-= SERVICE REQUESTS =-

1. Account & Access Management

- **New Account Creation:**

Subject/Object: New physician, nurse, administrative staff, or visiting consultant account

Description: Create user credentials and basic access permissions for new healthcare staff members, including access to EHR (Electronic Health Records), PACS, medical devices, and department-specific applications based on role and clinical responsibilities.

Solution: Submit request through IT Service Portal at https://hospital-it.service-now.com/new-account with completed HR onboarding form #HR-2024. Include: full name, employee ID, department, role, supervisor approval, and required system access list. Accounts provisioned within 24 hours for standard roles, 48 hours for specialized clinical access. For urgent same-day access, contact IT Help Desk at (555) 234-5600 ext. 1 with manager approval.

- **Password Reset:**

Subject/Object: Locked or forgotten password for EHR, email, or clinical systems

Description: Unlock user account and reset password for healthcare staff who cannot access critical clinical systems. Priority given to clinical staff needing immediate patient care access. Includes verification of identity per HIPAA security protocols.

Solution: For immediate reset, call IT Help Desk 24/7 at (555) 234-5600 and verify identity with employee ID and date of birth. Self-service option available at https://password.hospital.org using personal mobile number or security questions. Temporary password expires in 24 hours. For locked accounts due to multiple failed attempts, 15-minute automatic unlock or call Help Desk for immediate unlock. Critical clinical staff receive priority response within 5 minutes.

- **Access Rights Modification:**

Subject/Object: Department transfer, role change, or additional system access for existing staff

Description: Modify user permissions when staff changes departments (e.g., nurse moving from ER to ICU), gets promoted (e.g., resident to attending), or requires temporary access to specialized systems (e.g., oncology nurse needing radiation planning system access).

Solution: Manager submits Access Change Request Form (ACR-100) via IT portal at https://hospital-it.service-now.com/access-change with business justification and approval from both current and new department heads. Standard processing: 2-3 business days. For clinical role changes requiring immediate access (e.g., code team assignments), supervisor calls (555) 234-5600 ext. 2 for emergency provisioning. Annual access reviews required per HIPAA compliance. Management at (555) 234-5610.

- **Account Deactivation:**

Subject/Object: Departing employee, rotating resident, or expired contractor account

Description: Disable all system access for terminated employees, completed rotations, or expired contracts to maintain HIPAA compliance and prevent unauthorized PHI (Protected Health Information) access. Includes removal from all clinical and administrative systems.

Solution: HR automatically triggers deactivation through employee termination workflow in Workday. Immediate access revocation occurs within 1 hour of HR notification. For early deactivation (security concern), manager emails security@hospital.org or calls (555) 234-5601. All access logs archived for 7 years per HIPAA retention policy. Equipment return coordinated with IT Asset Management at (555) 234-5610.

2. Software & Applications

- **Software Installation:**

Subject/Object: Clinical software, medical imaging viewers, dictation software, or specialized department applications

Description: Install hospital-approved applications such as DICOM viewers for radiologists, speech recognition software for physicians, patient monitoring applications for nurses, or specialized tools like EMR add-ons, pharmacy dispensing software, or lab result interfaces.

Solution: Verify software is on approved clinical applications list at https://hospital-it.intranet/approved-software. Submit installation request via IT portal including clinical justification and budget code. Standard installations completed within 3-5 business days. For urgent clinical need, supervisor emails IT-Clinical-Apps@hospital.org or calls (555) 234-5620. Unapproved software requires Clinical Applications Committee review (monthly meetings) - submit CAC request form at https://hospital-it.service-now.com/cac-request.

- **Software License Request:**

Subject/Object: Additional licenses for EHR modules, medical reference databases, or clinical decision support tools

Description: Request new or renewal licenses for clinical staff needing access to UpToDate, Lexicomp, specialized EHR modules (e.g., cardiology, oncology), PACS workstations, or other licensed medical software required for patient care or research.

Solution: Check license availability in Software Asset Management portal at https://hospital-sam.dashboard.com. Submit license request with department budget approval through procurement system. For immediate clinical need (e.g., consultant requiring UpToDate access), contact License Management at (555) 234-5625 or license-admin@hospital.org. Temporary 30-day licenses available for evaluation. License renewals automated 60 days before expiration with budget holder notification.

- **Software Upgrade:**

Subject/Object: EHR version update, medical device software, or operating system upgrade

Description: Upgrade clinical workstations to latest approved versions of Epic/Cerner/Meditech, update medical device software (ventilators, infusion pumps), or perform OS updates on clinical PCs while ensuring compatibility with medical equipment and minimizing disruption to patient care.

Solution: Major clinical system upgrades scheduled during quarterly maintenance windows (announced 60 days in advance). Individual workstation upgrades scheduled via IT portal - select preferred time slot at https://hospital-it.service-now.com/software-upgrade. Critical security patches deployed automatically after-hours. For urgent medical device software updates (FDA-required), contact Biomedical Engineering at (555) 234-5630. Test environment available at https://test.hospital-ehr.com for training before production upgrades.

- **Mobile App Deployment:**

Subject/Object: Mobile EHR app, secure messaging, or clinical reference apps on smartphones/tablets

Description: Configure and deploy mobile applications for physicians and nurses including mobile EHR access (Epic Haiku, Cerner PowerChart Touch), secure clinical messaging (TigerText, Vocera), medication references, or bedside documentation apps on hospital-issued iOS/Android devices.

Solution: Request hospital-issued mobile device through IT portal if not already assigned. Approved clinical apps auto-deploy via MDM (Mobile Device Management) within 1 hour of approval. For new app requests, submit to Clinical Mobility Team at mobile-apps@hospital.org with clinical use case. Personal device BYOD enrollment at https://hospital.maas360.com with manager approval. Technical support for mobile apps: (555) 234-5640. Lost/stolen device reporting (24/7): (555) 234-5911 for immediate remote wipe.

