Audit Readiness Checklist – LVHN eKVM Remote Update

Version: 1.0 **Date:** 2025-11-11 **Purpose:** Pre-audit validation checklist for regulatory compliance (HIPAA, Joint Commission, SOC 2)

Configuration Custody Notice
Ionic Health engineering exclusively manages all eKVM configuration, firmware, and software changes. LVHN operations is solely responsible for provisioning, hardening, and maintaining the Windows jumper server environment. Any activity outside these custody boundaries requires written approval from both teams.

Network Visibility Scope
Compliance evidence focuses solely on LVHN-operated assets up to the jumper server; Ionic Health does not inspect the broader LVHN network.

Overview

Use this checklist to validate audit readiness **quarterly** or **prior to external audits**. Each section corresponds to common audit questions and required evidence.

Audit Scope: - Remote access controls for medical device updates - Data integrity and confidentiality safeguards - Audit trail completeness and retention - Incident response procedures

---

Section 1: Access Control

1.1 Account Management

- ☐ **Named Accounts Only:** Verify no shared/generic accounts used for remote access
  - **Evidence Required:**
    - Active Directory user list (filter: `*admin`)
    - Local account list on jumper server and eKVM devices
    - SIEM query: Event ID 4624 (successful logons) → filter for non-named accounts
  - **Validation Command:**
    ```
    Get-ADUser -Filter * | Where-Object {$_.SamAccountName -notlike "*.*"} | Select-Obj
    ```
- ☐ **JIT Access:** Confirm all privileged accounts are time-boxed (enabled only during change windows)
  - **Evidence Required:**

    - Change ticket dates/times vs. account creation/disable timestamps
    - Event ID 4720 (account created), 4726 (account deleted), 4725 (account disabled)
  - **Sample Size:** Last 3 change windows (minimum)
- ☐ **Password Policy:** Verify compliance with organizational password policy
  - **Policy Requirements:**
    - Minimum length: 14 characters
    - Complexity: Uppercase, lowercase, number, special character
    - Maximum age: 90 days
    - History: 24 passwords remembered
  - **Validation Command:**
    ```
    Get-ADDefaultDomainPasswordPolicy | Select-Object MinPasswordLength, PasswordHistor
    ```
- ☐ **MFA Enforcement:** Confirm multi-factor authentication required for all remote access
  - **Evidence Required:**
    - VPN authentication logs showing MFA prompts
    - PAM logs (if applicable) showing hardware token usage
    - Screenshots of MFA configuration in VPN/PAM system
  - **Test:** Attempt VPN login without MFA token (should fail)

1.2 Network Access Control

- ☐ **Network Segmentation:** Verify jumper server → eKVM access is isolated from other networks
  - **Evidence Required:**
    - Network topology diagram showing VLAN separation
    - Firewall rules (jumper IP → eKVM subnet)
    - Clinical network routing table (confirm no direct routes to maintenance VLAN)
- ☐ **Least Privilege Firewall Rules:** Confirm firewall permits ONLY jumper server IP to eKVM devices
  - **Evidence Required:**
    - Firewall rule export (Palo Alto: `show running security-policy`, Cisco: `show access-list`)
    - Rule review showing source IP = jumper server, destination = eKVM subnet, ports = 3389/5985/5986/445
  - **Test Command:**
    ```
    # From unauthorized workstation (should fail)
    Test-NetConnection -ComputerName ekvm-device-01 -Port 3389
    ```
- ☐ **Default Deny Policy:** Verify firewall default policy is deny-all (explicit allow required)
  - **Evidence Required:**

    - Firewall global policy showing default action = deny
    - Log sample showing denied connection attempts to eKVM from unauthorized sources

---

1.3 Session Management

- ☐ **Idle Timeout Configured:** Verify RDP sessions disconnect after 15 minutes of inactivity
  - **Evidence Required:**
    - Registry export: `HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services\MaxIdleTime`
    - GPO report: `gpresult /h gpresult.html` (section: Terminal Services)
  - **Test:** Establish RDP session, leave idle for 16 minutes, confirm disconnect
- ☐ **Session Logging:** Confirm all RDP/WinRM sessions generate audit logs
  - **Evidence Required:**
    - Event ID 21 (RDP session logon), 22 (shell start), 24 (disconnect), 25 (reconnect)
    - Event ID 4624 (logon Type 10 = RDP)
    - WinRM Event ID 6 (session created), 8 (session closed)
  - **Sample:** Last 10 RDP sessions from change windows

