Lippmann Psychiatry

Benjamin E. Lippmann, D.O., P.A.

Workforce Security Policy

Policies and Forms That Conform to the HIPAA Security Rule

Purpose

This Workforce Security Policy has been created and implemented to ensure that all members of *Benjamin E. Lippmann, D.O., P.A.*'s workforce have appropriate access to EPHI and to prevent all unauthorized workforce members from gaining access.[1]

Definitions

- **Access** means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.
- **Access Control** provides users with rights and/or privileges to access and perform functions using information systems, applications, programs, or files and should enable authorized users to access the minimum necessary information needed to perform job functions. Rights and/or privileges should be granted to authorized users based on a set of access rules that Benjamin E. Lippmann, D.O., P.A. deems appropriate.
- **EPHI Environment** is composed of all computer systems and components which transmit, process, access, maintain or store electronic Protected Health Information.
- **Protected Health Information (PHI)** is any data that identifies the individual or for which there is a reasonable basis to believe can be used to identify the individual. Individually identifiable health information includes many common identifiers (e.g., name, address, birth date, Social Security Number).
- **Workforce** refers to faculty, staff, volunteers, trainees, students, agents, and other persons whose conduct, in the performance of work for Benjamin E. Lippmann, D.O., P.A., is under the direct control of Benjamin E. Lippmann, D.O., P.A., whether or not Benjamin E. Lippmann, D.O., P.A. pays them.

Policy

All access to computer systems and EPHI will granted based on 'need to know' with the least privileges required for each workforce member to complete their assigned job roles and tasks.

Authorization and/or Supervision

- Benjamin E. Lippmann, D.O., P.A. will explicitly authorize each member of the workforce for access to EPHI in each system and application as well as field level restrictions as appropriate[2] for that workforce member or job role.

[1] §164.308(a)(3)

[2] §164.308(a)(3)(ii)(A)

- Benjamin E. Lippmann, D.O., P.A. will maintain proper supervision over any temporary workforce members with access to the EPHI Environment.
- Detailed Job Descriptions must be maintained and updated as the job duties change.
- Benjamin E. Lippmann, D.O., P.A. will immediately make the required modifications to access for changes in job roles, duties or responsibilities, including revocation of access no longer needed.

Workforce Clearance Policy

- Background checks[3] will be conducted (within the constraints of local laws) on workforce members, prior to hire or engagement, who will or may have access to the EPHI Environment.
- The Benjamin E. Lippmann, D.O., P.A. Security Official will review and approve all Workforce Members prior to granting access to the EPHI Environment.

Termination Policy

- All access to the EPHI Environment will be revoked immediately upon termination[4] of any Workforce Member.

Procedure

1) **Authorization**. The hiring supervisor will complete a Workforce Authorization Form for each workforce member given access to PHI. The form must be completed and signed by supervisor then delivered by the supervisor to the security officer or other designated team or individual to create an access account. Initial passwords will be created as defined in the Password Policy. When the account has been created, the form will then be handing to HR for retention in the individual's file.
2) **Supervision.** Each Workforce Member with access to PHI will have a supervisor who is responsible for proper monitoring, training, and discipline for that member.
3) **Job Descriptions**. Each Workforce Member will have a detailed Job Description which outlines when and how the Workforce Member will access PHI and reinforces the responsibilities to safeguard all PHI.
    a) **Review and Update**. All Job Descriptions will be reviewed and updated at least annually and any time there is a significant change in the organization. If the change requires increase access to PHI, or allows for more restricted access to PHI, the changes will implemented for all affected Workforce Members, current and future.

[3] §164.308(a)(3)(ii)(B)
[4] §164.308(a)(3)(ii)(C)

4) **Change in Role or Duties**. Anytime a Workforce Member has a change in role or duties, the manager will complete a new Workforce Authorization Form which will list the specific access needed for the new responsibilities. All other access will be revoked.

5) **Termination**. Immediately at termination, HR will notify the security officer who will delete or disable all user accounts which that Workforce Member had access to.

6) **Background Checks**. HR will perform or commission a full background check on all employees prior to finalizing any offer of employment. The background check will consist of **credit checks, criminal checks and reference checks**. HR will notify the security officer and hiring manager of the results of the checks. The **security officer** will make the final decision on questionable hires.

