Touchpoints Healthcare Security

External Security Assessment

HIPAA-Focused Cybersecurity Analysis

Patient Portal Example

Target:	[redacted]
Scan Date:	December 24, 2025
Report ID:	THS-20251224-215121

43

HIGH RISK

23 Findings | 1 Critical | 1 High | Top Risk: Portal

Touchpoints Healthcare Security

Christopher Reaves | Security Assessment Professional

20 Years Military Healthcare Experience

chris@securetouchpoints.com | (619) 693-7437 | www.securetouchpoints.com

7130 E Hyatt St, San Diego, CA 92111

Executive Summary

Assessment for **Patient Portal Example** on December 24, 2025. Identified **23 findings**: 1 critical, 1 high-severity.

Risk Level: HIGH

■■ HIGHEST RISK AREA: Portal (100/100 - VERY HIGH RISK)

Metric	Value	Action Timeline
Risk Score	43/100	HIGH
Total Findings	23	See detailed section
Critical	1	24-48 hours
High Priority	1	1-2 weeks
Medium	13	30-60 days
Low/Info	8	Routine

Note: Risk score uses weighted scoring where critical security areas (Network Exposure, Data Leaks, SSL/TLS) have 2-2.5x impact compared to informational categories.

External Risk Assessment Matrix

This matrix evaluates external threats to ePHI confidentiality, integrity, and availability based on identified vulnerabilities. Overall likelihood of successful external exploit: MEDIUM. Potential impact if breached: MEDIUM to HIGH (ePHI exposure, OCR fines $100-$50,000 per violation, reputational damage, breach notification costs).

Likelihood ↓ / Impact →	LOW Impact	MEDIUM Impact	HIGH Impact
HIGH Likelihood	—	—	—
MEDIUM Likelihood	—	Missing Headers	Weak Encryption
LOW Likelihood	Infrastructure	—	—

Note: This matrix focuses on external attack vectors. A comprehensive HIPAA Security Risk Assessment must also evaluate internal threats, natural disasters, human error, physical security, and insider threats. This assessment contributes to but does not replace your complete risk analysis requirement under §164.308(a)(1)(ii)(A).

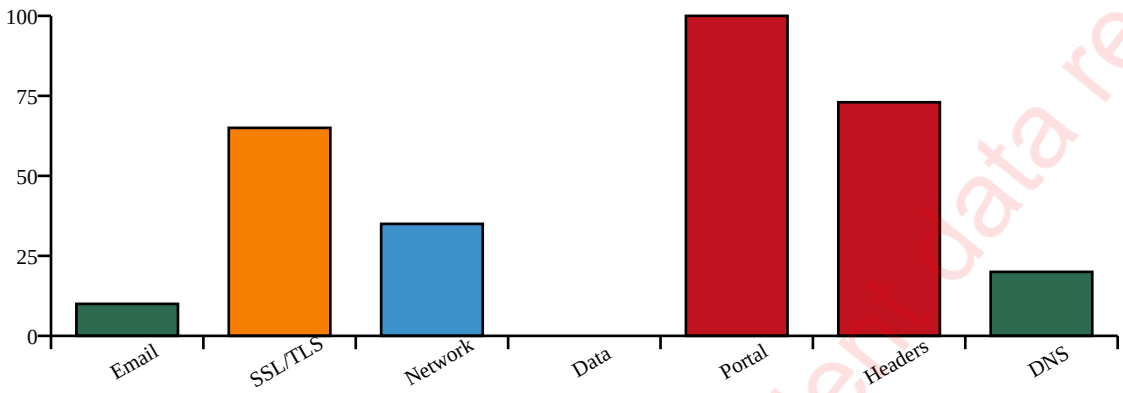
Individual Scanner Scores

Scanner Category	Score	Risk Level
Portal	100/100	VERY HIGH
Headers	73/100	VERY HIGH
SSL/TLS	65/100	HIGH
Network	35/100	MODERATE
DNS	20/100	LOW
Email	10/100	LOW
Data	0/100	LOW

***Note:** Scanner risk scores (0-100) measure the overall security posture of each category. Individual finding severities (Critical/High/Medium/Low) indicate the urgency of specific vulnerabilities. A scanner can have a high risk score without having any Critical severity findings.*

Risk Scores by Category

Higher scores indicate more risk. Colors: Red=Very High, Orange=High, Teal=Moderate, Green=Low.



