Rinehart-Thompson, Laurie A., "Legal Issues in Health Information Technology", in Johns, Merida L. (ed.) Health Information Management Technology, an Applied Approach, AHIMA: Chicago, IL, 2nd ed. 2007, chapter 15, sections 15.3-5 pp. 700 – 738

1. HIPAA regulations:
   a. Never preempt state statutes
   b. Always preempt state statutes
   c. Preempt less strict state statutes where they exist
   d. Preempt stricter state statutes where they exist

2. Protected health information (PHI):
   a. Relates to one's past, present, or future mental health condition
   b. Relates to one's past, present, or future physical condition
   c. Relates to payment for the provision of healthcare
   d. All of the above

3. The Privacy Rule extends to protected health information:
   a. In any form or medium, except paper and oral forms
   b. In any form or medium, including paper and oral forms
   c. That pertains to mental health treatment only
   d. That exists in electronic form only

4. The term *minimum necessary* means that healthcare providers and other covered entities must limit use, access, and disclosure to the minimum necessary to:
   a. Satisfy one's curiosity
   b. Accomplish the intended purpose
   c. Treat an individual
   d. Perform research

5. The Privacy Rule applies to:
   a. All covered entities involved, either directly or indirectly, with transmitting or performing any electronic transactions specified in the act
   b. Healthcare providers only
   c. Only healthcare providers that receive Medicare reimbursement
   d. Only entities funded by the federal government

6. Business associate agreements are developed to cover the use of PHI by:
   a. The covered entity's employees
   b. Organizations outside the covered entity's workforce that use PHI to perform functions for the covered entity
   c. The covered entity's entire workforce

d. The covered entity's janitorial staff

7. A covered entity's workforce can include:
   a. Employees
   b. Volunteers
   c. Employees of contractors
   d. All of the above

8. De-identified information:
   a. Does not identify an individual
   b. Is information from which personal characteristics have been stripped
   c. Cannot be later constituted or combined to re-identify an individual
   d. All of the above

9. Under the Privacy Rule, a code to re-identify de-identified information:
   a. Is never allowed
   b. Is allowed if it cannot be translated to the individual's identity
   c. May disclose the mechanism for re-identification
   d. None of the above

10. Under HIPAA privacy regulations, a patient does not have the right to access his or her:
   a. History and physical report
   b. Operative report
   c. Discharge summary
   d. Psychotherapy notes

11. The Privacy Rule establishes that a patient has the right of access to inspect and obtain a copy of his or her PHI:
   a. For as long as it is maintained
   b. For six years
   c. Forever
   d. For twelve months

12. A provider may deny a patient's request to review and copy his or her health information if:
   a. The patient agreed to temporarily suspend access during a research study
   b. The patient requests his psychotherapy notes
   c. A licensed healthcare professional determines that access to PHI would endanger the life or physical safety of the patient or another person
   d. All of the above

13. The Privacy Rule specifies that a covered entity must act on an individual's request for review of a copy of PHI no later than how long after the request is made:

a. Ninety days
b. Sixty days
c. Thirty days
d. Six weeks

14. An individual's request that a covered entity attach an amendment to his or her health record:
a. Must always be honored
b. Can always be denied
c. Can be denied if the PHI in question was not created by the covered entity
d. Must be acted on no later than six months after the request was made

15. An accounting of disclosures must include disclosures:
a. To carry out treatment, payment, and operations
b. For use in the facility's patient directory
c. To the individual about whom the information pertains
d. None of the above

16. The Privacy Rule states that an individual has the right to receive an accounting of certain disclosures made by a covered entity:
a. Within the twelve months prior to the date on which the accounting is requested
b. Since the covered entity came into existence
c. Within the six years prior to the date on which the accounting is requested
d. None of the above

17. When an individual requests that PHI be routed to an alternative location:
a. A health plan may decline such a request if no reason is given
b. Both health plans and healthcare providers may deny a request if it is unreasonable
c. Both health plans and healthcare providers may deny a request if no alternative contact information is provided
d. All of the above

18. A notice of privacy practices:
a. Is to be given to patients upon their first contact with the covered entity
b. Does not have to be given to inmates who are patients
c. Explains an individual's rights under the HIPAA Privacy Rule
d. All of the above

19. The Privacy Rule requires that individuals be able to:
a. Request restrictions on certain uses and disclosures of PHI
b. Request amendment of their PHI
c. Receive a paper copy of the notice of privacy practices
d. All of the above

20. A valid authorization must contain:
    a. A description of the information to be used or disclosed
    b. An expiration date or event
    c. A statement that the information being used or disclosed may be subject to redisclosure by the recipient
    d. All of the above

21. When a covered entity has given a patient a notice of privacy practices:
    a. A consent to use or disclose information for purposes of treatment, payment, or operations is not required
    b. A consent to use or disclose information for purposes of treatment, payment, or operations is also required
    c. An authorization to use or disclose information for the purpose of treatment, payment, or operations is also required
    d. No authorizations are required for any subsequent use or disclosure of PHI

22. An individual may:
    a. Revoke an authorization in writing
    b. Never revoke a valid authorization
    c. Not specify an expiration date on an authorization
    d. None of the above

23. Disclosure in a facility's patient directory:
    a. Can occur only with the patient's written authorization
    b. Is automatic upon a patient's admission to a healthcare provider
    c. Is subject to the patient having had the opportunity to informally agree or object
    d. Can include all PHI in the patient's designated record set

24. Under the Privacy Rule, the release of PHI to a patient's relatives is:
    a. Never allowed
    b. Allowed when the information is directly relevant to their involvement with the patient's care or treatment
    c. Allowed only if the patient is declared incompetent by a court of law
    d. None of the above

25. Release of birth and death information to public health authorities:
    a. Is prohibited without patient consent
    b. Is prohibited without patient authorization
    c. Is a "public interest and benefit" disclosure that does not require patient authorization
    d. Requires both patient consent and authorization

26. The Privacy Rule "public interest and benefit" purposes include:
    a. Facilitating organ donations
    b. Information about decedents
    c. Information provided to law enforcement
    d. All of the above

27. The Privacy Rule permits use or disclosure without written patient authorization:
    a. For specific Jaw enforcement purposes specified by the Privacy Rule
    b. For incidental disclosures
    c. To prevent or lessen serious threats to health or safety
    d. All of the above

28. The use or disclosure of PHI for marketing:
    a. Always requires written authorization from the patient
    b. Does not require written authorization for face-to-face communications with the individual
    c. Requires written authorization from the patient when products or services of nominal value are introduced
    d. None of the above

29. With regard to training in PHI policies and procedures:
    a. Every member of the covered entity's workforce must be trained
    b. Only individuals employed by the covered entity must be trained
    c. Training only needs to occur when there are material changes to the policies and procedures
    d. Documentation of training is not required

30. The privacy officer is responsible for:
    a. Handling complaints about the covered entity's violations of the Privacy Rule
    b. Developing and implementing privacy policies and procedures
    c. Providing information about the covered entity's privacy practices
    d. All of the above