Okay, here's a revised cybersecurity policy addressing the feedback and tailored for a low-risk healthcare environment, aligned with ISO/IEC 27001 principles. It's structured to be accessible to a broad audience while maintaining the necessary level of detail.

--Cybersecurity Policy - [Healthcare Organization Name]--

--Version:-- 1.0
--Date Issued:-- October 26, 2023
--Review Cycle:-- Annually (or more frequently upon significant organizational or technological change)
--Approved by:-- [Name and Title of Approving Authority - e.g., Chief Executive Officer, Compliance Officer]

--1. Introduction--

--1.1 Purpose:--

This Cybersecurity Policy outlines the mandatory requirements and best practices that [Healthcare Organization Name] (hereinafter referred to as "the Organization") must adhere to in order to protect the confidentiality, integrity, and availability of its information assets and systems. This policy aims to safeguard patient data, ensure business continuity, and maintain compliance with applicable laws, regulations (including HIPAA where applicable), and industry standards, specifically considering the principles of ISO/IEC 27001. It applies to all employees, contractors, vendors, volunteers, and any other individuals or entities accessing or using the Organization's information systems or data, regardless of location.

--1.2 Scope:--

This policy covers all aspects of cybersecurity, including but not limited to:

- All information assets, including electronic Protected Health Information (ePHI), paper records, and intellectual property.
- All information systems, networks, devices (including workstations, laptops, mobile devices, and servers), and applications owned, leased, or used by the Organization.
- All physical locations housing the Organization's information assets.
- All third-party service providers with access to the Organization's information assets.

--1.3 Objectives:--

- Establish a robust cybersecurity framework aligned with industry best practices and regulatory requirements.
- Protect patient privacy and comply with HIPAA (if applicable) and other relevant regulations.
- Minimize the risk of data breaches, cyberattacks, and other security incidents.
- Ensure business continuity and minimize disruption to patient care.
- Promote a culture of security awareness and responsibility throughout the Organization.

--2. Risk Assessment--

--2.1 Risk Management Framework:--

The Organization adopts a risk-based approach to cybersecurity. This means that security controls are implemented based on the assessed level of risk to our information assets. Our risk management framework consists of the following stages:

- --Risk Identification:-- Identifying potential threats and vulnerabilities that could compromise the confidentiality, integrity, or availability of our information assets.
- --Risk Assessment:-- Analyzing the likelihood and impact of identified risks to determine their overall severity.
- --Risk Treatment:-- Selecting and implementing appropriate controls to mitigate, transfer, avoid, or accept identified risks. Risk treatment options are evaluated based on cost-effectiveness and alignment with the Organization's risk appetite.
- --Risk Monitoring:-- Continuously monitoring the effectiveness of implemented controls and reassessing risks as the threat landscape evolves.
- --Communication and Consultation:-- Regularly communicating risk assessment findings and treatment plans to relevant stakeholders and consulting with them on risk-related decisions.

--2.2 Risk Appetite and Tolerance:--

The Organization has a --low-- risk appetite for threats that could compromise patient data or disrupt critical business operations. We have a --medium-- risk appetite for threats that cause minor business interruptions. A documented risk register that is reviewed at least annually will contain further information. Risk tolerance levels are defined based on the potential impact of a security incident, including financial loss, reputational damage, and legal liabilities. Risks exceeding our tolerance levels require immediate attention and remediation. The risk register is maintained by the [Designated Role, e.g., IT Security Officer] and is reviewed at least annually, or more frequently as needed.

--2.3 Risk Assessment Process:--

The organization conducts regular risk assessments (at least annually, and more frequently in response to significant changes) to identify, analyze, and evaluate cybersecurity risks. These assessments consider factors such as:

- The value of information assets.
- The likelihood of threats exploiting vulnerabilities.
- The potential impact of a successful attack.
- Applicable legal and regulatory requirements.

