Check Your Understanding
Supplemental Document

1. What are the main components of a HIPAA compliance program?

   Answer: The main components of a HIPAA compliance program include:
   - Privacy Rule compliance
   - Security Rule compliance
   - Breach Notification Rule compliance
   - Policies and procedures
   - Training
   - Auditing and monitoring

2. True or False: Covered entities under HIPAA include healthcare providers, health plans, and healthcare clearinghouses.

   Answer: **True**

3. What is the purpose of the HIPAA Privacy Rule?

   Answer: The **HIPAA Privacy Rule** establishes national standards for the protection of individuals' medical records and other personal health information.

4. What is the minimum necessary standard under HIPAA, and why is it important?

   Answer: The **minimum necessary** standard requires covered entities to limit the use, access, and disclosure of PHI to the minimum necessary to accomplish the intended purpose.

5. Explain the difference between a covered entity and a business associate under HIPAA

   Answer: A **covered entity** directly handles PHI, while a **business associate** performs certain functions or activities on behalf of, or provides certain services to, a covered entity involving the use or disclosure of PHI.

6. True or False: HIPAA allows patients the right to access their own medical records.

   Answer: **True**

7. Describe the requirements for notifying individuals in the event of a data breach under HIPAA.

   Answer: Covered entities must notify affected individuals, the Secretary of Health and Human Services, and, in some cases, the media, following a breach of unsecured PHI.

8. Define HITECH and explain its relationship to HIPAA.

   Answer: **HITECH** (Health Information Technology for Economic and Clinical Health) Act expanded HIPAA's privacy and security requirements and increased penalties for HIPAA violations.

9. True or False: Business associates are directly liable for compliance with certain HIPAA Privacy and Security Rule provisions.

   Answer: **True**

10. What are the penalties for HIPAA violations, and how are they categorized?

    Answer: Penalties for HIPAA violations can range from $100 to $50,000 per violation, with a maximum penalty of $1.5 million per year for violations of the same provision.

Check Your Understanding
Supplemental Document

In Depth Questions

1. Can you describe your process for distributing and documenting the distribution of compliance policies and standards of conduct to new employees and contractors?

2. What measures does your organization take to designate and empower a Compliance Officer to oversee your compliance program effectively?

3. What measures does your organization take to designate and empower a Compliance Officer to oversee your compliance program effectively?

4. What steps does your organization take to ensure that employees with access to Protected Health Information (PHI) and Personally Identifiable Information (PII) receive HIPAA Privacy and Security training?

5. How does your organization communicate the contact information of your Compliance Officer and the procedure for reporting compliance concerns to your employees and Downstream Entities?

6. Can you explain your process for performing exclusion screenings on employees and Downstream Entities to ensure compliance with federal healthcare program requirements?

7. How does your organization handle and respond to reports of suspected or detected non-compliance or potential Fraud, Waste, and Abuse from your employees and Downstream Entities?

8. Describe your organization's process for distributing HHHN's Code of Conduct and Medicare Compliance Policies (or your own comparable policies) to employees and downstream entities. How do you ensure these are understood and acknowledged?

9. How does your organization ensure the privacy and security of HHHN patient information, including Protected Health Information (PHI) and Personally Identifiable Information (PII)?

10. Describe the communication channels in place within your organization for reporting compliance issues or concerns. How does your organization ensure non-intimidation and non-retaliation for whistleblowers?