3. Hardware & Equipment

- **New Hardware Request:**

Subject/Object: Clinical workstation, COW (Computer on Wheels), medical tablet, or diagnostic equipment computer

Description: Provision new computers for nursing stations, physician workstations, mobile carts for bedside documentation, tablets for patient rounding, or dedicated PCs for medical imaging stations, lab systems, or pharmacy dispensing units.

Solution: Submit hardware request via IT Asset Portal at https://hospital-assets.service-now.com with department budget code and manager approval. Standard workstations delivered/installed within 5-7 business days. Rush orders (clinical urgency): contact IT Procurement at (555) 234-5650. Configure equipment preferences (monitor size, laptop vs. desktop) in request form. Ergonomic assessments available through Employee Health at (555) 234-5660. Equipment refresh cycle: workstations every 4 years, mobile devices every 3 years.

- **Hardware Replacement:**

Subject/Object: Failing clinical PC, broken COW, damaged medical tablet, or malfunctioning barcode scanner

Description: Replace non-functioning equipment critical to patient care including crashed workstations in ER/ICU, broken mobile carts used for medication administration, damaged tablets used for bedside charting, or failed barcode scanners for medication verification.

Solution: For failed equipment, immediately contact IT Help Desk at (555) 234-5600. Critical clinical areas (ER, ICU, OR) receive loaner equipment within 30 minutes while permanent replacement is ordered. Standard replacements: same-day for clinical workstations, next-day for administrative. Submit ticket at https://hospital-it.service-now.com/hardware-issue including asset tag number (located on device sticker). After-hours emergencies: page IT on-call at (555) 999-0123. Failed equipment returned to IT Asset Management for data sanitization and disposal.

- **Equipment Upgrade:**

Subject/Object: Increased memory for imaging workstation, faster processor for radiology reading station, or larger monitors for surgical planning

Description: Upgrade hardware to meet increasing clinical demands such as adding RAM to PACS workstations for faster image loading, upgrading CPUs in radiology reading rooms, or installing dual 4K monitors for detailed surgical planning and 3D reconstruction viewing.

Solution: Submit upgrade justification through department manager with clinical need documentation. Radiology workstation upgrades (RAM/monitors) approved by Imaging Informatics at imaging-it@hospital.org or (555) 234-5670. Standard approval process: 2-3 weeks. Budget must be confirmed before ordering. Schedule installation during low-volume periods via IT portal. For immediate performance issues affecting patient care, contact Help Desk for temporary solutions while upgrade is processed. Hardware specs published at https://hospital-it.intranet/hardwarestandards. Technical support: (555) 234-5640. Monthly device fees charged to department budget.

- **Mobile Device Provisioning:**

Subject/Object: Smartphones for on-call physicians, tablets for clinical rounds, or pagers for nursing staff

Description: Set up hospital-issued mobile devices including iPhones for attending physicians, iPads for bedside rounding and patient education, Android devices for specific clinical apps, or secure communication devices with appropriate clinical apps and secure messaging installed.

Solution: Clinical mobile devices requested through IT Mobile Device Portal at https://hospital-it.service-now.com/mobile-device with role-based justification. On-call physician phones provisioned within 24 hours. Device pickup at IT Service Desk (Main Hospital, 1st Floor, Room 105) Monday-Friday 7am-7pm. Setup includes: hospital email, secure messaging, mobile EHR, VPN profile, and MDM enrollment. Training resources at https://hospital-it.intranet/mobile-training. Technical support: (555) 234-5640. Monthly device fees charged to department budget.

- **Accessory Request:**

Subject/Object: Ergonomic peripherals, privacy screens, medical-grade keyboards, or mounting solutions

Description: Provide accessories for clinical workspaces including antimicrobial keyboards and mice for infection control, privacy filters for HIPAA compliance in public areas, ergonomic equipment for staff comfort, wall mounts for patient room monitors, or specialized input devices for radiology/pathology.

Solution: Standard accessories (keyboards, mice, cables) available immediately at IT Service Desk - no ticket required, exchange only. Specialized accessories (ergonomic equipment, privacy screens, medical-grade peripherals) requested via IT portal with department budget code. Infection Control-approved equipment list at https://hospital-it.intranet/ic-approved-equipment. Ergonomic assessments: contact Employee Health at (555) 234-5660. Wall mount installations: submit facilities request at (555) 234-5680. Accessory budget: $150/employee annually, manager approval required above this amount.

4. Network & Connectivity

- **VPN Access Request:**

Subject/Object: Remote access to EHR, on-call physician connectivity, or telehealth workstation setup

Description: Configure secure VPN access for physicians needing to review patient charts from home during on-call shifts, enable remote access for telemedicine consultations, or set up secure connections for administrative staff working remotely while maintaining HIPAA compliance.

Solution: Complete VPN Access Request Form at https://hospital-it.service-now.com/vpn-request with manager approval and HIPAA training certificate (complete at https://hospital.training/hipaa-annual). Install Cisco AnyConnect VPN client from https://vpn.hospital.org/downloads. Setup instructions emailed within 24 hours of approval. VPN credentials sync with network password. Technical support: (555) 234-5690. Two-factor authentication required via Microsoft Authenticator app. For urgent on-call access, supervisor calls (555) 234-5600 for same-day provisioning.

- **WiFi Access:**

Subject/Object: Guest WiFi for patients/visitors, clinical WiFi for medical devices, or secure WiFi for staff devices

Description: Provide WiFi credentials for patients and families (guest network), connect medical devices to clinical WiFi (telemetry monitors, infusion pumps), or enable staff personal devices on secure network while maintaining separation from clinical systems per security policies.

Solution: Staff: Use HospitalSecure network with network credentials. Guests: Patient/visitor WiFi credentials at registration desk or text "GUEST" to (555) 234-WIFI for automatic enrollment (valid 24 hours). Medical Devices: Contact Biomedical Engineering at (555) 234-5630 to register device MAC address and obtain clinical network credentials. BYOD: Enroll personal devices at https://hospital-byod.clearpass.com with manager pre-approval. Connection issues: forget/reconnect network or call Help Desk at (555) 234-5600. Network coverage maps at https://hospital-it.intranet/wifi-coverage.

