Okay, here's a comprehensive cybersecurity policy tailored for a low-risk healthcare environment, incorporating the feedback and aligning with COBIT, while considering both technical and non-technical audiences.

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

--Effective Date:-- October 26, 2023
--Revision Date:-- [Date of Next Review - Typically Annually]
--Version:-- 1.0
--Approved by:-- [Name and Title of Approving Authority - e.g., CEO, Compliance Officer]

--1. Introduction--

- --Purpose:-- This Cybersecurity Policy outlines the essential security standards, guidelines, and procedures for [Healthcare Organization Name] (hereafter referred to as "the Organization") to protect the confidentiality, integrity, and availability of Protected Health Information (PHI) and other sensitive data. This policy aims to ensure compliance with applicable laws, regulations (including HIPAA), and industry best practices, including the COBIT framework.

- --Scope:-- This policy applies to all employees, contractors, volunteers, students, and any other individuals who access, use, or manage the Organization's information systems, networks, and data, regardless of location or device used (including BYOD devices used for organizational purposes). This policy encompasses all electronic and physical forms of data and information systems.

- --Policy Objectives:--
- Safeguard PHI and other sensitive information 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 contractual obligations.
- Establish a framework for identifying, assessing, and managing cybersecurity risks.
- Promote a culture of security awareness throughout the Organization.
- Provide a consistent and standardized approach to cybersecurity practices.

- --COBIT Alignment:-- This policy is aligned with the COBIT (Control Objectives for Information and Related Technology) framework, a globally recognized best practice for IT governance and management. COBIT helps us to ensure that our IT investments are aligned with our business goals, risks are managed appropriately, and resources are used responsibly. We will strive to implement the principles of COBIT to continuously improve our cybersecurity posture.

--2. Risk Assessment--

- --Purpose:-- To systematically identify, analyze, and evaluate cybersecurity risks to the Organization's information assets.

- --Process:--
- --Identification:-- Conduct regular risk assessments (at least annually and more frequently if there are significant changes in the environment) to identify potential

threats, vulnerabilities, and potential impacts to the Organization's data and systems. This includes identifying assets (hardware, software, data, and personnel), understanding their value, and considering the potential impact of compromise.

- --Analysis:-- Analyze the likelihood and impact of identified risks to determine their overall severity.
- --Evaluation:-- Evaluate the acceptability of risks based on organizational risk tolerance levels. Prioritize risks for mitigation based on their severity and potential impact.
- --Documentation:-- Document all risk assessment findings, including identified risks, analysis results, and mitigation plans.

- --Responsibilities:-- The [Designated Role/Department - e.g., IT Security Officer, Compliance Officer, Risk Management Committee] is responsible for conducting and managing the risk assessment process. All departments and employees are responsible for cooperating with the risk assessment process and reporting potential security risks.

- --COBIT Alignment:-- This section aligns with COBIT process --APO12 Manage Risk--. Specifically, the risk assessment process will consider risk identification, risk analysis, risk response, and risk reporting, as outlined in APO12. For example, during risk analysis, we will use metrics and indicators defined within APO12 to assess the potential impact of a security breach on our organization's objectives.

--3. Data Protection--

- --Purpose:-- To protect PHI and other sensitive data from unauthorized access, use, disclosure, modification, or destruction.

- --Principles:--
- --Confidentiality:-- Ensuring that information is accessible only to authorized individuals.
- --Integrity:-- Maintaining the accuracy and completeness of information.
- --Availability:-- Ensuring that information and systems are accessible when needed by authorized users.
- --Data Minimization:-- Collecting, using, and retaining only the minimum amount of PHI necessary to accomplish the intended purpose. Data should not be kept longer than required by law or business need. When data is no longer needed, it should be securely destroyed or anonymized.

- --Specific Measures:--
- --Encryption:-- PHI stored on electronic devices and transmitted across networks must be encrypted using industry-standard encryption algorithms. This includes laptops, desktops, mobile devices, and cloud storage.
- --Access Controls:-- Implement access controls to restrict access to PHI to authorized personnel based on the principle of least privilege (see Section 4).
- --Data Backup and Recovery:-- Regularly back up PHI and other sensitive data to ensure business continuity in the event of a disaster or system failure. Test the restoration process regularly.
- --Data Sanitization and Disposal:-- Implement procedures for securely sanitizing or destroying electronic media containing PHI when it is no longer needed. Follow NIST

Special Publication 800-88 guidelines for media sanitization.

- --PHI Handling:-- All employees must adhere to established procedures for handling PHI, including proper storage, transmission, and disposal. This includes understanding the different types of PHI (e.g., demographic data, medical records, billing information) and the specific regulations and policies that apply to each. When faxing PHI, always verify the recipient's fax number before sending.

- --COBIT Alignment:-- This section aligns with COBIT process --DSS05 Manage Security Services--. Specifically, data protection measures are considered a key security service aimed at protecting the organization's information assets. For instance, the implementation of encryption and access controls directly supports the objective of preventing unauthorized access to sensitive data.

