Written Information Security Policy (WISP) for [Healthcare Organization Name]

Introduction

[Healthcare Organization Name] is dedicated to securing both personal and organizational information in alignment with the Commonwealth of Massachusetts' regulations, specifically adhering to the standards set forth in 201 CMR 17.00: Standards for The Protection of Personal Information of Residents of the Commonwealth. This Written Information Security Policy (WISP) outlines our organization's commitment and approach to safeguarding personal information against unauthorized access, use, modification, destruction, or disclosure.

Scope

This policy applies to all employees, contractors, affiliates, and any individual who handles personal information (PI) or personal identifiable information (PII) within [Healthcare Organization Name], which encompasses three hospitals and 25 clinics.

Policy Objectives

1. **Purpose**
   - To establish a comprehensive security program that incorporates administrative, technical, and physical safeguards designed to protect the PI and PII of Massachusetts residents.
2. **Risk Management**
   - Conduct regular risk assessments to identify and mitigate risks to PI and PII, evaluating and improving upon the effectiveness of the current security measures.
3. **Information Security Program**
   - Develop, implement, and maintain an ongoing comprehensive information security program that complies with the regulations of 201 CMR 17.00.
4. **Data Access Control**
   - Ensure that access to PI and PII is strictly limited to personnel who require such access to perform their job duties. Enforce access controls and authentication to prevent unauthorized access.
5. **Data Encryption**
   - Encrypt all transmitted records and files containing PI or PII that will travel across public networks, and encrypt any such information stored on laptops or other portable devices.
6. **Education and Training**
   - Provide regular security awareness training for all employees and contractors who handle PI or PII, emphasizing the importance of protecting personal and sensitive information.
7. **Incident Response**
   - Establish a detailed incident response plan to immediately address any breaches or potential breaches of personal information. This plan will include procedures for notification, as required by Massachusetts law.

8. **Vendor Management**
    - Ensure that third-party service providers with access to PI or PII are capable of maintaining appropriate security measures consistent with 201 CMR 17.00 and other relevant regulations. Contracts with vendors will require them to adhere to these security standards.
9. **Monitoring and Review**
    - Regularly monitor the effectiveness of the security program. Review and revise the WISP periodically, at least annually, or whenever there is a material change in business practices that may implicate the security or integrity of records containing PI or PII.
10. **Physical Security**
    - Implement secure management of physical access to records containing PI and PII, and ensure secure disposal of such information in a manner that prevents unauthorized access or use.
11. **Compliance**
    - Adhere to all applicable laws and regulations regarding the protection of personal information, including, but not limited to, 201 CMR 17.00.

Enforcement

Violations of this policy may result in disciplinary actions, up to and including termination of employment, legal action, and financial restitution. The security team, along with the compliance and legal departments, are responsible for enforcing this policy.

Policy Review and Modification

This policy will be reviewed annually and updated as necessary to ensure ongoing compliance with Massachusetts regulations and to reflect changes in technology, threats, and organizational operations.

Acknowledgment

All individuals subject to this policy must acknowledge that they have read, understood, and agreed to comply with its terms. This acknowledgment will be documented and maintained by [Healthcare Organization Name]'s Human Resources department.

By adhering to this Written Information Security Policy, [Healthcare Organization Name] demonstrates its commitment to protecting the privacy and security of personal information in accordance with the stringent requirements of the Commonwealth of Massachusetts.