- **Network Drive Mapping:**

Subject/Object: Department shared folders, medical imaging archives, or clinical documentation templates

Description: Connect users to network locations containing department protocols, shared patient education materials, nursing care plans, radiology teaching files, or standard clinical documentation templates used across departments while ensuring appropriate HIPAA access controls.

Solution: Network drives auto-map at login based on department membership. Missing drives: log off and back on to refresh group policy. Manual mapping instructions at https://hospital-it.intranet/drive-mapping or call Help Desk at (555) 234-5600. Common department shares: S:\ = Shared Department, H:\ = Home Directory (personal), P:\ = Clinical Protocols. Access issues: verify Active Directory group membership via IT Help Desk. New department share requests: submit to Network Storage Team at storage-admin@hospital.org with manager approval and estimated space requirements.

- **Printer Setup:**

Subject/Object: Label printers for pharmacy/lab, prescription printers, wristband printers, or document printers for medical records

Description: Configure specialized printers including pharmacy label printers for medication dispensing, lab specimen label printers, patient wristband printers for admissions, prescription printers in clinics, or secure printers for printing patient information with badge-release functionality.

Solution: Clinical printers auto-install via group policy when logging into workstations in that area. If missing: visit https://hospital-printers.printserver.com, search by location/floor, click "Install." Label/wristband printers: contact Biomedical Engineering at (555) 234-5630 for specialized driver installation. Prescription printers in clinics require DEA-compliant setup - call Pharmacy IT at (555) 234-5695. Secure/badge-release printers: tap badge on printer to release jobs. Printer not listed: call Help Desk at (555) 234-5600 with printer name/location. Supply orders: https://hospital-supplies.service-now.com.

- **IP Address Allocation:**

Subject/Object: Medical devices, imaging equipment, or clinical systems requiring static network addresses

Description: Assign static IP addresses to medical equipment requiring consistent network identity such as MRI/CT scanners, ultrasound machines, patient monitors, infusion pump servers, lab analyzers, or PACS storage systems to ensure reliable connectivity and integration with hospital information systems.

Solution: Submit static IP request to Network Engineering at network-admin@hospital.org including: device type, MAC address, department, business justification, and required VLAN (clinical/administrative/medical device). Medical device IPs: coordinate with Biomedical Engineering at (555) 234-5630 who maintains medical device network registry. Standard allocation: 3-5 business days. Emergency requests (new imaging equipment, urgent device deployment): call Network Operations Center at (555) 234-5700. Document IP assignments in hospital IPAM system at https://hospital-ipam.infoblox.com.

-= ISSUES =-

---

1. Performance & Functionality

- **Slow System Performance:**

Subject/Object: Clinical workstation sluggish during patient charting or medication administration

Description: Healthcare provider reports their computer is responding slowly when accessing EHR, documenting patient encounters, or scanning medications, potentially delaying patient care. May be caused by insufficient resources, background updates, or system resource conflicts affecting clinical workflow efficiency.

Solution: Immediate: Restart computer if not done in 7+ days, close unnecessary applications, check Task Manager (Ctrl+Shift+Esc) for high CPU/memory usage. If persists: Clear browser cache, run disk cleanup. Submit ticket at https://hospital-it.service-now.com/performance or call (555) 234-5600. IT will remote in to check: startup programs, pending Windows updates, antivirus scan conflicts, insufficient RAM (<8GB), full hard drive (>90%). Critical clinical workstations receive same-day response. May require hardware upgrade if device >4 years old. Temporary workstation available while issue resolved.

- **Application Freezing/Crashing:**

Subject/Object: EHR freezes during documentation, PACS viewer crashes while reading images, or pharmacy system becomes unresponsive

Description: Critical clinical application stops responding or closes unexpectedly during use, such as EHR freezing mid-documentation, radiology viewer crashing during diagnosis, or lab system hanging during order entry, interrupting clinical workflow and potentially impacting patient care delivery.

Solution: Immediate: Use Ctrl+Alt+Delete to end unresponsive application task, relaunch application. For EHR crashes: Unsaved documentation typically auto-recovers at next login - check "Recover Documents" link. Call Help Desk immediately at (555) 234-5600 if working on critical patient documentation. Submit ticket with: exact application name/version, error messages, what actions preceded crash. IT will check: application logs, Windows Event Viewer, conflicting software, corrupt user profile, insufficient system resources. May require: application reinstall, user profile rebuild, or software update. Known issues posted at https://hospital-it.statuspage.io.

- **Slow Citrix Speed:**

Subject/Object: Citrix-delivered clinical applications loading slowly or experiencing lag

Description: Healthcare staff experiencing delays when accessing EHR or other applications through Citrix virtual desktop, with slow screen refreshes, delayed mouse clicks, or sluggish typing response, affecting ability to efficiently document patient care or enter orders in real-time.

Solution: Immediate check: Internet speed test at https://speedtest.hospital.org (minimum 10 Mbps required). Close unused Citrix sessions at https://citrix.hospital.org/sessions. Remote users: Switch to wired connection if on WiFi, close bandwidth-heavy apps (streaming). Call Help Desk at

(555) 234-5600 if speed <10 Mbps or persistent lag. IT will check: Citrix server load (may move session to less busy server), network latency, VPN connection quality, receiver client version (update at https://citrix.hospital.org/receiver). Peak hour issues: Citrix team monitors at (555) 234-5705 and can scale resources. Alternative: thick client installation for frequent users.

- **Email Delays:**

Subject/Object: Clinical communications, lab results notifications, or urgent alerts arriving late

Description: Emails containing time-sensitive information such as critical lab results, patient transfer notifications, consultant recommendations, or urgent administrative communications are delayed, potentially affecting care coordination and timely clinical decision-making.

