose of this memorandum

This memorandum has been prepared by CyberScore B.V. at the request of the client and is intended for third parties — such as procurement officers, compliance officers, regulators and the client's customers — who wish to establish that an independent penetration test has been performed and what its outcome was. The document is self-contained and deliberately contains no technical details or descriptions of vulnerabilities.

This memorandum is not an assurance report within the meaning of ISAE 3000 or NOREA Guideline 3000 and does not replace the full penetration test report. That report is confidential and is held by the client. No conclusions other than the statement contained herein may be drawn from this memorandum.

The engagement

Client	Noorderlicht Zorggroep B.V.
Object of investigation	MijnNoorderlicht patient portal — web application, REST API and associated external infrastructure
Test type	Grey box, external, authenticated with two user roles (patient and care professional)
Standards framework	OWASP Web Security Testing Guide, OWASP Top 10, OWASP API Security Top 10, OWASP ASVS Level 2, PTES, NIST SP 800-115, CVSS 3.1
Test period	10 to 21 August 2026 · Retest: 1 September 2026
Performing tester	Thijs Vermeulen (CISSP, OSCP+), responsible for scoping, testing, reporting and retest
Independence	CyberScore is not involved in the development, management or hosting of the tested object.

Approach

The test was performed following a fixed, repeatable methodology in 6 phases. The environment was systematically examined for vulnerabilities; where possible, the actual impact was demonstrated within the agreed boundaries. The test concluded with reporting and a retest to verify remediation.

Results

Severity	At delivery	After retest	Status
Critical	1	0	Resolved
High	2	0	Resolved
Medium	2	1	In progress
Low	1	0	Resolved
Informational	1	1	Risk accepted
Total	**7**	**2**	

CyberScore: index score 0–100 based on the number and severity of open findings.

Following targeted remediation by the client and the retest on 1 September 2026, all critical and high findings have been resolved and verified. The CyberScore rose from 46 (Poor) to 96 (Excellent).

Statement

Based on the penetration test performed and the retest of 1 September 2026, CyberScore declares that on the retest date, within the scope of the engagement, no findings classified Critical or High remained in the tested object. All critical and high findings have been remediated by the client and verified by CyberScore by means of a retest. For the remaining finding classified Medium, the client has established a remediation plan with a planned resolution date of 30 September 2026.

Limitations and validity

- This memorandum is a snapshot as at the retest date, 1 September 2026.
- The statement is limited to the scope of the engagement.
- A penetration test provides no guarantee of the absence of vulnerabilities.
- Changes to the object after the retest date fall outside this statement.
- This statement is valid until one year after the retest date or until an earlier material change to the object.
- CyberScore recommends an annual retest.

Signature

Thijs Vermeulen
Senior penetration tester and director, CyberScore B.V. · CISSP, OSCP+

Place · Amersfoort
Date · 3 September 2026

The authenticity of this memorandum can be verified via **verificatie@cyberscore.nl** quoting reference TPM-2026-0147.
This memorandum may be shared by the client with third parties only in its entirety.