ChecklistGuro

Healthcare Patient Portal Access Checklist: Security & Usability

Patient Identity Verification

Ensuring accurate and secure patient identification before granting portal access.

Patient First Name

Write something...

Patient Last Name

Write something...

Date of Birth (Year)

Enter a number...

Date of Birth (Month)

Enter a number...

Date of Birth (Day)

Enter a number...

Gender

- [ ] Male
- [ ] Female
- [ ] Other
- [ ] Prefer not to say

Photo ID (e.g., Driver's License)

Upload File

Verification Method

- [ ] In-person verification
- [ ] Remote video verification
- [ ] Knowledge-based authentication

Authentication Methods

Reviewing and validating multi-factor authentication and password policies.

Primary Authentication Method

- [ ] Username/Password
- [ ] Multi-Factor Authentication (MFA)
- [ ] Biometric Authentication

MFA Type (if applicable)

- [ ] SMS OTP
- [ ] Authenticator App
- [ ] Email OTP
- [ ] Hardware Token

Minimum Password Length

Enter a number...

Password Complexity Requirements

- [ ] Uppercase Letter
- [ ] Lowercase Letter
- [ ] Number
- [ ] Special Character

Last Password Policy Review Date

Enter date...

Password Reset Procedure Documentation Link

Write something...

Access Control Permissions

Confirming appropriate access levels are assigned based on patient roles (e.g., patient, caregiver).

Patient Role Assignment

- [ ] Patient
- [ ] Caregiver
- [ ] Authorized Representative

Allowed Data Access

- [ ] Appointment Scheduling
- [ ] Lab Results
- [ ] Medication List
- [ ] Medical Records
- [ ] Billing Information

Appointment Scheduling Permissions

- [ ] View Only
- [ ] Request Changes
- [ ] Full Scheduling Access

Maximum Number of Caregivers

Enter a number...

Record Sharing Scope

- [ ] Patient Only
- [ ] Caregiver
- [ ] Authorized Representative

Data Encryption & Security

Verifying data encryption protocols both in transit and at rest within the portal.

Encryption Method Used (e.g., TLS 1.3, AES-256)

- [ ] TLS 1.2
- [ ] TLS 1.3
- [ ] AES-256
- [ ] Other (Specify in Long Text)

Encryption Key Rotation Frequency (days)

Enter a number...

Data Encryption at Rest?

- [ ] Yes
- [ ] No
- [ ] Partial (Specify in Long Text)

Description of Encryption Protocol Implementation

Write something...

Certificate Validation Status

- [ ] Valid
- [ ] Expired
- [ ] Revoked

Last Encryption Audit Date

Enter date...

Portal Usability & Accessibility

Assessing the portal's ease of navigation, clarity of information, and adherence to accessibility standards.

Navigation Clarity

- [ ] Very Clear
- [ ] Clear
- [ ] Somewhat Clear
- [ ] Unclear

Font Size Appropriateness

- [ ] Excellent
- [ ] Good
- [ ] Needs Adjustment
- [ ] Unreadable

Average Page Load Time (seconds)

Enter a number...

Accessibility Features Used (Select all that apply)

- [ ] Screen Reader Compatibility
- [ ] Keyboard Navigation
- [ ] Alternative Text for Images
- [ ] Color Contrast Options

Overall Ease of Use

- [ ] Extremely Easy
- [ ] Easy
- [ ] Neutral
- [ ] Difficult
- [ ] Very Difficult

Patient Privacy & Consent

Confirming patient understanding of privacy policies and obtaining necessary consent for data sharing.

Has the patient received a copy of the Privacy Notice?

- [ ] Yes
- [ ] No
- [ ] N/A

Brief summary of Privacy Notice explanation provided to patient.

Write something...

Does the patient understand how their data will be shared?

- [ ] Yes
- [ ] No
- [ ] Unsure

Patient Signature (acknowledging Privacy Notice and consent)

Date of Consent/Acknowledgement

Enter date...

Which data sharing categories has the patient consented to?

- [ ] Treatment Communication
- [ ] Payment Processing
- [ ] Research (optional)
- [ ] Care Coordination

Audit Logging & Monitoring

Reviewing audit logs for suspicious activity and ensuring adequate monitoring systems are in place.

Number of Audit Log Entries Reviewed

Enter a number...

Summary of Log Review Findings

Write something...

Severity of Identified Issues (if any)

- [ ] None
- [ ] Low
- [ ] Medium
- [ ] High

Date of Last Log Review

Enter date...

Time of Last Log Review

Audit Log Events Monitored

- [ ] Login Attempts
- [ ] Data Access
- [ ] Record Updates
- [ ] Password Changes
- [ ] Portal Configuration Changes

Number of Alerts Generated in Last Period

Enter a number...

Device Security & Compliance

Checking for device security protocols and compliance with organizational policies when accessing the portal.

Device Operating System

- [ ] Windows
- [ ] macOS
- [ ] Android
- [ ] iOS
- [ ] Other

Device Encryption Status (0 = Not Encrypted, 1 = Encrypted)

Enter a number...

Security Software Installed

- [ ] Antivirus
- [ ] Firewall
- [ ] Mobile Device Management (MDM)
- [ ] Endpoint Detection and Response (EDR)

Device Compliance Status

- [ ] Compliant
- [ ] Non-Compliant
- [ ] Pending Review

Last Security Scan Date

Enter date...

Notes / Comments on Device Security

Write something...

Training & Documentation

Ensuring staff have appropriate training on portal access procedures and maintaining accurate documentation.

Last Training Completion Date

Enter date...

Training Module Covered

- [ ] Portal Security Awareness
- [ ] Patient Privacy & HIPAA
- [ ] Usability & Navigation
- [ ] New Feature Updates

Number of Staff Trained

Enter a number...

Summary of Training Content

Write something...

Attach Training Certificates/Records

Upload File

Trainer Qualification

- [ ] Certified Healthcare Professional
- [ ] Designated Security Officer
- [ ] External Training Provider

Regular Security Assessments

Scheduling and conducting regular vulnerability scans and penetration tests.

Last Vulnerability Scan Date

Enter date...

Vulnerability Scan Score (e.g., CVSS)

Enter a number...

Scanning Tool Used

- [ ] Nessus
- [ ] Qualys
- [ ] Rapid7
- [ ] Other

Scan Report (PDF/CSV)

Upload File

Next Penetration Test Scheduled

Enter date...

Summary of Findings and Remediation Plan

Write something...