Student:	Email:
Bradley Adams	badams10@my.athens.edu

Time on Task:	Progress:
	100%

Report Generated: Tuesday, April 1, 2025 at 12:27 PM

Guided Exercises

Part 1: Research Remote Access Policies

4. **Write** a **brief summary** of the information during your research. In your summary, focus on the key elements of the remote access policy. You should also identify any unique elements of remote access policies for higher education and healthcare institutions. Be sure to provide links to the remote access policies you identified in steps 2 and 3.

Key elements:

Purpose and Scope: Policies must clearly state the goal of protecting organizational resources from unauthorized use and potential harm, such as data loss, reputational damage, or compliance violations.

User Responsibility: All remote users are accountable for maintaining security standards equivalent to on-site usage, including safeguarding login credentials, preventing unauthorized access by others, and assuring compliant use of devices and software.

Access Control and Connection Protocols: Secure remote access must utilize VPNs and strong authentication methods. Users should not connect to other networks simultaneously unless they are under complete user control.

Endpoint Security: Devices connecting to the network, whether personal or corporate-owned, must have current antivirus software and firewalls and meet configuration standards. These conditions seek to prevent malware from penetrating the internal environment.

Compliance and Monitoring: Remote access policies are enforced through audits, monitoring, and penalties for violations, including termination of access or employment. Any exceptions must be formally approved.

Unique Elements:

Healthcare (Dayton Children's Policy):
Policies must comply with HIPAA regulations to protect patient health information. Specific procedures

govern the issuance of access credentials. Personal use of connected devices is strictly limited, and users must sign formal agreements acknowledging their responsibilities and the consequences of misuse.

Higher Education (St. John's University Policy):
Due to the academic ecosystem, policies often reflect an open and collaborative nature. A higher education policy allows for broader access with strong governance through role-based controls. Remote access must support administrative and student access, adding complexity and balancing flexibility with security.

In sectors like healthcare and education, policies get tailored to address industry-specific threats, legal obligations, and usage.

References:

https://www.childrensdayton.org/sites/default/files/Remote%20Access%20Policy%20%284%29.pdf

https://www.stjohns.edu/my-st-johns/human-resources/policy-910-remote-access-policy

Part 2: Create a Remote Access Policy

2. **Identify** a security control or countermeasure to mitigate each risk and threat identified in the Remote Access Domain. These security controls or countermeasures will become the basis of the scope of the Remote Access Domain policy definition to help mitigate the risks and threats commonly found within the Remote Access Domain.

Unauthorized Remote Access
Implement a VPN solution that requires MFA to prevent unauthorized users from accessing internal systems remotely. The VPN must use SSL/TLS encryption and support client certificates and TOTP. This control aligns with GLBA's Safeguards Rule. A SIEM will monitor connection logs and assist with incident response.

Unencrypted Data Transmission
Enforce end-to-end encryption using TLS 1.3 or higher for all remote communication protocols and disable legacy or insecure protocols. Protocol configurations must be verified through regular scans using vulnerability assessment tools.

Weak Authentication
Strengthen authentication with a centralized Identity and Access Management (IAM) solution that enforces Role-Based Access Control (RBAC). Users are granted only the minimum permissions necessary for their job functions. Integrate with Active Directory based on user roles, device posture, and location.

A Lack of Monitoring Remote User Activity

Implement remote session recording and logging to maintain accountability and detect abnormal behavior. Configure alerting for unusual behavior, such as access outside business hours or large data transfers.

Phishing or Malware Introduced Through Remote Endpoints
Implement DNS filtering, email security gateways, and user awareness training to counteract phishing and malware threats. Secure DNS filtering services should block connections to known malicious domains. Email security tools should scan attachments and links for threats. Employees must receive regular training, including phishing simulations, to help identify social engineering attacks.

Internet Misuse and Data Leakage During Remote Access
Deploy a web proxy with integrated data loss prevention to prevent data exfiltration and inappropriate content access during remote sessions. Proxies can enforce content filtering policies and restrict access to non-business-related sites. DLP rules should monitor and block the transmission of sensitive data over web traffic or email.

Lack of Policy Enforcement on Remote Users
Create and enforce a Remote Access Acceptable Use Policy (AUP) to provide a consistent security posture. This policy must prohibit personal use of company systems and IT assets, especially during remote sessions. Regular policy reviews and acknowledgments are mandated for compliance.

Inadequate User Training on Secure Remote Access
The organization must mandate Security Awareness Training for all new and existing hires. This training should cover remote work best practices, secure use of company systems, recognizing phishing attempts, and GLBA-specific data protection requirements. Employees shall complete awareness training during onboarding and repeat it annually.