The risk assessment process is documented and includes:

- --Identification of assets:-- A comprehensive list of all information assets within the Organization's scope.
- --Threat identification:-- A list of potential threats to the Organization's information assets.
- --Vulnerability assessment:-- An evaluation of the weaknesses in systems, applications, and processes that could be exploited by threats.
- --Likelihood and impact assessment:-- An analysis of the probability and potential

consequences of a successful attack.
- --Risk prioritization:-- Ranking identified risks based on their severity.
- --Development of risk treatment plans:-- A detailed plan for mitigating, transferring, avoiding, or accepting each identified risk.

--2.4 Roles and Responsibilities:--

- The [Designated Role, e.g., IT Security Officer] is responsible for conducting risk assessments and developing risk treatment plans.
- Department heads are responsible for identifying and managing risks within their respective departments.
- All employees are responsible for reporting any potential security risks they identify.

--3. Data Protection--

--3.1 Data Classification:--

All data within the Organization is classified based on its sensitivity and criticality. This classification determines the appropriate level of protection required. The following data classification levels are used:

- --Confidential:-- Data that, if disclosed without authorization, could cause significant harm to the Organization or its patients (e.g., ePHI, financial records, trade secrets). Requires the highest level of protection, including encryption, strict access controls, and secure storage.
- --Internal:-- Data that is intended for internal use only and could cause moderate harm if disclosed (e.g., internal policies, procedures, and employee information). Requires appropriate access controls and protection against unauthorized disclosure.
- --Public:-- Data that is publicly available or intended for public release (e.g., marketing materials, public website content). Requires basic security measures to ensure integrity and availability.

--3.2 Data Encryption:--

Confidential data, both at rest and in transit, must be encrypted using industry-standard encryption algorithms. Encryption keys must be securely managed and protected.

- --Data at rest:-- Encryption is required for all hard drives on laptops and desktops containing ePHI, and for all servers storing confidential data.
- --Data in transit:-- Encryption is required for all network traffic transmitting ePHI or other confidential data. Secure protocols (e.g., HTTPS, SFTP, VPN) must be used for all external communications.

--3.3 Data Loss Prevention (DLP):--

The Organization implements DLP measures to prevent the unauthorized transfer of confidential data outside of the organization's control. This includes:

- Monitoring network traffic for potential data leaks.
- Controlling access to removable media (e.g., USB drives).
- Educating employees on the risks of data loss and the importance of data protection.

• DLP controls will be reassessed and adjusted based on continuous security risk monitoring

--3.4 Data Backup and Recovery:--

Regular backups of all critical data are performed to ensure business continuity in the event of a disaster or security incident.

• Backups are stored securely in a separate location from the primary data storage.
• Backup procedures are tested regularly to ensure that data can be restored successfully.
• Backups are retained in accordance with legal and regulatory requirements.
• The organization will leverage cloud-based backups with redundancy across geographically separated data centers.

--3.5 Data Disposal:--

Data must be securely disposed of when it is no longer needed.

• Electronic data must be securely wiped or physically destroyed.
• Paper records must be shredded or incinerated.
• Secure disposal methods must comply with relevant regulations (e.g., HIPAA).

--4. Access Controls--

--4.1 User Account Management:--

• All users must have unique user accounts.
• Shared accounts are prohibited.
• User accounts are created, modified, and disabled in a timely manner.
• The principle of least privilege is followed: users are granted only the minimum level of access necessary to perform their job duties.
• Access rights will be reviewed at least annually.

--4.2 Password Policy:--

All users must adhere to the following password requirements:

• --Minimum Length:-- 12 characters.
• --Complexity:-- Must include a combination of uppercase letters, lowercase letters, numbers, and symbols.
• --Change Frequency:-- Passwords must be changed every 90 days.
• --Password Reuse:-- Previous 12 passwords cannot be reused.
• --Account Lockout:-- Accounts will be locked out after 5 incorrect login attempts.
• --Multi-Factor Authentication (MFA):-- MFA is enabled for all users accessing sensitive systems and data, including email, remote access, and applications containing ePHI.