IMPORTANT - ASSESSMENT SCOPE:

This external security assessment provides HIPAA Security Rule mapping for identified technical safeguards. It focuses on your internet-facing systems and their security posture.

This assessment provides:
- External security vulnerability identification
- HIPAA Security Rule requirement mapping
- Technical safeguard gap analysis
- OCR audit preparation documentation
- Contributes to your Security Risk Assessment

This assessment does NOT constitute:
- A complete HIPAA Security Risk Assessment (SRA)
- Internal network or systems assessment
- Administrative safeguards evaluation (policies, training, etc.)
- Physical safeguards evaluation (facility security, workstation controls)
- Business associate agreement review

A comprehensive HIPAA SRA requires assessment of internal systems, administrative controls, physical security, workforce training, policies, procedures, and business associate management in addition to this external technical assessment.

Use this report to: Document external security posture, support your risk analysis process (§164.308(a)(1)(ii)(A)), and prepare for potential OCR audits. Integrate findings with your internal risk assessment for complete HIPAA compliance documentation.

Legal Disclaimer: This report is for informational purposes only and does not constitute legal, compliance, or professional advice. Consult qualified legal counsel, HIPAA compliance professionals, and technical experts for implementation guidance specific to your organization.

HIPAA Security Rule Mapping

This table maps scanner risk scores to HIPAA Security Rule Technical Safeguards (45 CFR §164.312). Lower risk scores indicate better security posture for each requirement. **Note:** Mappings are interpretive based on external impacts and how vulnerabilities affect technical safeguard requirements.

Scanner Category	Score	HIPAA Requirement	Compliance Gap
Email Security	10/100 risk	§164.312(e)(1) Transmission Security	Low risk - Address during routine maintenance
SSL/TLS Configuration	65/100 risk	§164.312(e)(1) Transmission Security	High risk - Address within 30 days
Network Exposure	35/100 risk	§164.312(a)(1) Access Control	Moderate risk - Address within 60-90 days
Data Exposure	0/100 risk	§164.312(a)(2)(iv) Encryption and Decryption	No external issues found
Portal Security	100/100 risk	§164.312(d) Person or Entity Authentication	Very high risk - Immediate action required
Security Headers	73/100 risk	§164.312(c)(1) Integrity	Very high risk - Immediate action required
DNS Security	20/100 risk	§164.312(c)(1) Integrity	Low risk - Address during routine maintenance

Note: *Risk scores show external security posture only. Complete HIPAA compliance requires internal controls, administrative safeguards, physical security, workforce training, and documented policies. This assessment supports but does not replace your comprehensive Security Risk Assessment.*

External Compliance Gap Analysis

This analysis evaluates your external security posture against HIPAA Technical Safeguards requirements (§164.312). Gaps are prioritized based on risk to ePHI and potential regulatory impact to achieve maximum risk reduction.

Scan Limitations: This external assessment captures publicly visible security posture. Some findings may represent incomplete DNS records, firewall restrictions, or configuration variations rather than vulnerabilities. DNS errors and certain scan failures are noted but may require manual verification for complete accuracy. Internal systems, authentication mechanisms beyond login pages, and post-authentication session security are not assessed in this external scan.