Section 2: Data Integrity

2.1 Binary Integrity Verification

- ☐ **SHA-256 Verification Documented:** Confirm every update includes hash verification at 3 stages
  - **Evidence Required:**
    - MOP section 5.3-5.6 (hash verification steps)
    - Evidence package: `01_Hashes_Pre_Transfer.txt`, `03_Hashes_Post_Transfer.txt`
    - PowerShell transcript showing `Get-FileHash` commands and output
  - **Sample:** Last 5 change tickets
- ☐ **Hash Mismatch Handling:** Verify process aborts on hash mismatch (no installation proceeded)
  - **Evidence Required:**
    - MOP rollback procedure (section 7)
    - Test scenario: Intentional hash mismatch → verify installation aborted
    - Incident report (if any real mismatch occurred)
- ☐ **Code Signing (Optional):** If applicable, verify Authenticode signatures validated

- **Evidence Required:**
  - PowerShell transcript showing `Get-AuthenticodeSignature` output
  - Certificate chain validation (issuer, expiration, revocation status)

2.2 Malware Scanning

☐ **AV/EDR Active:** Verify anti-malware software is running on jumper server and eKVM devices
- **Evidence Required:**
  - `Get-MpComputerStatus` output (Windows Defender) or EDR console screenshot
  - AV definition update date (must be <7 days old)
- **Validation Command:**

```
Get-MpComputerStatus | Select-Object AntivirusEnabled, AntivirusSignatureLastUpdate
```

☐ **Pre-Transfer Scanning:** Confirm all binaries scanned before transfer to eKVM
- **Evidence Required:**
  - Evidence package: `02_AV_Scan_Results.txt`
  - AV scan logs showing file path, scan result (no threats), timestamp
- **Sample:** Last 5 change tickets

☐ **Threat Detection Handling:** Verify process for handling detected threats
- **Evidence Required:**
  - MOP section on AV scan failure (abort installation, quarantine file, notify Ionic)
  - Test scenario: Simulate threat detection (EICAR test file) → verify abort

---

Section 3: Encryption and Confidentiality

3.1 Encryption in Transit

☐ **TLS 1.2+ Enforced:** Verify RDP and WinRM use TLS 1.2 or higher (no SSL 3.0, TLS 1.0, TLS 1.1)
- **Evidence Required:**
  - Registry export: `HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\`
  - RDP Hardening Guide validation script output
  - Network packet capture (Wireshark) showing TLS 1.2 handshake
- **Validation Command:**

```
Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\WinS
# Expected: SecurityLayer=2 (TLS), MinEncryptionLevel=3 (High/128-bit)
```

- ☐ **NLA Enabled:** Verify Network Level Authentication required for RDP
  - **Evidence Required:**
    - Registry: `UserAuthentication = 1`
    - RDP connection test from non-NLA client (should fail with error message)
  - **Validation Command:**

```
(Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\Terminal Server\Wir
# Expected: 1
```

- ☐ **Certificate Validity:** Verify TLS certificates are valid (not expired, trusted CA)
  - **Evidence Required:**
    - Certificate export: `Get-ChildItem Cert:\LocalMachine\My | Where-Object {$_.Subject -match "ekvm"}`
    - Certificate details: Issuer, NotBefore, NotAfter, Thumbprint
  - **Validation:** Cert expiration >30 days in future

3.2 Data Loss Prevention

- ☐ **Clipboard Redirection Disabled:** Verify clipboard copy/paste disabled during RDP sessions
  - **Evidence Required:**
    - Registry: `HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services\fDisableClip = 1`
    - GPO report showing policy applied
  - **Test:** Establish RDP session, attempt clipboard paste (should fail)
- ☐ **Drive Mapping Controlled:** Verify drive mapping disabled by default (enabled only during window if needed)
  - **Evidence Required:**
    - Registry: `fDisableCdm = 1` (baseline), `fDisableCdm = 0` (during window), `fDisableCdm = 1` (post-window)
    - Change ticket documenting GPO change schedule
  - **Validation:** Query registry before/after window
- ☐ **Printer/COM Port Redirection Disabled:** Verify unnecessary redirection disabled
  - **Evidence Required:**
    - Registry: `fDisableCpm = 1` (printer), `fDisableLPT = 1` (LPT port), `fDisableCcm = 1` (COM port)

Section 4: Audit and Accountability

4.1 Logging Completeness

- ☐ **Event Log Forwarding:** Verify logs forwarded from jumper + eKVM to SIEM

- **Evidence Required:**
  - SIEM ingestion dashboard showing log sources (jumper-server-01, ekvm-device-*)
  - Recent log entries (within last 15 minutes) for each source
- **Test:** Generate test event (failed login), query SIEM within 5 minutes

☐ **Event ID Coverage:** Confirm all required event IDs are logged
- **Required Event IDs:**
  - Security: 4624, 4625, 4634, 4672, 4688, 4776, 4778, 4779
  - RDP: 21, 22, 24, 25, 39, 40
  - PowerShell: 4103, 4104
  - WinRM: 6, 8, 142, 161
- **Evidence Required:** SIEM query results showing event count per ID (last 30 days)

