Episcopal SeniorLife Communities

Corporate Policy

Policy Name: HIPAA Compliance

Policy: It is the policy of Episcopal SeniorLife Communities (ESLC) to comply with The Health Insurance Portability and Accountability Act of 1996 (HIPAA) which establishes national standards to protect individuals' medical records and other personal health information and requires appropriate safeguards to protect the privacy of personal health information and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Act also gives patients' rights over their health information, including rights to examine and obtain a copy of their health records, and to request corrections.

The Health Information Technology for Economic and Clinical Health (HITECH) Act, enacted as part of the American Recovery and Reinvestment Act of 2009, promotes the adoption and meaningful use of health information technology. It addresses the privacy and security concerns associated with the electronic transmission of health information, in part, through several provisions that strengthen the civil and criminal enforcement of the HIPAA rules.

The HIPAA Security Rule requires covered entities to maintain reasonable and appropriate administrative, technical, and physical safeguards for protecting electronic protected health information (ePHI).

Entities or individuals who contract to perform services for a covered entity with access to protected health information (Business Associates) are also required to comply with the HIPAA privacy and security standards.

Policy Purpose: The purpose of this policy is to ensure ESLC's compliance with the HIPAA Act including the HIPAA Privacy and Security Rules, the Breach Notification Rule, the Omnibus Rule, and the HITECH Act.

Policy Scope: This policy applies to all ESLC.

Procedures:

A designated HIPAA Security Officer and HIPAA Privacy Officer provide organization-wide leadership for ensuring HIPAA compliance.

Administrative Safeguards: The HIPAA Security Officer

- Performs on-going risk analysis as part of ESLC's security management process.
    - Evaluates the likelihood and impact of potential risks to ePHI.
    - Implements appropriate security measures to address the risks identified in the risk analysis
    - Documents the chosen security measures and, the rational for adopting those measures
    - Maintains continuous, reasonable, and appropriate security protections including tracking access to ePHI and detecting security incidents.
- Ensures compliance with the ePHI security policies and procedures
- Ensures compliance with the authorizing role-based access to ePHI policies and procedures.
- Ensures compliance with policies and procedures related to authorization and supervision of workforce members who work with ePHI.
    - Ensures all employees are trained regarding ePHI security policies and procedures.
    - Ensures sanctions against employees who violate ePHI security policies and procedures are documented and reviewed

Physical Safeguards: The HIPAA Security Officer

- Ensures physical access is limited to only authorized access (Facilities Access and Control).
- Ensures compliance with the policies and procedures regarding transfer, removal, disposal, and re-use of electronic media to ensure appropriate protection of ePHI (Workstation and Device Security).

Technical Safeguards: The HIPAA Security Officer ensures:

- Access Control allowing only authorized persons to access ePHI
- Audit Controls by implementing hardware, software, and/or procedural mechanisms to record and examine access and other activity in information systems that contain or use ePHI
- Integrity Controls by confirming electronic measures are in place to confirm that ePHI is not improperly altered or destroyed
- Transmission Security by implementing technical security measures that guard against unauthorized access to ePHI that is being transmitted over an electronic network.

The ESLC Security Officer will periodically review and update its documentation in response to environmental or organizational changes that affect the security of ePHI.

The ESLC Privacy Officer ensures that ESLC has a Business Associate Contract with all Business Associates ESLC shares ePHI with that outlines how the Business Associate will handle and protect the data they receive.

The HIPAA Privacy Officer is responsible for:

- Adopting appropriate Policies and Procedures to comply with the HIPAA Privacy Rule.
- Updating Privacy Policies and Procedures (annually)
- Providing the Notice of Privacy Practices to all new patients/individuals upon admission, as well as, notifying patients when the Notice of Privacy Practices is modified
- Collecting Business Associate Agreements from all Business Associates and updating any Business Associate Agreements as needed (initially, distribute)
- Monitoring Business Agreements to make sure they are correctly implementing their HIPAA compliance program
- Ensuring all HIPAA-related documents and information is correct and up-to-date
- Overseeing the implementation of client and/or employee Privacy Rights
- Monitoring all covered items for compliance with Privacy Policies and Procedures
- Receiving and responding to complaints of alleged non-compliance with the HIPAA Privacy Rule
- Working closely with legal counsel and the Security Officer
- Coordinating the training of all employees that come in contact with PHI
- Answering HIPAA-related questions from fellow employees and clients

ESLC will maintain, for six years after last effective date, written security policies and procedures and written records of required actions, activities or assessments.

Reviewed: January 2023
Approved by: Lisa J. Marcello, President/CEO
Episcopal SeniorLife Communities

Board Approved: January 18, 2022