Okay, here's a revised cybersecurity policy tailored to a "low-risk" healthcare environment, keeping RMF compliance in mind and addressing the weaknesses identified in the evaluation feedback. I've aimed for clarity and accessibility for a diverse audience.

--Cybersecurity Policy for [Organization Name]--

--Effective Date:-- [Date]
--Revision Date:-- [Date]
--Approved By:-- [Name and Title]

--1. Introduction--

- --Purpose:-- This Cybersecurity Policy outlines the essential security measures required to protect the confidentiality, integrity, and availability of Protected Health Information (PHI) and other sensitive data managed by [Organization Name]. While we operate in what is considered a comparatively "low-risk" segment of the healthcare industry, the potential impact of a data breach involving PHI remains significant. Therefore, this policy establishes a framework to mitigate risks and ensure compliance with applicable laws, regulations, and industry best practices, including the Risk Management Framework (RMF).
- --Scope:-- This policy applies to all employees, contractors, vendors, volunteers, and any other individuals or entities accessing or using [Organization Name]'s information systems, networks, and data, regardless of location or device. This includes but is not limited to workstations, laptops, mobile devices, servers, cloud services, and any physical or digital media containing organizational data.
- --Policy Objectives:--
- Protect PHI and other sensitive data from unauthorized access, use, disclosure, disruption, modification, or destruction.
- Maintain the confidentiality, integrity, and availability of information systems and data.
- Ensure compliance with applicable laws, regulations, and industry standards, including HIPAA, HITECH, and the Risk Management Framework (RMF).
- Establish a culture of security awareness and accountability among all personnel.
- Provide a framework for identifying, assessing, and mitigating cybersecurity risks.
- Respond effectively to security incidents and breaches.
- --Policy Statement:-- [Organization Name] is committed to maintaining a robust cybersecurity program that protects its information assets and ensures the privacy and security of patient data. We will continuously improve our security posture through ongoing risk assessments, implementation of appropriate controls, and regular monitoring and auditing.

--2. Risk Assessment--

- --Risk Management Framework (RMF) Alignment:-- This policy is aligned with the Risk Management Framework (RMF) to systematically manage cybersecurity risks. The RMF process involves:

1. --Categorize:-- Categorize information systems and data based on their sensitivity and criticality.
2. --Select:-- Select security controls from the NIST 800-53 or other applicable control

catalog.

3. --Implement:-- Implement the selected security controls.
4. --Assess:-- Assess the effectiveness of the implemented security controls.
5. --Authorize:-- Authorize the operation of the information system.
6. --Monitor:-- Continuously monitor the security controls and the system's security posture.

- --Risk Assessment Process:-- [Organization Name] will conduct a comprehensive risk assessment at least annually, or more frequently if significant changes occur in the organization's environment, such as new technologies, business processes, or threat landscape. The risk assessment will:
- Identify potential threats and vulnerabilities to information systems and data.
- Assess the likelihood and impact of identified threats exploiting vulnerabilities.
- Determine the overall level of risk.
- Prioritize risks for mitigation.
- Document the risk assessment process and findings.
- --Risk Mitigation:-- Based on the risk assessment results, [Organization Name] will implement appropriate security controls to mitigate identified risks. Risk mitigation strategies may include:
- Implementing technical controls (e.g., firewalls, intrusion detection systems, encryption).
- Implementing administrative controls (e.g., policies, procedures, training).
- Transferring risk (e.g., cyber insurance).
- Accepting risk (with documented justification).
- --Vulnerability Scanning:-- Regularly scheduled vulnerability scanning of all servers and workstations on the network to remediate vulnerabilities.

--3. Data Protection--

- --Data Classification:-- All data will be classified based on its sensitivity and criticality. Classification levels may include:
- --Highly Sensitive:-- PHI, financial information, employee records, and other data requiring the highest level of protection.
- --Sensitive:-- Confidential business information, internal communications, and data requiring protection against unauthorized disclosure.
- --Public:-- Information intended for public dissemination.
- --Data Encryption:--
- --Data in Transit:-- All data transmitted over public networks (e.g., the internet) must be encrypted using strong encryption protocols such as TLS 1.2 or higher with cipher suites following industry best practices (e.g., ECDHE-RSA-AES256-GCM-SHA384).
- --Data at Rest:-- Sensitive data stored on any device, including laptops, desktops, mobile devices, and servers, must be encrypted using strong encryption algorithms such as AES-256. Key management must follow industry best practices, including secure key generation, storage, and rotation. [Specify the key management system or procedures used].
- --Data Loss Prevention (DLP):-- DLP measures will be implemented to prevent sensitive data from leaving the organization's control. This may include:

- Monitoring network traffic for unauthorized data transfers.
- Blocking access to unauthorized websites or applications.
- Restricting the use of removable media.
- Implementing content filtering on email.
- --Data Backup and Recovery:-- Regular backups of all critical data will be performed and stored securely in an offsite location. Backup procedures will be tested regularly to ensure data can be restored in a timely manner in the event of a disaster. [Specify backup frequency, retention policies, and recovery time objectives].
- --Data Disposal:-- Data must be disposed of securely when it is no longer needed. This includes:
- Shredding paper documents containing sensitive information.
- Wiping or destroying electronic media using secure data sanitization methods (e.g., DoD 5220.22-M standard).
- Physically destroying hard drives and other storage devices.