Solution: Check email server status at https://hospital-it.statuspage.io. For outbound delays: verify recipients received message (may be their server issue). For inbound delays: check junk/spam folders, verify sender not blocked. Critical clinical delays (lab results >15 min): call Help Desk at (555) 234-5600 and notify sender to use alternative contact method (phone/text page). Submit ticket including: time sent/expected, sender/recipient addresses, message subject. IT will check: mail queue, spam filter holds, mail routing rules, server performance. For urgent clinical communications: use secure text messaging via TigerConnect instead of email.

- **Print Quality Issues:**

Subject/Object: Prescription printouts, patient education materials, lab labels, or medical records printing poorly

Description: Printed materials showing faded text, streaks, or color problems affecting readability of prescriptions, patient instructions, medication labels, wristbands, or medical record printouts, potentially creating safety concerns if information is illegible.

Solution: Immediate: Check toner/ink levels (printer display panel), clean print heads (printer menu > maintenance > clean), verify correct paper type loaded. For streaks: wipe scanner glass. For faded prints: replace toner cartridge. Supplies ordered at https://hospital-supplies.service-now.com or call Supply Chain at (555) 234-5720. If quality issues persist with new toner: call Help Desk at (555) 234-5600 for service ticket. Biomedical Engineering services label/wristband printers at (555) 234-5630. For prescription printers: contact Pharmacy at (555) 234-5695. Critical print jobs: redirect to alternate printer listed at https://hospital-printers.printserver.com.

2. Connectivity & Access

- **Cannot Connect to VPN:**

Subject/Object: On-call physician unable to access EHR remotely or telehealth connection failing

Description: Healthcare provider working remotely or on-call cannot establish VPN connection to access patient records, review imaging studies, enter orders, or conduct telehealth visits, preventing them from providing remote patient care or responding to clinical consultations.

Solution: Immediate: Verify internet connection (browse non-hospital website), restart VPN client, toggle WiFi off/on. Ensure using correct VPN address: vpn.hospital.org. Common fixes: Update Cisco AnyConnect client from https://vpn.hospital.org/downloads, disable other VPN software, check firewall/antivirus blocking connection, verify network password not expired. Call Help Desk at (555) 234-5690 for urgent on-call access. IT will: verify account active, reset VPN profile, check MFA enrollment, test connection from their side. Alternative: Citrix remote access at https://citrix.hospital.org (web-based, no VPN needed). VPN status page: https://hospital-it.statuspage.io/vpn.

- **WiFi Connectivity Issues:**

Subject/Object: Mobile devices losing connection, medical equipment dropping off network, or COW experiencing intermittent WiFi

Description: Wireless connectivity problems affecting mobile clinical devices such as tablets losing connection during patient rounds, wireless telemetry monitors dropping signals, or nurses' mobile carts losing network connection during medication administration, disrupting real-time documentation and monitoring.

Solution: Immediate: Toggle WiFi off/on, forget network and reconnect, restart device, move closer to access point. Verify connecting to correct network (HospitalSecure for staff). Call Help Desk at (555) 234-5600 if issue persists. For medical devices: contact Biomedical Engineering at (555) 234-5630 immediately if patient monitoring affected. IT will check: device MAC address whitelisting, network authentication, access point health, device WiFi adapter drivers, IP address conflicts. May need to: re-register device, issue new credentials, install WiFi driver updates. WiFi coverage maps at https://hospital-it.intranet/wifi-coverage. For dead zones: submit coverage expansion request.

- **Cannot Access Shared Drive:**

Subject/Object: Department protocols, clinical templates, or shared patient education materials unavailable

Description: Staff member unable to access network folders containing critical resources such as clinical care pathways, standardized order sets, nursing protocols, patient education handouts, or department-specific documentation templates needed for patient care activities.

Solution: Immediate: Verify VPN connected if remote, check path spelling (case-sensitive), try accessing via UNC path: \hospitalfiles\departmentname. Log off and back on to refresh permissions. Call Help Desk at (555) 234-5600 if unable to access. Provide: exact drive letter or path, error message, department name. IT will verify: Active Directory group membership, share permissions, network connectivity to file server, drive mapping policy. May require: manager approval for access, addition to AD security group (24-48hr). Temporary solution: colleague can email needed files or grant guest access folder. Storage quota exceeded: contact storage-admin@hospital.org to increase allocation.

- **Login Failures:**

Subject/Object: Valid credentials rejected by EHR, PACS, or other clinical systems

Description: Healthcare provider can enter username and password but system refuses authentication despite correct credentials, preventing access to patient records or clinical applications. Different from password reset as credentials are known to be correct but system rejects them.

Solution: Immediate: Verify Caps Lock off, check typing correct username format (domain\username or firstname.lastname@hospital.org), try different device/browser. Do NOT repeatedly attempt (triggers account lock). Call Help Desk immediately at (555) 234-5600 - priority given to clinical staff. IT will check: account not disabled/expired, password not marked for change at next login, account not locked by security policy, system time sync issues, domain controller connectivity. May require: account unlock, password reset (if expired without notification), re-enable account, verify AD replication. For repeated issues: check with HR if employment status changed or security clearance issue.

- **Printer Not Found:**

Subject/Object: Prescription printer, label printer, or wristband printer not detected by clinical system

Description: Clinical workstation cannot locate or connect to required printer for patient care tasks such as printing prescriptions in clinic, generating medication labels in pharmacy, printing patient wristbands at registration, or producing lab specimen labels, halting critical workflow.

Solution: Immediate: Verify printer powered on and online (check printer display - should show "Ready"), restart print spooler (call Help Desk for instructions), try adding printer manually from https://hospital-printers.printserver.com. Call Help Desk at (555) 234-5600 if critical (prescriptions, labels). Provide: printer name, location, type of printer. IT will check: printer network connection, print server status, driver installation, group policy print mappings. For label/wristband printers: contact Biomedical Engineering at (555) 234-5630. Immediate workaround: identify alternate printer in area, redirect print jobs. May require: driver reinstall, print queue clear, printer IP address refresh.