☐ **Log Retention:** Verify logs retained for 6 years
- **Evidence Required:**
  - SIEM retention policy configuration screenshot
  - Archive storage location + retention schedule
  - Oldest available log timestamp (should be 6+ years if system operational that long)

☐ **Log Integrity:** Confirm logs protected from tampering (forwarded off-system, read-only)
- **Evidence Required:**
  - SIEM RBAC showing operators have read-only access
  - Event log channel config: `wevtutil gl Security` → MaxSize, Retention (overwrite as needed or archive)

4.2 Evidence Collection

☐ **Evidence Package Template:** Verify all change tickets include complete evidence package
- **Required Files per Section 8.3:**
  - 00_Metadata.txt
  - 01_Legal_Banner.png
  - 01_Hashes_Pre_Transfer.txt
  - 02_AV_Scan_Results.txt
  - 03_Hashes_Post_Transfer.txt
  - 04_Installation_Log.txt
  - 05_Service_Verification.txt
  - 06_Connectivity_Test.txt
  - 07_Windows_Event_Logs/*.evtx
  - 08_Screenshots/*.png
  - transcript-*.txt
- **Sample:** Randomly select 3 change tickets; verify all 10+ files

present

- ☐ **Evidence Accessibility:** Confirm evidence packages retrievable for audit
  - **Storage Location:** [Document management system path]
  - **Access Control:** [Who has access? Security team, compliance, auditors]
  - **Test:** Retrieve evidence for CHG0012345 within 5 minutes

---

Section 5: Change Management

5.1 Change Approval

- ☐ **Approved Change Tickets:** Verify all updates performed under approved change ticket
  - **Evidence Required:**
    - Change ticket status = "Approved" before execution window
    - CAB meeting minutes (if applicable)
  - **Sample:** Last 10 updates
- ☐ **Change Ticket Content:** Verify change tickets include all required fields
  - **Required Fields:**
    - Change number
    - Target device(s) (hostname, IP, location)
    - Update version
    - Scheduled window (start/end times)
    - Operator name(s)
    - Rollback plan reference
    - Business justification
  - **Sample:** Review 5 recent change tickets
- ☐ **Post-Implementation Review:** Verify change tickets closed with evidence attached
  - **Evidence Required:**
    - Change ticket status = "Closed Successful"
    - Work notes documenting outcome
    - Evidence package attached or linked
  - **Sample:** Last 10 change tickets

5.2 Configuration Management

- ☐ **Baseline Configurations Documented:** Verify hardening baselines exist and are current
  - **Required Baselines:**
    - Jumper server hardening guide
    - RDP hardening checklist
    - WinRM configuration checklist

    - Firewall rule templates
  - **Evidence Required:** Dated documents in `docs/` and `runbooks/` directories
- ☐ **Configuration Drift Detection:** Verify periodic validation of configuration compliance
  - **Evidence Required:**
    - Validation script: `Validate-RDP-Hardening.ps1` output (last run date)
    - Quarterly audit reports showing configuration compliance %
  - **Frequency:** Quarterly (minimum)

Section 6: Incident Response

6.1 Incident Detection

- ☐ **SIEM Alerting Active:** Verify SIEM alerts configured for security events
  - **Required Alerts:**
    - Event ID 4625 (>5 failed logins within 1 hour)
    - Unauthorized source IP attempting RDP/WinRM
    - SHA-256 hash mismatch
    - AV threat detection
    - Account lockout (Event ID 4740)
  - **Evidence Required:** SIEM alert rule list + recent alert history
- ☐ **Alert Response Testing:** Verify alerts trigger incident response
  - **Test Scenario:** Simulate failed login >5 times → confirm alert fires, IR team notified
  - **Evidence Required:** Test alert log + IR team acknowledgment email

---

6.2 Incident Handling

- ☐ **Rollback Procedure Documented:** Verify rollback steps exist and are tested
  - **Evidence Required:** MOP Section 7 (Rollback Procedure)
  - **Test:** Simulate rollback scenario (lab environment or tabletop exercise)
- ☐ **Escalation Path Defined:** Verify contact list current and accurate
  - **Evidence Required:** MOP Appendix C (Contact Information)
  - **Test:** Attempt to contact each escalation contact (email or phone)
- ☐ **Incident Reporting:** Verify security incidents reported to LVHN IT Security
  - **Evidence Required:**

    - Email notification to infosec@lvhn.org (if incident occurred)
    - Incident ticket in security incident tracking system
  - **Sample:** Last 12 months (if any incidents occurred)

Section 7: Vendor Management (Ionic)