--4.3 Access Control Lists (ACLs):--

ACLs are used to restrict access to files, folders, and other resources based on user roles and permissions. ACLs are regularly reviewed and updated to ensure that they remain accurate and effective.

--4.4 Remote Access:--

Remote access to the Organization's network and systems is permitted only through a secure Virtual Private Network (VPN) connection. MFA is required for all remote access connections.

--4.5 Physical Access Control:--

The physical security of the organization will include the following measures:

- Building access will be limited to only authorized personnel using a key card system.
- Visitors will be required to sign in and be escorted at all times.
- All server rooms will have both physical and logical security, and will be placed in a secure room with access limited to only authorized personnel.
- Security cameras will be placed on the property.

--5. Incident Response--

--5.1 Incident Response Plan:--

The Organization has a documented Incident Response Plan (IRP) that outlines the procedures for responding to security incidents. The IRP is tested regularly to ensure its effectiveness.

--5.2 Incident Reporting:--

All suspected security incidents must be reported immediately to the [Designated Role, e.g., IT Security Officer] or the [Designated Department, e.g., IT Department].

--5.3 Incident Response Process:--

The Incident Response Process includes the following steps:

1. --Detection:-- Identifying and confirming that a security incident has occurred.
2. --Containment:-- Taking steps to prevent the incident from spreading.
3. --Eradication:-- Removing the cause of the incident.
4. --Recovery:-- Restoring affected systems and data to normal operation.
5. --Post-Incident Activity:-- Reviewing the incident and implementing corrective actions to prevent future occurrences.

--5.4 Communication:--

Communication protocols will be established for internal and external communication of incidents.

- --Internal:-- Employees need to be notified of security incidents.
- --External:-- Regulatory agencies, insurance, and patients should be notified as needed

--5.5 Contact Information and Escalation Paths:--

- --IT Security Officer:-- [Name, Phone Number, Email Address]
- --IT Department:-- [Phone Number, Email Address]
- --Compliance Officer:-- [Name, Phone Number, Email Address]
- --Escalation Path:-- If the IT Security Officer is unavailable, contact the IT Department Manager. If the IT Department Manager is unavailable, contact the Compliance Officer.

--6. Security Awareness Training--

--6.1 Training Program:--

All employees, contractors, and vendors must complete security awareness training upon hire and annually thereafter.

--6.2 Training Content:--

The training program covers the following topics:

• Phishing awareness
• Password security
• Data protection
• Social engineering
• Incident reporting
• Physical security
• Policy and procedures

--6.3 Training Delivery:--

Training is delivered through a combination of online modules, in-person sessions, and simulated phishing campaigns.

--6.4 Tracking and Reporting:--

Completion of security awareness training is tracked and reported to management. Remedial training is provided to individuals who do not meet the required standards.

--7. Compliance and Auditing--

--7.1 Compliance Requirements:--

The Organization is committed to complying with all applicable laws, regulations, and industry standards, including HIPAA (if applicable), ISO/IEC 27001, and any other relevant data privacy regulations.

--7.2 Auditing:--

Regular internal and external audits are conducted to assess compliance with this policy and other security requirements.

• Audit findings are documented and reported to management.
• Corrective actions are implemented to address any identified deficiencies.

--7.3 Policy Review:--

This policy is reviewed and updated at least annually, or more frequently as needed, to ensure that it remains current and effective. Any changes to the policy must be approved by the [Designated Approving Authority, e.g., CEO, Compliance Officer].

--8. Conclusion--

This Cybersecurity Policy is a critical component of the Organization's overall risk management strategy. 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. The organization is dedicated to creating a secure environment for patients, employees, and stakeholders.

--[Signature of Approving Authority]--

--[Printed Name and Title]--