HIPAA Category	Requirement Summary	Current Status	Gap Priority	Recommended Action
Access Control §164.312(a)	Unique user ID, emergency access, automatic logoff, encryption/decryption of ePHI	Gaps Found	**HIGH**	Close unnecessary ports; strengthen authentication; implement MFA; restrict access by IP
Audit Controls §164.312(b)	Hardware/software mechanisms to record and examine activity in systems with ePHI	COMPLIANT	LOW	Maintain audit controls; ensure log retention meets HIPAA requirements
Integrity §164.312(c)	Mechanisms to protect ePHI from improper alteration or destruction	Gaps Found	**MEDIUM**	Implement CSP, X-Frame-Options, X-Content-Type-Options; prevent directory listing; encrypt data at rest
Authentication §164.312(d)	Verify that person/entity seeking access to ePHI is who they claim to be	Gaps Found	**HIGH**	Strengthen authentication; implement MFA; enforce strong password policies; add account lockout
Transmission Security §164.312(e)	Guard against unauthorized access to ePHI during electronic transmission	Gaps Found	**HIGH**	Enable TLS 1.3; disable TLS 1.0/1.1; implement HSTS; use perfect forward secrecy; update certificates
Overall External Posture	Combined assessment of all external technical safeguards	**Partial Gaps**	**HIGH**	Address high-priority gaps first; see Prioritized Remediation Roadmap for detailed timeline

Gap Analysis Summary: This external assessment identified **3 high-priority** and **1 medium-priority** compliance gaps requiring attention. Prioritize remediation on Access Control, Authentication, and Transmission Security as these directly protect ePHI. All high-priority gaps should be addressed within 30 days to reduce regulatory risk and improve security posture.

OCR Audit Preparation Checklist

The Office for Civil Rights (OCR) enforces HIPAA compliance and conducts audits of covered entities. This checklist maps your external security assessment to common OCR audit elements. **Retain this report for 6 years** per HIPAA documentation requirements (§164.316(b)(2)(i)).

OCR Audit Element	Description	Status	Evidence in Report	Next Steps
Risk Analysis §164.308(a)(1)(ii)(A) *Required*	Conduct accurate and thorough assessment of potential risks/vulnerabilities to ePHI	Partial - External risks identified	• Risk Scores (Exec Summary) • Findings (Detailed section) • HIPAA Mapping	• Complete internal SRA • Document admin/physical controls • Update annually
Risk Management §164.308(a)(1)(ii)(B) *Required*	Implement security measures to reduce risks to reasonable/appropriate level	In Progress - Remediation plan provided	• Prioritized Roadmap • Remediation steps • Timelines by priority	• Implement fixes • Document completion • Re-scan to verify
Vulnerability Management *Best Practice*	Periodic assessments to identify security weaknesses	Compliant - External scan complete	• All findings with CVSS • Severity classifications • Detailed remediation	• Schedule quarterly scans • Track remediation • Maintain documentation
Transmission Security §164.312(e) *Addressable*	Implement technical security measures to guard ePHI transmission	Gaps Found	• SSL/TLS findings • Cipher analysis • Certificate review	• Implement TLS 1.3 • Disable old protocols • Enable HSTS
Access Controls §164.312(a) *Required*	Implement policies/procedures to allow access only to authorized persons	Gaps Found	• Network exposure findings • Port analysis • Authentication review	• Close unnecessary ports • Implement IP restrictions • Document firewall rules
Audit Controls §164.312(b) *Required*	Implement hardware/software/procedures to record/examine ePHI access	Partial - External capabilities assessed	• DNS security findings • Email authentication • Logging capabilities	• Enable comprehensive logging • Review logs monthly • Retain per policy (6 yrs)
Security Incident Procedures §164.308(a)(6) *Required*	Identify and respond to security incidents; mitigate harmful effects	Preparation - Vulnerabilities identified	• Baseline established • Risk priorities • Response guidance	• Develop incident response plan • Train staff • Conduct drills
Business Associate Oversight §164.308(b) *Required*	Obtain satisfactory assurances BAs will appropriately safeguard ePHI	Client Responsibility	N/A - Client manages BAAs	• Review BAAs with all vendors • Ensure scan vendor BAA on file • Audit BA compliance
Documentation & Policies §164.316 *Required*	Maintain written policies/procedures; document actions/activities	Partial - Assessment documented	• This complete report • Findings documentation • Remediation timelines	• Document all policies • Review annually • Train workforce • Retain 6 years

Priority Actions for OCR Audit Readiness:

1. **Immediate (1-30 days):** Address all CRITICAL and HIGH priority gaps from detailed findings
2. **Short-term (30-90 days):** Complete internal risk analysis for systems not in this external assessment
3. **Ongoing:** Document all policies, procedures, and workforce training; maintain for 6 years
4. **Annual:** Review and update BAAs; conduct security awareness training; update risk assessment
5. **Quarterly:** Re-scan external systems; review audit logs; test incident response procedures

Prioritized Remediation Roadmap

This roadmap organizes remediation activities by priority and provides realistic timelines for implementation. Focus on high-priority items first to achieve maximum risk reduction quickly. Dependencies are noted to ensure fixes are implemented in the correct order.