Policy Statement
Define your policy verbiage.

Policy Statement

Healthwise Health Care ensures the confidentiality, integrity, and availability of electronic protected health information (ePHI) accessed remotely across its distributed healthcare network. To support its mission of delivering high-quality patient care through regional clinics, in-home services, and mobile health operations, the organization permits remote access to critical systems and medical records over the public Internet.

This policy establishes the mandatory technical, administrative, and training requirements for secure remote access to Healthwise systems and data. All remote access activities must comply with the Health Insurance Portability and Accountability Act (HIPAA), related federal and state regulations, and Healthwise's internal security standards.

Remote access is permitted only through approved, secure technologies and must be used exclusively for authorized clinical and operational purposes. All individuals granted remote access privileges must complete required security awareness training and adhere to all procedures and controls defined in this policy.

Purpose/Objectives

Define the policy’s purpose as well as its objectives and policy definitions

Purpose

This Remote Access Policy establishes a formal framework for the secure use of remote access technologies that enable authorized Healthwise Health Care personnel, including remote clinic staff, mobile nurses, and hospice caregivers, to access electronic protected health information (ePHI) and other critical healthcare systems via the public Internet. This policy assures compliance with the Health Insurance Portability and Accountability Act (HIPAA) Security Rule and protects the confidentiality, integrity, and availability of Healthwise's digital assets and patient information.

Objectives

Ensure Secure Access: Provide a secure remote access solution that prevents unauthorized use of Healthwise systems and patient data.

Protect ePHI: Enforce encryption, authentication, and endpoint security controls to safeguard all ePHI accessed or transmitted over public networks.

Maintain Regulatory Compliance: Adhere to HIPAA Security Rule requirements for remote access, focusing on access controls, audit controls, and transmission security.

Standardize Remote Access Mechanisms: Define approved remote access technologies such as VPNs, secure web portals, and endpoint configurations.

Monitor and Audit Activity: Require system logging, audit trails, and real-time monitoring of all remote access sessions.

Mandate User Training: Ensure that all remote users receive initial and ongoing security awareness training focusing on HIPAA, ePHI protection, and remote work preventative practices that maintain the health and security of their systems, devices, and data.

Policy Definitions

Remote Access: Any technology enabling users to connect to Healthwise's internal systems or access ePHI outside a Healthwise-managed facility.

Authorized User: Any employee, contractor, or third party granted explicit permission to access Healthwise systems remotely for business purposes.

Electronic Protected Health Information (ePHI): Individually identifiable health information transmitted or maintained electronically as HIPAA defines.

Endpoint Device: Any computing device that initiates a remote connection to Healthwise's network or applications.

Scope

Define whom this policy covers and its scope. What elements, IT assets, or organization-owned assets are within this policy's scope?

Scope

This policy applies to all authorized individuals remotely accessing Healthwise Health Care's information systems, networks, or electronic protected health information (ePHI). This policy applies to but is not limited to:

Full-time and part-time employees
Contractors
Temporary staff
Third-party service providers
Remote clinicians, nurses, hospice staff, and administrative personnel

This policy applies to all remote access activities initiated from outside Healthwise-controlled physical locations, including access over the public Internet from:

Private residences
Mobile work environments
Third-party healthcare locations
Regional or satellite clinics

Scope Elements and Assets

The following IT and organization-owned assets and elements are within the scope of this policy:

Electronic Health Record (EHR) systems and patient management platforms that are accessible via VPN or secure web applications.

Healthwise's VPN infrastructure and any associated remote connectivity technologies.

Secure web-based portals that are used to access ePHI, patient records, and clinical documentation.

Cloud-based services containing patient data and/ or internal communications.

Email systems and internal messaging tools used with remote work.

Authorized endpoint devices used for remote access.

Audit logging and remote access monitoring systems.

Standards

Does the policy statement point to any hardware, software, or configuration standards? If so, list them here and explain the relationship of this policy to these standards. In this case, Remote Access Domain standards should be referenced, such as encryption standards and VPN standards; make any necessary assumptions.

Standards

This policy adheres to technical and security configuration standards for deploying and managing remote access technologies within Healthwise Health Care. These standards provide for the secure transmission, access, and handling of ePHI and other sensitive organizational data over public and untrusted networks.