--4. Access Controls--

- --Principle of Least Privilege:-- Access to information systems and data will be granted based on the principle of least privilege. Users will only be granted the minimum level of access required to perform their job duties.
- --User Account Management:--
- All users must have unique user accounts.
- User accounts will be created, modified, and deleted promptly based on employee onboarding, transfers, and terminations.
- Inactive user accounts will be disabled or deleted after [specify time period].
- --Password Policy:-- All users must adhere to a strong password policy that includes the following requirements:
- Minimum password length: 12 characters
- Password complexity: Must include a combination of uppercase letters, lowercase letters, numbers, and symbols.
- Password history: Passwords must be unique and not reused from previous [specify number] passwords.
- Password rotation: Passwords must be changed every [specify time period], e.g., 90 days.
- Account lockout: After [specify number] failed login attempts, the account will be locked for [specify time period].
- --Multi-Factor Authentication (MFA):-- MFA will be required for all users accessing sensitive systems and data, especially for remote access. Acceptable MFA methods include:
- One-time passwords (OTP) sent via SMS or email.
- Authenticator apps.
- Hardware tokens.
- --Remote Access:-- Remote access to [Organization Name]'s network and systems must be secured using a Virtual Private Network (VPN) with strong encryption. All devices used for remote access must be compliant with the organization's security policies.
- --Physical Security:-- Physical access to [Organization Name]'s facilities and data centers must be controlled to prevent unauthorized entry. This includes:
- Using access badges or other authentication methods.

- Monitoring access points with surveillance cameras.
- Maintaining visitor logs.
- Securing server rooms and data centers.

--5. Incident Response--

- --Incident Response Plan:-- [Organization Name] will maintain a comprehensive incident response plan (IRP) that outlines the procedures for detecting, analyzing, containing, eradicating, and recovering from security incidents and breaches. The IRP will be reviewed and tested at least annually.
- --Incident Response Team (IRT):-- The IRT will be responsible for managing security incidents and breaches. The IRT will consist of representatives from:
- Information Technology (IT)
- Security Officer
- Privacy Officer
- Legal Counsel
- [Optional: Public Relations/Communications, depending on size of org]
- [Optional: Senior Management]
- --Incident Reporting:-- All suspected security incidents must be reported immediately to the IRT. Reporting channels include [Specify reporting methods, e.g., phone, email, online portal].
- --Incident Handling Procedures:-- The IRP will detail specific procedures for handling various types of security incidents, including:
- Data breaches involving PHI.
- Malware infections.
- Phishing attacks.
- Denial-of-service attacks.
- Insider threats.
- --Post-Incident Review:-- Following a security incident, a post-incident review will be conducted to identify the root cause of the incident, evaluate the effectiveness of the incident response, and implement corrective actions to prevent future incidents. This review will be documented.

--6. Security Awareness Training--

- --Training Program:-- All employees, contractors, and other users will receive security awareness training upon hire and annually thereafter. The training will cover:
- Overview of cybersecurity threats and vulnerabilities.
- [Organization Name]'s security policies and procedures.
- Protecting PHI and other sensitive data.
- Identifying and reporting security incidents.
- Safe computing practices (e.g., password security, avoiding phishing scams, using secure websites).
- Social Engineering and the dangers of revealing information.
- Mobile device security.
- --Training Delivery:-- Security awareness training will be delivered through a variety of methods, including:

- Online training modules.
- Classroom training.
- Security newsletters.
- Phishing simulations.
- Posters and other awareness materials.
- --Training Records:-- Records of all security awareness training will be maintained.

--7. Compliance and Auditing--

- --Compliance:-- [Organization Name] is committed to complying with all applicable laws, regulations, and industry standards, including HIPAA, HITECH, and the Risk Management Framework (RMF).
- --Internal Audits:-- Regular internal audits will be conducted to assess compliance with this Cybersecurity Policy and the effectiveness of security controls.
- --Scope:-- Audits will cover all aspects of the cybersecurity program, including:
- Access controls.
- Data protection.
- Incident response.
- Security awareness training.
- Configuration management.
- Physical security.
- --Frequency:-- Audits will be conducted at least annually, or more frequently if deemed necessary based on risk assessments or incident history.
- --Types:-- Audits may include:
- Policy reviews.
- Technical assessments (e.g., vulnerability scans, penetration tests).
- Compliance reviews.
- User access reviews.
- --Logging and Monitoring:-- Comprehensive logging and monitoring capabilities will be implemented to detect and respond to security incidents.
- --Scope:-- Logging will cover all critical systems and applications, including:
- Authentication attempts.
- Access to sensitive data.
- System changes.
- Network traffic.
- --Retention:-- Log data will be retained for [Specify retention period] to support incident investigation and compliance requirements.
- --Monitoring:-- Log data will be monitored regularly for suspicious activity. Automated alerts will be configured to notify the IRT of potential security incidents.
- --Third-Party Audits:-- [Optional: If applicable] [Organization Name] may engage third-party auditors to conduct independent assessments of its cybersecurity program.
- --Policy Review:-- This Cybersecurity Policy will be reviewed and updated at least annually, or more frequently as needed to reflect changes in the organization's environment, the threat landscape, or applicable laws and regulations.

--8. Conclusion--

This Cybersecurity Policy is critical to protecting [Organization Name]'s information assets and ensuring the privacy and security of patient data. All personnel are responsible for understanding and adhering to this policy. Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or contract. We are committed to creating a secure environment for all.

--Amendments--
Any amendments to this policy will be documented and communicated to all relevant personnel.