Priority Level	Count	Timeline	Estimated Effort	Dependencies	Responsible Party
CRITICAL (24-48 hours)	1 findings	Immediate action Complete within 2 days Document completion	4-6 hours total Varies by complexity	None - start immediately May require vendor	IT Administrator Security Team Management approval
HIGH (1-2 weeks)	1 findings	Week 1: Planning & procurement Week 2: Implementation & testing Verify completion	3-5 hours total Some may need vendor help	Complete after CRITICAL items Some interdependent	IT Administrator Web Developer Hosting Provider
MEDIUM (30-60 days)	13 findings	Days 1-30: Configuration changes Days 31-60: Testing & verification Document updates	26-39 hours total Mostly config changes	After HIGH priority complete Some config-dependent	IT Team External Vendors DNS Provider
LOW / ROUTINE (Ongoing)	8 findings	Address during routine maintenance No urgent deadline Schedule as capacity allows	8-16 hours total Minor adjustments	As time permits Low priority queue	Ongoing Maintenance IT Staff
OVERALL	**23 total findings**	**Phased approach over 90 days**	**23-92 hours total** Spread across team	Follow priority order Test after each phase	Cross-functional team IT + Management

Implementation Strategy & Best Practices:

1. Quick Wins First: Start with high-impact, low-effort items (typically security headers, DNS records). These provide immediate risk reduction and build momentum for larger projects.

2. Follow Dependencies: Some fixes must be completed before others (e.g., implement TLS 1.3 before enabling HSTS). Respect the dependency chain to avoid rework.

3. Test Thoroughly: After each fix, verify it works correctly and doesn't break existing functionality. Test in non-production first when possible. Use SSLLabs, SecurityHeaders.com, and other free tools.

4. Document Everything: Record all changes, configurations, and test results. This documentation is required for HIPAA compliance (§164.316) and invaluable for OCR audits. Include: what changed, when, who made it, why, and verification results.

5. Re-scan After Major Changes: Run follow-up external scans after completing each priority phase to verify fixes are effective and no new issues were introduced. This creates an audit trail of continuous improvement.

6. Prioritize by Risk, Not Ease: While quick wins are valuable, don't delay high-risk items just because they're difficult. Critical and high-priority findings directly impact ePHI security and HIPAA compliance.

Total Estimated Timeline: 23-92 hours of effort spread across 30-90 days. Actual timeline depends on team size, vendor responsiveness, and complexity of your environment. Budget extra time for testing, documentation, and unexpected issues.

Detailed Findings & Remediation

Plain-English explanations with step-by-step fixes.

■■ IMPORTANT - TEST BEFORE PRODUCTION:

Always test changes in a non-production environment first. Some configurations can cause service disruption if misconfigured:

- **HSTS:** Can lock out users if HTTPS breaks - only enable after confirming HTTPS works perfectly
- **TLS changes:** May break older client compatibility - test with actual users first
- **Firewall rules:** Can block legitimate access - verify before applying to production
- **DNS changes:** Propagation takes time - have rollback plan ready

Have rollback procedures documented before making changes. Monitor systems closely after deployment.

Note on Administrative Safeguards: Some findings reference §164.308 (administrative safeguards such as password policies and access procedures). While outside the scope of this external technical assessment, these recommendations support your overall HIPAA compliance program.

✓ IDENTIFIED STRENGTHS

- No external data leaks detected - ePHI not exposed in public repositories
- Email authentication partially configured - Basic anti-spoofing measures present
- DNS infrastructure shows reasonable security posture

CRITICAL SEVERITY

#1: Patient Portal Accessible via HTTP

What This Means: Patient portal accessible via unencrypted HTTP. Credentials and PHI transmitted in clear text.