3. Data & File Management

- **File Corruption:**

Subject/Object: Medical images not opening, clinical documents displaying errors, or research data files damaged

Description: Healthcare provider unable to open important files such as imported medical images, scanned patient documents, clinical research data, or exported reports showing corruption errors, preventing review of patient information or completion of clinical/research activities.

Solution: Immediate: Try opening on different computer, try older version of application, attempt file recovery tools built into application (Word: File > Info > Recover Unsaved Documents). Do NOT repeatedly open or save file (worsens corruption). Call Help Desk immediately at (555) 234-5600 if critical patient data. Provide: file location, file type, when last successfully opened. IT will attempt: file repair utilities, restore from shadow copy (previous versions), restore from backup (nightly backups retained 30 days). For DICOM images: contact PACS team at (555) 234-5670. Prevention: enable AutoSave/AutoRecover, save frequently, report system crashes immediately. If unrecoverable: document incident per policy and recreate if possible.

- **Missing Files:**

Subject/Object: Saved clinical templates, patient education documents, or department protocols disappeared

Description: Staff cannot locate previously saved files such as custom documentation templates, patient education materials they created, personal clinical reference files, or department-specific protocols, requiring recovery or recreation to continue clinical workflow.

Solution: Immediate: Check Recycle Bin, search entire computer using Windows search, check other common save locations (Downloads, Desktop, Documents). For network files: right-click folder > Properties > Previous Versions to restore deleted files (available up to 30 days). Call Help Desk at (555) 234-5600 for backup restoration request beyond 30 days (backups retained 90 days). Submit ticket at https://hospital-it.service-now.com/data-recovery with: approximate deletion date, file name, original location. Critical clinical documents: check EHR document repository for scanned copies. Prevention: save to network drives (H:\ or S:\) instead of local C:\ drive - only network locations backed up.

- **Storage Full:**

Subject/Object: User profile reaching capacity, preventing document saves or EHR screenshot storage

Description: Healthcare provider's network storage full, preventing them from saving clinical notes, screenshots of patient data for teaching, downloaded imaging studies for presentation, or personal clinical reference materials, requiring storage cleanup or expansion.

Solution: Immediate: Run Disk Cleanup (search Windows for "Disk Cleanup"), empty Recycle Bin, delete Downloads folder contents, clear browser cache. Check Outlook mailbox size (File > Info >

Cleanup Tools > Mailbox Cleanup) - archive old emails or delete large attachments. Call Help Desk at (555) 234-5600 if unable to free space. Submit quota increase request at https://hospital-it.service-now.com/storage-increase with business justification and manager approval. IT will analyze: largest folders/files, quota allocation (standard 50GB), move data to archive storage if appropriate. For clinical imaging: contact PACS team at (555) 234-5670 - do not store images locally. Receive low storage warnings at 80% and 90% capacity.

- **Email Attachment Problems:**

Subject/Object: Clinical documents, lab results, or medical images cannot be sent or received via email

Description: Staff unable to send or receive email attachments containing patient information (within HIPAA-compliant secure email), consult reports, meeting agendas, policy documents, or educational materials, affecting communication and information sharing across care teams.

Solution: Immediate: Verify attachment size <25MB limit, check recipient not blocking sender domain, try compressing file (right-click > Send to > Compressed folder). For files >25MB: upload to OneDrive/SharePoint and share link instead. Verify sending/receiving to hospital addresses uses secure email. Call Help Desk at (555) 234-5600 if persistent issues. Submit ticket with: attachment file type, size, error message. IT will check: spam filter holds, attachment type blocking policies (executables blocked), email routing rules, recipient mailbox full. For PHI: use secure file transfer at https://hospital-secure-share.org (up to 2GB files). Alternative: document sharing via EHR secure messaging.

4. Device & Hardware

- **No Sound/Audio Issues:**

Subject/Object: No audio from telehealth appointments, dictation software not hearing voice, or alert sounds not working

Description: Healthcare provider experiencing audio problems such as inability to hear patients during telehealth visits, dictation software not capturing spoken notes, or missing audible alerts for critical lab values or patient monitoring alarms, impacting patient care and clinical communication.

Display Problems:

Subject/Object: Radiology reading monitor flickering, external displays not detected, or resolution incorrect for imaging workstation

Description: Visual display issues affecting clinical work such as radiology monitors with unstable images making diagnosis difficult, dual monitors not working for surgery planning, or resolution problems making EHR text illegible, impacting ability to review patient information effectively.

Solution: Immediate: Check volume not muted (system tray speaker icon), verify correct output device selected (right-click speaker icon > Open Sound Settings > choose device), check physical connections (headphones plugged in fully). For USB headsets: try different USB port. Test with different application (YouTube) to isolate issue. For telehealth: call (555) 234-5640 immediately for troubleshooting. For dictation software: contact Clinical Documentation team at (555) 234-5645. Submit ticket at https://hospital-it.service-now.com if unresolved. IT will check: audio driver updates, Windows audio service running, device manager errors, hardware recognition. May require: driver reinstall, hardware replacement, audio adapter for older equipment.

- **Keyboard/Mouse Malfunction:**

Subject/Object: Clinical workstation input devices not responding during patient charting or order entry

Description: Keyboard or mouse at nursing station, physician workstation, or mobile cart not functioning properly, causing missed keystrokes, erratic cursor movement, or complete non-responsiveness, preventing efficient patient documentation and order entry.

Solution: Immediate: For wireless devices: replace batteries, check USB receiver connected, toggle power off/on. For wired devices: try different USB port, check for visible cable damage. Test on different computer to isolate device vs. computer issue. Exchange at IT Service Desk (Main Hospital, 1st Floor, Room 105) during business hours - no ticket needed. After-hours clinical emergencies: call Help Desk at (555) 234-5600 for immediate replacement delivery. For intermittent issues: update keyboard/mouse drivers, check USB power settings. Antimicrobial keyboards/mice available per Infection Control requirements. Ergonomic options available with Employee Health approval.