All remote access technologies must meet or exceed the following minimum standards:

Encryption Standards

All remote access connections must use strong encryption algorithms for data in transit and data at rest. These standards enforce HIPAA Security Rules for secure data transmission and securing ePHI. The following encryption standards apply:

*Transport Layer Security (TLS) version 1.2 or higher for all web-based remote applications.
*IPsec VPNs shall be configured to use AES-256 encryption and SHA-2 hashing.
*Full-disk encryption using AES-256 for all laptops and mobile devices that store or process ePHI.
*Legacy or insecure protocols are explicitly prohibited.

VPN Standards

Healthwise's VPN infrastructure must meet the following configuration standards:

*Support for Multi-Factor Authentication.
*Session idle timeouts set to 15 minutes of inactivity.
*Device compliance checks via endpoint validation.
*VPN clients must support TLS 1.2+ and use certificate-based authentication with username/password combinations.

Authentication Standards

To support HIPAA's access control requirments, all remote access must meet the following:

*Password requirements must comply with NIST SP 800-63B:
  - Minimum 12-character passwords
  - Blocklist checks for breached credentials
  - No periodic expiration without cause
*All remote access systems must require MFA using at least two of the following:
  - Something you know
  - Something you have

- Something you are
- Something you obtain

Endpoint Security Standards

*Operating Systems must be patched with the latest security updates.
*Antivirus and EDR tools must be installed and centrally managed.
*Personal Firewalls must be enabled on all remote devices.
*USB and external storage ports must be disabled or monitored through device control policies.

Logging and Monitoring Standards

*Logs must capture:
- User ID
- Source IP
- Accessed systems
- Timestamp
- Session duration

*Logs must be:
- Stored securely for a minimum of six years.
- Forwarded to a central SIEM for real-time monitoring.
- Protected against unauthorized access, alteration, or deletion.

Procedures

Explain how you intend to implement this policy for the entire organization.

Procedures

The IT Department, Information Security Team, and all designated system administrators shall follow the following procedures:

User Access Provisioning

Access Request and Approval
* All users requiring remote access must submit a formal request.
*The request must include:
  - Justification for remote access
  - Specific systems or applications required
  - Type of device(s) to be used
*Requests must be approved by the user's supervisor and the ISO.
*Upon approval, the IT department will:
  - Configure user accounts with role-based access control.
  - Enable MFA.
  - Assign users to appropriate access groups.

User Training Completion Requirement
*Before access is granted, users must:
  - Complete mandatory Remote Access Security Awareness Training.
  - Acknowledge the AUP and HIPAA data handling requirements.

Device Validation and Configuration

Endpoint Compliance Check
*All devices used for remote access must:
  - Be owned or approved by Healthwise.
  - Pass security validation

Device Hardening and Monitoring
*The IT team will:
  - Install and configure EDR agents on all endpoints.
  - Enforce disk encryption, host firewalls, and secure boot controls.
  - Disable unnecessary services such as telnet.

VPN Deployment and Access Control

VPN Configuration
*AES-256 encryption
*TLS 1.2+ tunnels
*Device compliance checks
*MFA enforcement

Session Controls
*Timeouts after 15 minutes of inactivity
*Device and location-based restrictions

Logging and Monitoring

System Logging Configuration
*logs capturing user ID, IP, session time, and resource access.
*Forward logs to the central SIEM

Log Review and Audit
*Logs will be reviewed:
- Daily for abnormalities.
- Monthly for compliance reporting.

*Suspicious or unauthorized access attempts will be escalated immediately to the Incident Response Team.

User Training and Policy Enforcement

Initial and Ongoing Training
*All employees with remote access rights must:
- Complete HIPAA-focused Remote Access Security Training before access is granted.
- Complete annual refresher training.

Policy Violation Handling
*Violations of this policy will be:
- Escalated to HR and Compliance as needed.
- Subject to disciplinary action

Policy Change Management
*Any procedural changes must be:
- Reviewed by the Information Security Governance Team
- Communicated to affected users
- Accompanied by updated training material

Guidelines

Explain any roadblocks or implementation issues that you must overcome in this section and how you will surmount them per defined guidelines. Any disputes or gaps in the definition and separation of duties responsibility may need to be addressed in this section.

Guidelines

Implementing a secure, HIPAA-compliant remote access policy across a distributed healthcare environment presents operational, technical, and administrative challenges. The following guidelines provide practical guidance for overcoming common implementation concerns and resolving potential conflicts.

Device Ownership and BYOD Challenges

Issue:
Due to convenience or resource constraints, many mobile nurses, hospice staff, or temporary contractors may prefer using their personal devices for remote access.