Why This Matters: Patient credentials and health information exposed to interception. Man-in-the-middle attacks possible. Severe HIPAA violation. Mandatory breach notification likely required.

HIPAA: §164.312(e)(1) | CVSS: 9.8 (CRITICAL)

How to Fix:

Configure web server to redirect all HTTP to HTTPS

Implement HSTS header

Obtain valid SSL certificate if needed

Test all portal pages for HTTPS

Disable HTTP access completely

Conduct security incident assessment

HIGH SEVERITY

#2: Password Requirements Not Visible

What This Means: Password complexity requirements not displayed on login page. May indicate weak password policy or poor UX.

Why This Matters: Users may create weak passwords. Unclear security expectations.

HIPAA: §164.308(a)(5)(ii)(D) | CVSS: 7.5 (HIGH)

How to Fix:

Display password requirements on login/registration

Require: minimum 12 characters

Require: mix of upper, lower, numbers, symbols

Provide password strength indicator

Link to password policy

MEDIUM SEVERITY

#3: Email Digital Signature Missing (DKIM)

What This Means: DKIM adds an invisible signature to your emails proving they're really from you. Without it, your legitimate emails look suspicious.

Why This Matters: Your emails may be marked as spam or rejected. Email authentication fails. Phishing protection incomplete.

HIPAA: §164.312(e)(1) | CVSS: 5.3 (MEDIUM)

How to Fix:

1. Contact your email provider for DKIM setup instructions
2. Generate DKIM keys through your mail server
3. Add DKIM DNS record provided by your email service
4. Test using mail-tester.com or mxtoolbox.com
5. Verify emails now show 'Signed-by' header

Timeline: 1-2 hours | Your email provider will guide you

#4: Outdated Encryption Protocol

What This Means: Your website uses old encryption that was cracked years ago. It's like using a padlock that everyone has a key to.

Why This Matters: Patient data sent to your website can be intercepted. HIPAA requires current encryption. Fines range from $100-$50,000 PER RECORD if breached.

HIPAA: §164.312(e)(2)(i) | CVSS: 5.3 (MEDIUM)

How to Fix:

1. Contact your web hosting provider or IT team
2. Ask them to disable TLS 1.0 and TLS 1.1
3. Enable only TLS 1.2 and TLS 1.3
4. This is usually a simple server config change
5. Test at ssllabs.com after the change
6. Verify website still loads correctly

Timeline: 1-2 hours | Cost: Usually free

#5: Certificate Hostname Mismatch

What This Means: Certificate issued for admin.openemr.io but used on demo.openemr.io. Browsers will show warnings.

Why This Matters: Certificate validation errors. User trust issues.

HIPAA: §164.312(e)(2)(i) | CVSS: 5.3 (MEDIUM)

How to Fix:

Request certificate with correct domain

Consider wildcard certificate if needed

Install and verify

#6: Forward Secrecy Not Supported

What This Means: Cipher suite does not support Perfect Forward Secrecy (PFS). Past communications could be decrypted if private key is compromised.

Why This Matters: Reduced long-term confidentiality of encrypted communications.

HIPAA: §164.312(e)(2)(i) | CVSS: 4.3 (MEDIUM)

How to Fix:

Prioritize ECDHE and DHE cipher suites

Update server configuration

Test compatibility

#7: Port 22 Open - SSH Exposed

What This Means: SSH is remote access to your servers - like a back door to your office.

Why This Matters: Attackers use automated tools to guess passwords. If they get in, they control everything.

HIPAA: §164.312(a)(2)(i) | CVSS: 5.3 (MEDIUM)

How to Fix:

1. Use SSH keys instead of passwords (PRIMARY DEFENSE)
2. Require VPN before allowing SSH access
3. Add IP restrictions to only allow known locations

4. Optionally: Change from default port 22 (reduces automated scans)

5. Monitor SSH login attempts for suspicious activity

Timeline: 2-4 hours | URGENT - HIGH RISK

#8: HSTS Header Missing

What This Means: HSTS forces browsers to always use HTTPS. Without it, attackers can downgrade connections to HTTP.