7.1 Business Associate Agreement (BAA)

- ☐ **HIPAA BAA Executed:** Verify current Business Associate Agreement in place
  - **Evidence Required:**
    - Signed BAA document
    - BAA effective date and renewal date
    - Scope of BAA covers remote access to eKVM devices
- ☐ **BAA Terms Compliance:** Verify Ionic compliant with BAA terms
  - **Key Terms to Review:**
    - PHI access limitations
    - Incident reporting requirements (notify LVHN within 24 hours)
    - Audit rights (LVHN can audit Ionic compliance)
    - Data destruction upon termination

7.2 Security Assessments

- ☐ **Ionic Security Questionnaire:** Verify current security assessment on file
  - **Evidence Required:**
    - Completed security questionnaire (annual)
    - Ionic SOC 2 Type II report (if available)
    - Ionic HITRUST certification (if available)
- ☐ **Vulnerability Disclosure:** Verify Ionic notifies LVHN of vulnerabilities in eKVM software
  - **Evidence Required:**
    - Vulnerability disclosure policy
    - Past notifications (if any vulnerabilities discovered)

Section 8: Training and Awareness

8.1 Operator Training

- ☐ **Training Records:** Verify all operators trained on MOP procedures
  - **Evidence Required:**
    - Training attendance roster
    - Training materials (MOP presentation, runbook walkthroughs)

        - Training date (within last 12 months)
    - **Required Operators:** List all personnel performing updates
- ☐ **Training Content:** Verify training covers security and compliance topics
    - **Required Topics:**
        - MFA usage
        - JIT account provisioning
        - SHA-256 verification
        - Evidence collection
        - Rollback procedures
        - PHI handling (do not copy clinical data)
- ☐ **Competency Assessment:** Verify operators demonstrate competency
    - **Evidence Required:**
        - Hands-on lab exercise or dry-run
        - Supervisor sign-off on competency
    - **Frequency:** Annual refresher training

Section 9: Physical Security (If Applicable)

9.1 Jumper Server Physical Access

- ☐ **Physical Access Controls:** Verify jumper server in secured data center
    - **Evidence Required:**
        - Badge access logs to data center
        - Video surveillance (if applicable)
        - Visitor log (if applicable)
- ☐ **Environmental Controls:** Verify fire suppression, HVAC, UPS in place
    - **Evidence Required:** Facility assessment report or data center SLA

Section 10: Disaster Recovery and Business Continuity

10.1 Backup and Recovery

- ☐ **Jumper Server Backup:** Verify jumper server backed up regularly
    - **Evidence Required:**
        - Backup schedule (daily/weekly)
        - Last successful backup timestamp
        - Backup restoration test (annual)
- ☐ **Disaster Recovery Plan:** Verify DR plan includes jumper server rebuild procedure
    - **Evidence Required:**
        - DR plan document
        - RTO (Recovery Time Objective): 4 hours
        - RPO (Recovery Point Objective): 24 hours
    - **Test:** Annual DR exercise

Audit Readiness Score

Scoring: - **Green (Pass):** 95% of checklist items compliant - **Yellow (Warning):** 85-94% compliant (minor gaps) - **Red (Fail):** <85% compliant (significant gaps)

Current Score: _____ / _____ items compliant (**_____%**)

Remediation Plan (If Gaps Identified)

Item #	Gap Description	Remediation Action	Owner	Due Date	Status
Example: 1.1	Shared account "admin" found on ekvm-02	Disable shared account; create named JIT accounts	LVHN IT	2025-12-01	Open

---

Approval and Sign-Off

Audit Readiness Review Completed By:

Name	Role	Date	Signature
[Name]	LVHN Information Security	_____	_____
[Name]	LVHN Compliance Officer	_____	_____
[Name]	Ionic Quality Assurance	_____	_____

Appendix: Sample Audit Questions

Question 1: "How do you ensure that only authorized personnel can remotely access medical devices?" - **Answer Reference:** Section 1.1 (Named Accounts, JIT Access), Section 1.2 (Network ACLs), Section 1.3 (MFA)

Question 2: "How do you verify the integrity of software updates before installation?" - **Answer Reference:** Section 2.1 (SHA-256 Verification), Section 2.2 (Malware Scanning)

Question 3: "How do you protect patient data during remote access sessions?" - **Answer Reference:** Section 3 (Encryption in Transit), Section 3.2 (DLP - clipboard/drive redirection disabled)

Question 4: "How long do you retain audit logs, and how are they protected?" - **Answer Reference:** Section 4.1 (Log Retention: 6 years, SIEM off-system storage, read-only access)

Question 5: "What happens if a security incident occurs during a remote access session?" - **Answer Reference:** Section 6 (Incident Response), MOP Section 8.2 (Escalation Path)

Question 6: "How do you ensure operators are trained on security procedures?" - **Answer Reference:** Section 8 (Training Records, Competency Assessment)

Document Owner: LVHN Compliance + Ionic Quality Assurance **Last Updated:** 2025-11-11 **Next Review:** 2026-02-11 (Quarterly)

End of Audit Readiness Checklist