- **Battery Draining Quickly:**

Subject/Object: Mobile clinical tablet or laptop losing charge rapidly during patient rounds

Description: Battery-powered clinical device depleting much faster than normal, such as physician's tablet dying mid-rounds, nurse's mobile documentation device requiring frequent charging, or on-call laptop not lasting through shift, disrupting mobile clinical workflows.

Solution: Immediate: Check battery health (Windows: Settings > System > Battery), close unnecessary apps, reduce screen brightness, disable Bluetooth/WiFi when not needed. Verify power plan set to "Balanced" not "High Performance". For clinical tablets used on COW: contact Biomedical Engineering at (555) 234-5630 to check charging dock. Submit ticket at https://hospital-it.service-now.com/hardware if battery <2 hours life. Provide: device age, typical battery life vs. current. IT will check: battery health report, power-hungry applications, hardware issues. Battery replacement: devices <3 years old eligible for battery replacement, older devices replaced entirely. Loaner device available during repair. Keep devices plugged in when stationary.

- **Device Overheating:**

Subject/Object: Clinical workstation or mobile device running excessively hot during normal use

Description: Clinical computer, laptop, or tablet generating excessive heat during routine tasks such as EHR documentation or PACS image viewing, causing performance throttling, unexpected shutdowns, or physical discomfort for users, potentially indicating hardware failure risk.

Solution: Immediate: Shut down device and let cool 15 minutes, ensure air vents not blocked, place on hard flat surface (not soft surfaces blocking ventilation), check fan running (listen for noise). Do NOT continue using if excessively hot (burn risk/hardware damage). Call Help Desk at (555) 234-5600 for urgent replacement if clinical workstation. Submit ticket at https://hospital-it.service-now.com/hardware. IT will: test device temperature sensors, clean dust from fans/vents, check for hardware intensive processes, verify thermal paste integrity. May require: professional cleaning, fan replacement, device replacement if overheating caused by component failure. Do not use compressed air yourself (policy violation). Temporary replacement provided for clinical staff while device serviced.

-= PROBLEMS =-

---

1. Infrastructure & Systems

- **Recurring Network Outages:**

Subject/Object: Hospital wing or department losing network connectivity repeatedly

Description: Multiple areas of hospital experiencing repeated network disconnections affecting clinical systems, such as entire floors losing access to EHR, nursing stations unable to access pharmacy systems, or OR suites losing connection to imaging, representing systemic infrastructure problem requiring root cause analysis and permanent fix.

Solution: Escalate immediately to Network Operations Center (NOC) at (555) 234-5700 - 24/7 monitoring. NOC will: identify affected network segments, check switch/router health, analyze network logs for patterns, perform cable/port diagnostics. Submit formal incident report at https://hospital-it.service-now.com/major-incident for tracking. Network Engineering will: schedule comprehensive infrastructure assessment, replace faulty switches/routers, upgrade network firmware, implement redundant paths. Temporary solution: mobile hotspots for critical clinical areas. Major infrastructure projects escalated to IT Director at director@hospital-it.org. Post-incident review conducted to prevent recurrence. Network status updates at https://hospital-it.statuspage.io. Affected areas receive advance notification of remediation maintenance windows.

- **Server Performance Degradation:**

Subject/Object: EHR server, PACS archive, or lab system server running consistently slow for all users

Description: Backend clinical systems experiencing persistent performance issues affecting entire hospital, such as EHR server causing slow response times for all users, PACS storage system delaying image retrieval across all radiology workstations, or lab system server causing order entry delays hospital-wide.

Solution: Immediately escalate to Systems Engineering team at (555) 234-5710 and email systems-critical@hospital.org. Team will: monitor server resources real-time (CPU, RAM, disk I/O), identify resource-intensive processes, check database performance, analyze application logs. For EHR server: contact EHR vendor support (Epic/Cerner) concurrently for application-side investigation. Short-term solutions: restart services, clear cache, redistribute load across servers. Long-term fixes: hardware upgrades (additional RAM, faster storage), database optimization, application code improvements, implement load balancing. Schedule maintenance window for major fixes. Communicate planned downtime to clinical staff 7 days in advance via email and https://hospital-it.statuspage.io. Post-implementation performance monitoring for 30 days.

- **Email System Failures:**

Subject/Object: Hospital email server experiencing repeated crashes or outages

Description: Email infrastructure repeatedly failing causing hospital-wide communication disruptions, including delayed or bounced messages with critical lab results, consultant communications interrupted, or scheduled downtime notifications not delivered, affecting care coordination across departments.

Solution: Contact Messaging Team immediately at (555) 234-5715 or email-admin@hospital.org. Team will: check Exchange server status, verify mail flow between servers, analyze mail queue, review server event logs, test internal/external mail routing. For recurring outages: implement high-availability configuration with failover servers, increase server resources, optimize database, apply vendor patches. Temporary solution during outages: use TigerConnect secure messaging for clinical communications or alternative email addresses (@hospitalbkup.org). Schedule emergency maintenance if critical service restoration needed. Communication plan: status page updates every 30 minutes at https://hospital-it.statuspage.io, text alerts to leadership. Root cause analysis completed within 5 business days with prevention measures.

- **VPN Infrastructure Issues:**

Subject/Object: Remote access system repeatedly failing for on-call providers

Description: VPN infrastructure experiencing systemic problems preventing multiple remote physicians from accessing patient records, causing widespread connectivity drops during on-call coverage, or consistently slow performance for all remote users, indicating need for capacity increase or infrastructure upgrade.

Solution: Escalate to Network Security Team at (555) 234-5720 or vpn-admin@hospital.org. Team will: monitor VPN concentrator performance (concurrent users, bandwidth utilization, authentication latency), check VPN server health, analyze authentication server logs, test from multiple locations. For capacity issues: add VPN concentrators, increase bandwidth, implement load balancing across multiple VPN endpoints. For authentication issues: check RADIUS/MFA server connectivity, verify certificate validity. Temporary solution: Citrix web access at https://citrix.hospital.org (no VPN required). Communication: notify on-call physicians via text of alternatives, post status at https://hospital-it.statuspage.io. Consider split-tunneling to reduce VPN bandwidth. Capacity planning: upgrade infrastructure before reaching 80% utilization.