Why This Matters: Man-in-the-middle attacks can strip HTTPS and intercept data. SSL stripping attacks succeed.

HIPAA: §164.312(e)(1) | CVSS: 4.3 (MEDIUM)

How to Fix:

1. TEST IN STAGING FIRST - HSTS can lock out users if misconfigured

2. Add header: Strict-Transport-Security: max-age=31536000

3. This forces HTTPS for one year

4. Only add after confirming HTTPS works perfectly on all pages

5. Can add includeSubDomains for extra security

6. Test at hstspreload.org

Timeline: 30 minutes

#9: Content Security Policy Missing

What This Means: CSP controls what resources your website can load. Without it, attackers can inject malicious scripts.

Why This Matters: Cross-site scripting (XSS) attacks easier. Malicious code can run on your site and steal user data.

HIPAA: §164.312(a)(2)(iv) | CVSS: 6.1 (MEDIUM)

How to Fix:

1. Start with basic CSP header

2. Example: Content-Security-Policy: default-src 'self'

3. Test and adjust based on your site's needs

4. Monitor CSP violation reports

5. Gradually tighten policy for better security

Timeline: 2-4 hours (testing required)

#10: Clickjacking Protection Missing

What This Means: Attackers can embed your login page in an invisible frame on their site and trick users into clicking.

Why This Matters: Users think they're clicking on safe site but actually entering credentials on attacker's page.

HIPAA: §164.312(a)(2)(iv) | CVSS: 4.3 (MEDIUM)

How to Fix:

1. Add header: X-Frame-Options: SAMEORIGIN
2. This prevents your site from being embedded in frames
3. Add to web server config or .htaccess
4. Test by trying to iframe your site

Timeline: 30 minutes

#11: X-Content-Type-Options Missing

What This Means: X-Content-Type-Options header not present. Prevents MIME type sniffing attacks.

Why This Matters: Browser may misinterpret file types, leading to script execution.

HIPAA: §164.312(a)(2)(iv) | CVSS: 5.3 (MEDIUM)

How to Fix:

Add X-Content-Type-Options header to web server configuration
Recommended value: nosniff
Test configuration
Verify header in browser developer tools

#12: X-XSS-Protection Missing

What This Means: X-XSS-Protection header not present. Enables browser XSS filtering (legacy, CSP preferred).

Why This Matters: Additional layer against XSS in older browsers.

HIPAA: §164.312(a)(2)(iv) | CVSS: 6.1 (MEDIUM)

How to Fix:

Add X-XSS-Protection header to web server configuration
Recommended value: 1; mode=block
Test configuration
Verify header in browser developer tools

#13: Permissions-Policy Missing

What This Means: Permissions-Policy header not present. Controls browser feature permissions.

Why This Matters: Limits browser APIs that third parties can access.

HIPAA: §N/A | CVSS: 5.3 (MEDIUM)

How to Fix:

Add Permissions-Policy header to web server configuration
Recommended value: geolocation=(), camera=(), microphone=()
Test configuration
Verify header in browser developer tools

#14: DNS Security Extensions Missing (DNSSEC)

What This Means: Your domain name system isn't cryptographically signed. Attackers can redirect your patients to fake websites.

Why This Matters: DNS poisoning attacks can send patients to attacker-controlled sites. They enter credentials on fake site, attackers steal them.

HIPAA: §N/A | CVSS: 5.9 (MEDIUM)

How to Fix:

1. Contact your domain registrar (GoDaddy, Namecheap, etc.)
2. Enable DNSSEC in domain settings
3. Your registrar will provide specific instructions
4. This is usually a checkbox in domain control panel
5. Test at dnssec-analyzer.verisignlabs.com

Timeline: 1-2 hours | Cost: Usually free

#15: Certificate Authority Authorization Missing (CAA)

What This Means: CAA records prevent attackers from getting fake SSL certificates for your domain.

Why This Matters: Without CAA, attackers can obtain legitimate SSL certificates for your domain and run fake versions of your site.