Guideline:
Healthwise will adopt a restricted BYOD policy, allowing access only to approved devices compliant with baseline security standards.

*Personal devices that fail to meet compliance requirements will be denied access.
*Healthwise will issue corporate-owned secure mobile endpoints to remote roles that require such devices.

Internet Connectivity and Infrastructure Gaps

Issue:
Remote branches and in-home care locations may have unreliable or insecure Internet connections, which can risk encrypted communication.

Guideline:
Healthwise will standardize always-on VPN clients that automatically connect and verify endpoint compliance upon startup.
*Staff operating in areas with poor network infrastructure will receive mobile hotspot devices preconfigured with VPN tunneling.

Training Compliance and Resistance

Issue:
Staff may view security training as burdensome or may not prioritize HIPAA security requirements.

Guideline:
HR will integrate training into onboarding and performance reviews to confirm participation and accountability.
*Interactive, role-specific training modules will increase relevance and engagement.

*Failure to complete the training will temporarily suspend the user's remote access privileges until the training is completed.

Logging, Privacy, and Workforce Concerns

Issue:
Some employees may raise concerns about privacy or the scope of monitoring on their remote sessions or personal devices.

Guideline:
Healthwise will communicate that:
*Logging is limited to business activity on Healthwise systems and is required for HIPAA compliance.
*Personal activities are not monitored unless performed on corporate devices, which violates policy.

Legacy Systems or Incompatible Applications

Issue:
Some applications used by remote branches may not support modern VPNs or encryption standards.

Guideline:
The Information Security team will develop a modernization plan to:
*Identify legacy systems via a remote access asset inventory.
*Work with vendors to bring software into compliance with Healthwise's Remote Access and Encryption Standards.

Challenge Exercise

Use the internet to find information about remote access policies and home network protection, and then use this information to create a training document for remote employees.

Healthwise Remote Access Guide

1. Securing Your Home Network
2. Safely Accessing Healthwise Systems While Traveling
3. Ongoing Security Best Practices
4. What to Do If You Suspect a Security Incident

Secure Your Wi-Fi Router

*Change Default Credentials
- Log into your router and change the default admin username and password.

*Enable WPA3 or WPA2 Encryption
- Your Wi-Fi should use WPA3 (if available) or WPA2 encryption. Avoid WEP or open networks.

*Disable WPS
- WPS is vulnerable to brute-force attacks. Turn off this feature in your router settings.

*Rename Your SSID
- Change the default network name (SSID) to something non-identifiable.

*Update Router Regularly
- Check for updates via your router’s web interface. Updates patch critical security vulnerabilities.

*Enable Network Segmentation
- Use one segment for non-work devices such as smart TVs and reserve the primary network for work use only.

Limit Device Access

*Only allow authorized devices on your home network.
*Disable unused ports and services such as remote management and UPnP.
*Regularly monitor connected devices

Use a Local Firewall and Antivirus

*Enable your device’s firewall.
*Use only Healthwise-approved Antivirus and endpoint protection tools.
*Never install unauthorized software on a company device.

Secure Remote Access While Traveling

Avoid Public Wi-Fi or Secure It Properly

*Do not use open or unsecured public Wi-Fi to access Healthwise systems.
*If necessary, connect only through Healthwise's VPN.
*Always use your mobile hotspot

Always Use the VPN

*Use the Healthwise VPN client for all remote access.
*Ensure VPN auto-connect is enabled.
*Do not disable the VPN unless otherwise instructed by verified IT Support.

Use Screen Privacy Controls

*Use a privacy screen filter when accessing ePHI in public places.
*Be aware of your surroundings and never leave your device unattended or visible in public.

Secure Your Device in Transit

*Do not place laptops in check-in luggage; always carry them in your carry-on luggage.
*Lock your screen or power down your device before transit.
*Store devices in a locked case or drawer when not in use.

Prohibited Behavior

*Do not use personal email, cloud storage, or USB drives to transfer or store ePHI.
*Do not share your device with family members or others.
*Do not install unapproved software or browser extensions.

Reporting

If you notice any of the following:
*Your laptop is lost or stolen
*Your VPN connection fails unexpectedly
*You clicked a suspicious email or link
*You see unexpected pop-ups or software installations
*You suspect your account was compromised

Immediately take these steps:
1. Disconnect from the network.
2. Do not turn off your device unless instructed.
3. Call the Healthwise IT Security Hotline immediately.

Contact Information

*IT Security Helpdesk: davidlightman@healthwise.wargames.care
*IT Security Hotline: 800-555-1212