2. Security & Compliance

- **Multiple Failed Login Attempts:**

Subject/Object: Multiple accounts or systems showing suspicious authentication activity

Description: Security monitoring detecting repeated failed login attempts across multiple user accounts or from suspicious IP addresses, potentially indicating brute force attack, compromised credentials, or unauthorized access attempts to clinical systems containing PHI, requiring immediate security investigation and response.

Solution: Immediate response: Contact Security Operations Center (SOC) at (555) 234-5900 (24/7) or security@hospital.org. SOC will: identify affected accounts, review authentication logs, determine attack origin (IP addresses), check for patterns indicating brute force or credential stuffing. Actions: immediately block suspicious IPs at firewall, force password resets for targeted accounts, enable MFA if not active, temporarily lock high-risk accounts pending investigation. Notify affected users via phone (not email - may be compromised). Review: security event logs, correlate with other suspicious activity, check for successful breaches. Long-term: implement account lockout policies, deploy adaptive authentication, increase password complexity requirements. Incident documented per HIPAA security rule. Report to Security Committee and CISO. User awareness communication if widespread attack.

- **Malware Detection:**

Subject/Object: Virus or ransomware detected on clinical workstations or servers

Description: Antivirus or security systems identifying malicious software on hospital computers, potentially compromising patient data security, disrupting clinical operations, or spreading across network. Requires immediate isolation, remediation, and investigation of scope to protect PHI and maintain HIPAA compliance.

Solution: IMMEDIATE - DO NOT TURN OFF DEVICE: Call Security Operations Center (SOC) at (555) 234-5900 immediately. Disconnect network cable or disable WiFi if device still operational. SOC will: remotely isolate infected systems from network, initiate forensic investigation, identify malware type and scope, check lateral movement to other systems. For ransomware: activate incident response plan, contact ransomware response team, assess backup integrity, notify leadership immediately - do NOT pay ransom per hospital policy. Actions: quarantine/reimage affected systems, scan connected systems, restore from clean backups, apply security patches. Notify: HIPAA Privacy Officer if PHI potentially compromised, potentially notify HHS per breach notification rule. Post-incident: enhanced monitoring for 90 days, security awareness training for staff, update antivirus signatures, patch vulnerabilities. Incident report to executive leadership within 24 hours.

- **Phishing Attack Response:**

Subject/Object: Multiple staff reporting suspicious emails requesting credentials or containing malicious links

Description: Healthcare staff receiving phishing emails targeting hospital credentials, fake invoices, or impersonating executives requesting sensitive information. Multiple reports indicate organized attack requiring coordinated response to identify compromised accounts, educate staff, and implement protective measures.

Solution: Do NOT click links or download attachments: Forward suspicious email to phishing@hospital.org immediately, then delete from inbox/deleted items. Call Security Awareness Team at (555) 234-5905. Team will: analyze email headers/content, identify targeted users, check if credentials entered (if yes, immediate password reset required), scan for malicious links/attachments, trace email origin. Actions: quarantine/delete emails across organization via email admin, block sender domains, add URLs to web filter blocklist, force password resets for compromised accounts, monitor accounts for suspicious activity. Communication: security alert to all staff with screenshot of phishing email (training opportunity), post warning at https://hospital-it.intranet/security-alerts. If widespread attack: mandatory security awareness training for all staff. Report attempts to Anti-Phishing Working Group at reportphishing@apwg.org.

- **Data Breach Investigation:**

Subject/Object: Suspected unauthorized access to patient records or PHI exposure

Description: Evidence suggesting unauthorized viewing of patient records, potential PHI disclosure, lost/stolen devices containing patient data, or misconfigured system exposing protected health information. Requires formal investigation per HIPAA breach notification rules and potential regulatory reporting.

Solution: CRITICAL - IMMEDIATE ESCALATION: Contact HIPAA Privacy Officer at (555) 234-5950 and Security Officer at (555) 234-5955 immediately. Do NOT delete any logs or evidence. Privacy Office will: assemble breach response team, secure affected systems, begin formal investigation per breach protocol, document timeline of events. Investigation: determine what PHI accessed/disclosed, identify individuals affected, assess risk of harm, determine if breach meets reporting threshold (>500 individuals requires HHS notification, media notification). Concurrent IT investigation: how breach occurred, systems affected, remediation steps. Timeline: risk assessment completed within 48 hours, individual notifications if required within 60 days, HHS notification within 60 days for breaches >500 individuals. Actions: remediate security vulnerabilities, implement additional controls, provide credit monitoring if appropriate. Report to Board Risk Committee. Legal counsel engaged for potential liability.

- **Policy Violation Alerts:**

Subject/Object: Repeated alerts for inappropriate chart access or security policy violations

Description: Monitoring systems flagging patterns of policy violations such as staff accessing records of patients not under their care, sharing passwords, leaving workstations unlocked in public areas, or repeatedly violating security protocols, indicating need for retraining, policy enforcement, or disciplinary action.

Solution: Escalate to Compliance Office at (555) 234-5960 or compliance@hospital.org. Compliance will: review violation details, interview involved staff member, assess if willful neglect vs. inadvertent, determine appropriate corrective action. For inappropriate chart access: immediate supervisor notified, access logs reviewed (what records accessed, frequency, dates), potential disciplinary action per HR policy (verbal warning → written warning → termination based on severity/frequency). For technical violations (shared passwords, unlocked workstations): mandatory retraining, increased audit monitoring for 90 days. For repeated violations: escalate to HR for performance improvement plan or disciplinary action. System-level fixes: implement role-based access controls, enable auto-lock after 5 minutes idle, deploy privileged access management. Quarterly access audits per HIPAA requirements. Anonymous reporting available via Compliance Hotline at (555) 234-5965.

