HIPAA Privacy Rules:

- **Minimum Necessary Standard:** Healthcare providers must use, disclose, and request only the minimum amount of protected health information (PHI) necessary to accomplish the intended purpose.

- **Authorization Requirement:** Healthcare providers generally need written authorization from the patient to use or disclose PHI for purposes other than treatment, payment, and healthcare operations.

- **Notice of Privacy Practices:** Covered entities (healthcare providers, health plans, etc.) are required to provide patients with a notice of privacy practices that explains how their PHI will be used and their privacy rights.

- **Right to Access:** Patients have the right to access and obtain a copy of their own PHI held by covered entities.

- **Right to Request Amendments:** Patients can request amendments or corrections to their PHI if they believe it to be inaccurate.

- **Accounting of Disclosures:** Covered entities must provide patients with a list of who has accessed their PHI and for what purposes, upon request.

- **Restrictions on Marketing:** Patients must provide authorization for any marketing activities involving their PHI. This rule restricts the use of PHI for marketing purposes without patient consent.

- **Breach Notification:** Covered entities are required to notify affected individuals and the U.S. Department of Health and Human Services (HHS) of breaches of unsecured PHI.

- **Confidential Communications:** Covered entities must accommodate reasonable requests from patients for confidential communications of their PHI, such as sending mail to an alternative address.

- **Penalties and Enforcement:** HIPAA includes provisions for the enforcement of privacy rules and sets penalties for violations, which can be substantial.

- **Business Associate Agreements:** Covered entities are required to have business associate agreements in place with third-party service providers who handle PHI on their behalf. Business associates are also held to certain HIPAA privacy rules.

HIPAA Security Rules:

1. **Administrative Safeguards:**
   - **Security Management Process**: Establish policies and procedures to prevent, detect, contain, and correct security violations.
   - **Security Officer:** Designate an individual responsible for security management.
   - **Workforce Training and Management:** Train employees on security policies and procedures and manage their access to ePHI.
   - **Information Access Management:** Implement procedures for authorizing, monitoring, and revoking access to ePHI.

2. **Physical Safeguards:**

   - **Facility Access Control:** Implement physical access controls to protect against unauthorized access to ePHI.
   - **Workstation Security:** Implement policies for the use and access to workstations and devices with ePHI.
   - **Device and Media Controls:** Implement procedures for the disposal, re-use, and accountability of electronic media and devices that contain ePHI.

3. **Technical Safeguards:**

   - **Access Control:** Implement technical controls to restrict access to ePHI to authorized users.
   - **Audit Controls:** Implement hardware, software, and procedural mechanisms to record and examine activity in systems containing ePHI.
   - **Integrity Controls:** Implement mechanisms to ensure the integrity and authenticity of ePHI.
   - **Transmission Security:** Implement security measures to protect ePHI during electronic transmission.

4. **Organizational Requirements:**

   - Business Associate Agreements: Enter into agreements with business associates who have access to ePHI to ensure they also comply with HIPAA security requirements.
   - Policies and Procedures: Establish and maintain security policies and procedures.
   - Documentation and Records: Maintain records of policies, procedures, and security-related activities.

5. **Risk Analysis and Management:**

   - Conduct regular risk assessments to identify and address security vulnerabilities and risks to ePHI.
   - Implement security measures to mitigate identified risks.

6. **Incident Response:**

- Develop and maintain an incident response plan to address security incidents.
- Report and respond to security incidents in a timely and effective manner.

7. **Contingency Planning:**

- Create data backup and disaster recovery plans for ePHI.
- Test and revise these plans periodically.

8. **Evaluation:**

- Perform periodic evaluations to assess compliance with HIPAA security standards.
- Make any necessary changes to improve security measures.