HIPAA: §N/A | CVSS: 5.3 (MEDIUM)

How to Fix:

1. Add CAA record to DNS
2. Example: 0 issue "letsencrypt.org"
3. This restricts certificates to your chosen provider only
4. Most DNS providers have CAA record option
5. Test at caatest.co.uk

Timeline: 30 minutes

LOW SEVERITY

#16: Password Autocomplete Not Disabled

What This Means: Password field does not disable autocomplete. Browsers may save patient portal passwords.

Why This Matters: Patient credentials may be stored in browser. Shared computer risk.

HIPAA: §164.312(a)(2)(i) | CVSS: 3.7 (LOW)

How to Fix:

Add autocomplete="off" to password field

Or use autocomplete="new-password"

Test browser behavior

#17: Account Enumeration Prevention

What This Means: Login should not reveal whether username/account exists. Cannot be tested without active authentication attempts.

Why This Matters: Attackers can identify valid patient accounts. Targeted phishing and social engineering. Privacy concern - confirms patient relationship.

HIPAA: §164.312(a)(2)(i) | CVSS: 3.7 (LOW)

How to Fix:

Use generic error messages

Return "Invalid username or password" for all failures

Same response time for valid and invalid users

No different behavior for existing accounts

Rate limit login attempts

Monitor for enumeration attacks

#18: Referrer-Policy Missing

What This Means: Referrer-Policy header not present. Controls referrer information sent to other sites.

Why This Matters: PHI in URLs may leak to external sites via referrer.

HIPAA: §164.512(e) | CVSS: 3.7 (LOW)

How to Fix:

Add Referrer-Policy header to web server configuration

Recommended value: strict-origin-when-cross-origin or no-referrer

Test configuration

Verify header in browser developer tools

#19: Server Version Disclosure

What This Means: Reveals web server type and version.: nginx/1.21.1

Why This Matters: Aids reconnaissance by revealing technology stack.

HIPAA: §N/A | CVSS: 3.7 (LOW)

How to Fix:

Configure web server to suppress Server

Or replace with generic value

Reduces information available to attackers

INFO SEVERITY

#20: No Login Rate Limiting or CAPTCHA

What This Means: Attackers can try unlimited login attempts. Automated tools can try thousands of passwords per minute.

Why This Matters: Brute force attacks will eventually crack weak passwords. No protection against automated attack tools.

HIPAA: §164.308(a)(5)(ii)(D)

How to Fix:

1. Add CAPTCHA after 3 failed login attempts
2. Implement account lockout after 5 failed attempts
3. Add 30-minute lockout period
4. Consider IP-based rate limiting
5. Send email alerts for multiple failed logins

Timeline: 4-8 hours (development time)

#21: Brute Force Protection Recommended

What This Means: Brute force protection should be implemented. This assessment cannot verify rate limiting without active testing.

Why This Matters: Without rate limiting, attackers can attempt unlimited login attempts. Credential stuffing attacks from breached password databases.

HIPAA: §164.308(a)(5)(ii)(D)

How to Fix:

Implement account lockout after 5-10 failed attempts
Lock account for 15-30 minutes
Implement exponential backoff
Use IP-based rate limiting
Monitor for credential stuffing patterns
Alert security team on multiple lockouts
Provide account unlock mechanism

#22: Multi-Factor Authentication Not Enabled

What This Means: Patient portal only requires username and password. If password is stolen, attacker has full access.

Why This Matters: One stolen password = access to patient records. With MFA, stolen passwords alone aren't enough.

HIPAA: §164.312(d)

How to Fix:

1. Enable MFA in your patient portal settings
2. Preferred: Authenticator app (Google/Microsoft Authenticator) per NIST guidance
3. Alternative: Email codes (SMS less secure due to SIM swapping)

4. Make MFA mandatory for all users

5. Provide instructions to patients on setting up MFA

6. Have IT support ready for patient questions

Timeline: 1 week (includes patient communication)

#23: Encrypted DNS Support

What This Means: DNS over HTTPS (DoH) and DNS over TLS (DoT) provide encrypted DNS queries. Recommend configuring if authoritative nameserver supports it.