3. Application & Software

- **Software Connection Failures:**

Subject/Object: EHR unable to connect to lab system, pharmacy system losing connection to drug database

Description: Critical clinical applications repeatedly losing database connections or timing out, such as EHR unable to retrieve lab results, pharmacy system unable to check drug interactions, or medication administration system unable to validate orders, affecting patient safety and requiring urgent resolution.

Solution: Contact Application Support Team immediately at (555) 234-5730 or app-support@hospital.org. For EHR-related: also notify EHR vendor support (Epic/Cerner dedicated line). Team will: check application logs for connection errors, verify database server health, test network connectivity to database, check connection pool exhaustion, review recent changes.

Immediate fixes: restart application services, clear connection pools, verify service accounts not locked/expired, check firewall rules. If database issue: engage Database Administration team at (555) 234-5735 to investigate queries, locks, performance. For intermittent failures: implement connection retry logic, increase timeout values, add database connection monitoring. Critical systems: implement high-availability database clusters. Document incident at https://hospital-it.service-now.com/major-incident. Communication: post status updates at https://hospital-it.statuspage.io every 30 minutes until resolved. Post-resolution: root cause analysis within 5 business days.

- **Integration Failures:**

Subject/Object: PACS not syncing with radiology reporting system, EHR orders not reaching lab/pharmacy systems

Description: Healthcare system interfaces failing to exchange information properly, such as radiology images not displaying in dictation system, lab orders not transmitting from EHR to lab analyzers, or medication orders not reaching automated dispensing cabinets, disrupting clinical workflows and care coordination.

Solution: Escalate to Integration/Interface Team at (555) 234-5740 or interfaces@hospital.org. Team will: check interface engine (Rhapsody/Mirth) status, review interface queue for backed-up messages, analyze HL7 message errors, test interface endpoints. For PACS-RIS integration: contact Imaging Informatics at (555) 234-5670. For lab interfaces: notify Laboratory IT at (555) 234-5675. Investigation: review interface logs, verify sending/receiving system operational, check network connectivity between systems, test message mapping/translation. Immediate action: manually restart interface, reprocess failed messages, verify no duplicate transmissions. For critical failures (lab orders, medication orders): implement manual workaround (phone orders, paper backup) until interface restored. Long-term: implement interface monitoring/alerting, redundant interface engines, message persistence. Test interfaces after any system upgrades. Document resolution and update runbook at https://hospital-it.confluence/interfaces.

- **Licensing Conflicts:**

Subject/Object: Multiple users unable to access EHR module or clinical application due to license limits

Description: Concurrent user license limits reached preventing additional staff from accessing critical clinical systems during peak hours, such as all cardiology module licenses in use blocking other cardiologists, or PACS viewer licenses exhausted during high-volume diagnostic imaging periods.

Solution: Contact License Management at (555) 234-5625 or license-admin@hospital.org immediately. Team will: check current license usage dashboard, identify users consuming licenses (possibly idle sessions), review license allocation vs. actual need. Immediate solution: reclaim inactive sessions, log off users not actively using system, deploy temporary concurrent licenses if available. For critical clinical access: prioritize clinical staff over administrative users. Long-term: analyze usage patterns, request additional licenses with budget justification (submit to finance for approval), implement license harvesting (auto-logoff idle users after 30 minutes), deploy named user licenses for frequent users vs. concurrent for occasional users. Schedule license reviews quarterly. For EHR modules: work with clinical departments to optimize license allocation by shift/role. Emergency license procurement: contact vendor account manager for immediate temporary licenses (typically 30-day trial). Communication: notify department managers of license constraints, post guidance at https://hospital-it.intranet/license-management on proper logoff procedures. Dashboard at https://hospital-sam.dashboard.com shows real-time license availability by application.

- **Compatibility Issues:**

Subject/Object: Recent software update causing conflicts between clinical applications or medical device software

Description: Software updates creating incompatibilities affecting clinical operations, such as new EHR version breaking integration with lab system, Windows update preventing medical device software from launching, or updated PACS viewer unable to open older imaging studies, requiring compatibility restoration.

Solution: Escalate to Application Support Team at (555) 234-5730 and Change Management at (555) 234-5745. Team will: document what changed (Windows update, application upgrade, patch deployment), identify affected systems/users, test rollback feasibility. Immediate actions: halt further deployments, isolate affected systems, test in lab environment to reproduce issue. For medical device software: immediately contact Biomedical Engineering at (555) 234-5630 and device manufacturer. Solutions: apply vendor compatibility patches, roll back problematic update if safe, implement workaround configuration, deploy updated application version. For Windows updates causing issues: use WSUS to uninstall specific KB updates, block deployment to remaining systems. Testing: validate fix in test environment before production deployment. Communication: incident notification via https://hospital-it.statuspage.io, email department managers, document in known issues database. Prevention: enhanced change testing procedures, maintain compatibility matrix at https://hospital-it.confluence/compatibility, staged rollouts with pilot groups. Post-incident review within 10 business days.

- **Application Performance Bottlenecks:**

Subject/Object: Hospital-wide slowdowns in EHR, PACS, or other critical clinical systems during peak usage

Description: System-wide performance degradation affecting all users during high-demand periods such as morning rounds, shift changes, or emergency situations, indicating insufficient server capacity, database performance issues, or network bandwidth problems requiring infrastructure optimization or scaling.

Solution: During incident: Contact Application Support at (555) 234-5730 and Systems Engineering at (555) 234-5710 for emergency response. Teams will: monitor real-time server metrics (CPU, memory, disk, network), identify resource constraints, check active user count vs. capacity, analyze application logs for errors/slowness. Immediate relief: restart application services, scale up to additional servers if available, implement read-only mode if appropriate, clear application cache, kill runaway processes. For EHR: contact vendor support for application-side investigation concurrently. Executive escalation: if issue exceeds 2 hours or affects patient safety, notify CIO at (555) 234-5000 and Clinical Leadership.