Privacy Policy - HIPAA Privacy Program: General

Policy Purpose

Organization will comply with its responsibilities to ensure the privacy, integrity and security of the information we use, transmit, create and maintain as well as the individual ‘s rights for accessing, sharing, amending, and an accounting of the use and disclosure of their PHI and to be notified when the PHI is shared or accessed when it should not have been.

Policy

Organization will appoint a Privacy Officer, adopt and follow policies and procedures, train its workforce members, safeguard protected health information, notify individuals how their information may be used, establish procedures for the receipt and response to complaints regarding HIPAA compliance, establish a clear disciplinary process for violations of HIPAA requirements, mitigate any harm from improper use or disclosure of protected health information, prohibit retaliation against anyone seeking in good faith to enforce HIPAA rights or responsibilities, and appropriately retain HIPAA documentation. Organization may not require individuals to waive their rights to file a complaint with HHS regarding HIPAA compliance as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

At all times, Organization shall have one individual identified and assigned to HIPAA Privacy responsibility. This individual is known as the HIPAA Privacy Officer. Organization’s workforce members must understand the protections to PHI’s privacy, security and integrity, when and how individuals and others can access this information, and what to do when they notice it may have been used improperly when working with this protected health information (PHI) on the Organization’s behalf.

The Privacy Officer is responsible for Organization’s overall compliance with the HIPAA Privacy Rule, and for ensuring that Organization’s HIPAA Privacy Rule policies and procedures are developed, implemented, and followed. The Privacy Officer is the point person for Organization’s Privacy Program, through which the Privacy Officer’s and other Organizational duties are carried out.

The Organization must follow the below procedures under the Privacy Program.

Procedures

Designation of Individuals

1. Designation of the *Privacy Officer*, who is responsible for development and implementation of Organization’s policies and procedures.
2. Designation of a contact person or an office (may be either the Privacy Officer or another designated individual or location) responsible for receiving privacy-related complaints, and providing further information about Organization’s Notice of Privacy Practices.

Training

Organization must train all workforce members on its Privacy Policies and Procedures, as necessary and appropriate for workforce members to carry out their functions within the Organization. Training shall be provided as follows:

- To each new member of the workforce within a reasonable period of time after the person joins the workforce;

- To each member of Organization's workforce whose functions are affected by a significant change in Organization's privacy policies and procedures, within a reasonable period of time after that change becomes effective.
- To any member of the workforce whose responsibilities have changed when different policies and procedures apply to their new role.
- Organization must document that the training has been provided.

Questions concerning training or any aspect of training may be directed to the Privacy Officer.

Safeguards

Organization must reasonably safeguard protected health information (PHI) from any intentional or unintentional use or disclosure that violates the HIPAA Privacy Rule. Organization must also reasonably safeguard protected health information to limit incidental PHI uses or disclosures that are made pursuant to an otherwise permitted or required use or disclosure. Following a risk assessment of the PHI held by Organization, it shall implement physical, administrative and technical safeguards to reasonably address the risk of improper access, use or disclosure of PHI in all forms including verbal, visual, paper, electronic (also addressed separately in the security policies), film, or any other form.

Examples of appropriate safeguards by type are:

- Administrative Safeguards – Policies and Procedures including discipline, training, and guidance, sign in sheets;
- Physical Safeguards: locks, segregation of PHI in secured areas, access restrictions;
- Technical Safeguards: encryption, key card access, firewalls, multi-factor authentication.

Organization will conduct physical audits of its locations to identify and address risks which require reasonable safeguards to be implemented. Organization will review privacy complaints and incidents on an annual basis, or more frequently if a significant number of complaints are received or incidents occur, to determine if additional safeguards are necessary for any recurring incident or complaint types.

Complaints

Organization must provide a process for individuals to make complaints concerning its compliance with the HIPAA Privacy Rule, the HIPAA Breach Notification Rule, and Organization's policies and procedures related to these rules. Organization will address all complaints received and keep records of complaints and their resolution. Please refer to Privacy Policy - Complaints to the Organization for more details. Organization will handle any complaints that are also found to be privacy incidents under Privacy Policy - HIPAA Incident Response and Reporting and Breach Determination.

Sanctions

Organization must develop and apply appropriate sanctions against workforce members who fail to comply with its privacy policies and procedures and/or the HIPAA Privacy Rule. Organization must document all sanctions and apply them in a consistent manner. The Privacy Officer shall be responsible for the determination of appropriate sanctions and may involve human resources in any decision. In deciding upon the appropriate sanction, Organization may review the severity of the violation, the impact of the violation, and the workforce member's work history. The Privacy Officer, in his or her discretion, may review the sanction decision at the request of a workforce member.

Mitigation

Organization must mitigate, to the extent practicable, any harmful effect that is known to it of a use or disclosure of PHI in violation of its policies and procedures or the HIPAA Privacy Rule by Organization or its business associates.

Organization will ensure that mitigation plans are developed, implemented and applied in accordance with these policies and procedures. In response to a report of or information about a workforce member's or business associate's unauthorized use or disclosure of PHI, Organization shall act promptly to reduce any known or reasonably anticipated harmful effects from the disclosure. Organization shall contact the recipient of the information that was subject of the unauthorized disclosure and request that such recipient either destroy or return the information. Organization will take other appropriate action to prevent further use or disclosure.

No Retaliation

Organization will not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against anyone

- who files a complaint either with the Organization or with HHS,
- who exercises a right to which they are entitled under the Privacy Rule or the Breach Notification Rule, or
- who testifies, assists with or participates in an investigation, compliance review, or proceeding, or opposes any act or practice that he or she reasonably believes is unlawful under these regulations.

Waiver of Rights

Organization will not require any individual to waive his or her right to file a complaint with Organization or HHS. Organization may not condition the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits on an individual's waiver of their right to file such a HIPAA compliance complaint.

Policies and Procedures

The policies and procedures to be developed and reviewed by the Privacy Officer must comply with all Privacy Rule standards, implementation specifications, and requirements. The policies and procedures must be reasonably designed, taking into account both the Organization's size and the type of activities related to PHI Organization undertakes.

Changes to Policies and Procedures

Organization must change its policies and procedures as necessary and appropriate to comply with changes in the law. Whenever a change in law necessitates a change to Organization's policies or procedures, Organization must promptly document and implement the revised policy or procedure. If the change in law materially affects the content of the Notice of Privacy Practices, Organization must change the contents of the notice accordingly. If the Organization has not retained the right to revise its Notice of Privacy Practice, it may amend the Notice, policies and procedures but, in that case, the changes are only applicable to PHI created, received, maintained or transmitted after the effective date of the revision. Organization may not implement a change to a policy or procedure prior to the effective date of the revised notice.

Documentation

Organization must maintain its policies and procedures in written or electronic form and must maintain all required documentation (which includes the policies and procedures, and any communications or actions the HIPAA Privacy Rule requires to be in writing) for six years from the date of its creation or the date when it was last in effect, whichever is later.

RELEVANT HIPAA REGULATIONS:

- 45 CFR Part 164 Subpart E
- 45 CFR 164.530 HIPAA Privacy Program Administrative Requirements