Project 2: Policies, Procedures and Practice

Alexis Fenderson

*Appropriate parties are delegated by operational teams in accordance with Marie-Life operations

Marie-Life Hospital - Backup Data Policies & Procedures

Purpose:

All ePHI data must be encrypted and stored safely based on the mandated practices listed below in the policy section.

This policy ensures and reflects Marie-Life Hospitals' commitment to safely securing, managing and maintaining all Electronic Protected Health Information (ePHI) on its information systems and digital media platforms. By defining set policies, we hope to establish safe procedures of regulating all ePHI information.

Definitions:

(ePHI) – Stands for electronic Protected Health Information. This is data regarding individual health. This information can include health conditions, treatment plans, payment plans or another private information that is transmitted, stored, created or managed electronically.

Digital media platforms – Websites, social media platforms, digital data and data bases and other digital surfaces.

HIPAA – Health Insurance Portability and Accountability Act. Publicize standards for electronic transfer, security and privacy for health information.

Scope:

This policy is applicable to all personnel who are tasked with the collection, storage, access or protection of ePHI. This also covers any third-party partners, vendors or other associated parties who may have access to such information. Said policy guarantees data is managed in accordance with regulation, operating and legal requirements of the United States. The focus of this policy is on the processing of data and its retainment in affecting systems. This includes physical and digital formats. It is mandatory to follow these procedures to ensure the protection and privacy of patient data.

Policy:

1: For validation of the implementation and assurance of this policy, a security assurance team will be assigned the responsibility of this task. The team will be led by a

*Appropriate parties are delegated by operational teams in accordance with Marie-Life operations

Security lead who will be tasked with reviewing data security and delegating assurance tasks to other officers.

A. Data Access and Collection:
    a. For all direct employees of Marie-Life Hospital: All ePHI data may only be accessed from a Marie-Life Hospital workstation using said Employees login credentials. Data may never be accessed or stored on an employee's private device or workstation.
    b. Local Backup: For local backups of data, employees must store ePHI data on the delegated WellnessHealth server. The file(s) must be named correctly using the ISO 15489-1:2016 international standard for record management. Local Backup's can be accessed by appropriate parties*.

    c. Offsite Backup: An offsite backup must also be maintained in the event of a disruption in the regular backup of data. Copies of patient ePHI, will be stored and updated here. This data will be backed up once every day regardless of business operation. This offsite location will be decided by the Security lead in collaboration with Marie-Life operational executives. This site must be in a state outside of Marie-Life's general hospital location.

B. Backup Schedule:
    a. Retention: ePHI will be maintained on Marie-Life systems for approximately however much time state-law dictates. In the event of an emergency, this retention period can expand to longer dates dictated by the Marie-Life operational team. It is mandatory that this information remains encrypted during this period.
    b. Deletion: After a 5-year period, backup data is to be deleted from the Offsite backup location. This will include digital and physical copies of data. Deletion of data will be handled by the security assurance team and appropriate parties*. Destruction of ePHI must be handled properly via acceptable destruction methods delegated by the security assurance team and federal law.

Procedures

1. Step 1: ePHI will be collected and stored in Marie-Life information systems. These systems include the WellnessHealth server and other applications that in associated with patient data. All data collected must be signed off by the appropriate parties*.

*Appropriate parties are delegated by operational teams in accordance with Marie-Life operations

2. Step 2: Once data has entered appropriate information systems, data must be encrypted in compliance with HIPAA Security Rule standards.
3. Step 3: If physical applications of stored data must be moved, it is mandatory to follow HIPAA and other regulatory requirements.
4. Step 4: At the end of the day, a copy of the collected ePHI is to be created as a backup and sent to the delegated Offsite Backup location. Recording the verification of this process is mandatory and must be handled by the Security Lead. A separate document must store this data in both electronic and physical formats.

Compliance and Disciplinary Measures:

For validation of the implementation and assurance of this policy, a security assurance team will be assigned the responsibility of this task. The team will be led by a Security lead who will be tasked with reviewing data security and delegating assurance tasks to other officers.

Failure to comply with the compliance of this policy will result in disciplinary actions in accordance with the rule handbook of said employee's department. Additional consequences can be advocated for by the Security lead in collaboration with the security assurance team.

*Appropriate parties are delegated by operational teams in accordance with Marie-Life operations