Why This Matters: Encrypted DNS prevents eavesdropping on patient portal lookups. Protects against DNS snooping and manipulation.

HIPAA: §N/A

How to Fix:

Check if DNS provider supports DoH/DoT

Cloudflare, Google, Quad9 support encrypted DNS

Configure DoH/DoT if available

Educate users on encrypted DNS benefits

Scan Methodology

This assessment was conducted using industry-standard security scanning tools and techniques.

Scanner	Tools/Techniques	Purpose
Network Exposure	Nmap port scanning	Identify open ports and exposed services
SSL/TLS Configuration	SSL Labs API, OpenSSL analysis	Evaluate encryption strength and protocol support
Security Headers	HTTP header analysis	Check for protective HTTP response headers
DNS Security	DNS query tools, DNSSEC validation	Assess DNS configuration and security features
Email Security	SPF/DKIM/DMARC record checks	Verify email authentication mechanisms
Data Exposure	Web crawling, directory enumeration	Detect exposed files and sensitive data
Patient Portal	Authentication testing, session analysis	Evaluate login security and session management

Scan Date: *December 24, 2025*
Limitations: *External assessment only - does not include internal network scans, penetration testing, or social engineering. Non-invasive scanning methods used to avoid service disruption.*

References & Standards

This assessment is based on industry-recognized security standards and best practices.

Standard/Framework	Description	Relevance
HIPAA Security Rule (45 CFR §164.312)	Federal regulations for ePHI protection	Primary compliance framework
NIST SP 800-53	Security and Privacy Controls	Technical safeguard guidance
NIST SP 800-63B	Digital Identity Guidelines	Authentication best practices
NIST SP 800-52	TLS Implementation Guidelines	Encryption standards
OWASP Top 10	Web Application Security Risks	Common vulnerability framework
CIS Controls	Center for Internet Security Benchmarks	Security baseline configurations
CVE/CVSS	Common Vulnerabilities and Exposures	Vulnerability severity scoring
HHS OCR Guidance	Office for Civil Rights audit protocols	HIPAA enforcement standards

Security Terms Glossary

Quick reference for technical terms used in this report.

Term	Definition
BAA	Business Associate Agreement - Required contract for HIPAA compliance
CVE	Common Vulnerabilities and Exposures - Publicly known security flaws
CVSS	Common Vulnerability Scoring System - 0-10 scale for vulnerability severity
DKIM	DomainKeys Identified Mail - Digitally signs emails to prove authenticity
DMARC	Domain-based Message Authentication - Protects against email spoofing
DNSSEC	DNS Security Extensions - Prevents domain redirection attacks
Firewall	Security system that controls network traffic - like a security guard
HIPAA	Health Insurance Portability and Accountability Act - Protects patient data
MFA	Multi-Factor Authentication - Requires multiple proofs of identity
OCR	Office for Civil Rights - Federal agency that enforces HIPAA compliance
Phishing	Fraudulent emails or websites designed to steal information
Port	A network entry point - like a door to your building
RDP	Remote Desktop - allows remote computer control
SMB	File sharing protocol - often targeted by ransomware
SPF	Sender Policy Framework - Verifies mail servers sending email for your domain
SRA	Security Risk Assessment - Comprehensive analysis required by HIPAA
TLS/SSL	Transport Layer Security - Encrypts data between users and your website
XSS	Cross-Site Scripting - Malicious scripts injected into websites
ePHI	Electronic Protected Health Information - Patient data in electronic form

Need Help? Contact Us

Questions about implementing these fixes? We offer consultations, verification scans, and ongoing monitoring.

Contact	Details
Company	Touchpoints Healthcare Security
Professional	Christopher Reaves
Experience	20 Years Military Healthcare Experience
Certifications	PenTest+, Security+, CompTIA, BSCSIA, MSHCI
Email	chris@securetouchpoints.com
Phone	(619) 693-7437
Website	www.securetouchpoints.com
Address	7130 E Hyatt St, San Diego, CA 92111
Services	External Security Assessments
	Security Assessment Services
	Follow-up Verification
	Security Consulting