--4. Access Controls--

- --Purpose:-- To ensure that access to information systems and data is restricted to authorized individuals and based on the principle of least privilege.

- --Policies:--
- --User Authentication:-- Implement strong authentication methods, such as multi-factor authentication (MFA), for all users accessing the Organization's network and systems. Require strong passwords and regular password changes.
- --Authorization:-- Grant access to data and systems based on job role and responsibilities. Implement role-based access control (RBAC).
- --Account Management:-- Establish procedures for creating, modifying, and terminating user accounts in a timely manner. Conduct regular reviews of user access rights to ensure they remain appropriate. Disable inactive accounts promptly.
- --Physical Access:-- Control physical access to facilities and equipment containing sensitive data through measures such as keycard access, security cameras, and visitor logs.
- --Remote Access:-- Implement secure remote access solutions (e.g., VPN) and enforce strong authentication for all remote users.

- --COBIT Alignment:-- This section aligns with COBIT process --DSS05 Manage Security Services-- and --DSS03 Manage Problems--. The access controls are part of ensuring secure access to the IT system for the organization. Access controls are implemented in such a way that system access is only granted to personnel with the rights to do so.

--5. Incident Response--

- --Purpose:-- To establish a structured approach for detecting, responding to, and recovering from cybersecurity incidents.

- --Incident Response Plan:-- The Organization maintains a comprehensive Incident Response Plan (IRP) that outlines the steps to be taken in the event of a security incident. The IRP will be reviewed and tested at least annually.

- --Incident Reporting:-- All employees are required to report suspected or actual security incidents immediately to the [Designated Contact/Department - e.g., IT Help Desk, Security Officer].

- --Incident Response Process:--
- --Detection and Analysis:-- Identify and analyze security incidents to determine their scope and impact.
- --Containment:-- Take immediate steps to contain the incident and prevent further damage. This may involve isolating affected systems, disabling compromised accounts, or blocking malicious traffic.
- --Eradication:-- Remove the cause of the incident, such as malware or vulnerabilities.
- --Recovery:-- Restore affected systems and data to their normal state.
- --Post-Incident Activity:-- Conduct a post-incident review to identify lessons learned and improve security controls.

- --Communication and Escalation:--
- --Internal Communication:-- The Incident Response Team will communicate regularly with stakeholders, including senior management, legal counsel, and public relations, to provide updates on the incident and its impact.
- --Escalation Paths:-- The Incident Response Plan clearly defines escalation paths for different types of incidents, ensuring that appropriate personnel are notified in a timely manner. For example, a confirmed data breach involving PHI will be immediately escalated to the Privacy Officer and Compliance Officer.
- --External Reporting:-- Comply with all applicable legal and regulatory reporting requirements, including reporting data breaches to relevant authorities (e.g., HHS OCR) as required by HIPAA.

- --COBIT Alignment:-- This section aligns with COBIT process --DSS02 Manage Service Requests and Incidents--. The incident response process is designed to manage security incidents effectively, minimizing disruption to business operations. For example, incident reporting and escalation procedures ensure that incidents are addressed in a timely and coordinated manner, as outlined in DSS02.

--6. Security Awareness Training--

- --Purpose:-- To educate employees and other users about cybersecurity risks and their responsibilities in protecting the Organization's information assets.

- --Training Program:--
- All employees will receive mandatory security awareness training upon hire and annually thereafter.
- Training will cover topics such as:
- Identifying and reporting phishing emails
- Password security best practices
- Data protection policies and procedures
- Social engineering awareness
- Incident reporting procedures
- HIPAA compliance
- Provide ongoing security awareness reminders and updates through newsletters, posters, and other channels.

- --COBIT Alignment:-- This section aligns with COBIT process --APO14 Manage Training and

Awareness--. Security awareness training contributes to a better cybersecurity environment at the company. The goal of the training sessions is to make the user more aware of the security environment.

--7. Compliance and Auditing--

- --Purpose:-- To ensure compliance with applicable laws, regulations, and contractual obligations, and to verify the effectiveness of the Organization's cybersecurity controls.

- --Compliance Activities:--
- Conduct regular compliance reviews to ensure adherence to HIPAA and other relevant regulations.
- Maintain documentation of all compliance activities.
- Stay up-to-date on changes in laws and regulations that may impact cybersecurity.

- --Auditing:--
- Conduct periodic internal and external audits to assess the effectiveness of cybersecurity controls.
- Address any audit findings in a timely manner.
- Maintain records of all audit activities.

- --COBIT Alignment:-- This section aligns with COBIT process --MEA03 Manage Compliance with External Requirements--. Through compliance monitoring and audit testing, we are able to ensure that we are meeting the goals of the regulatory bodies that oversee our industry.

--8. Conclusion--

This Cybersecurity Policy is essential for protecting the Organization's information assets and ensuring compliance with applicable laws and regulations. All employees and other users are responsible for adhering to this policy and reporting any security concerns. This policy will be reviewed and updated at least annually to reflect changes in the threat landscape, technology, and regulatory requirements.

--Enforcement:--

Failure to comply with this policy may result in disciplinary action, up to and including termination of employment or termination of contracts.