FEDERAL HIPAA LAW COMPLIANCE FOR PHARMACISTS

Pamela Sardo, PharmD, B.S.

Pamela Sardo, PharmD, B.S., is a licensed pharmacist and Freelance Medical Writer at Sardo Solutions in Texas.

Topic Overview

HIPAA refers to the federal law that protects sensitive patient health information from being disclosed without the patient's consent. Another purpose of this legislation was to improve the portability and accountability of health insurance coverage for employees between jobs and to reduce fraud and abuse in healthcare. HIPAA rules apply to pharmacists and pharmacy staff. This course discusses HIPAA privacy and security rules, and the penalties for noncompliance. Health technology is advancing rapidly. Pharmacists and pharmacy staff need to keep pace with these changes.

Accreditation Statement:

RxCe.com LLC is accredited by the Accreditation Council for Pharmacy Education (ACPE) as a provider of continuing pharmacy education.

Universal Activity Number (UAN): The ACPE Universal Activity Number assigned to this activity is **0669-0000-22-060-H03-P.**

Credits: 1 hour of continuing education credit

Type of Activity: Knowledge

Media: Internet **Fee Information:** $3.99

Estimated time to complete activity: 1 hour, including Course Test and course evaluation

Release Date: November 11, 2022 **Expiration Date:** November 11, 2025

Target Audience: This educational activity is for pharmacists.

How to Earn Credit: From November 11, 2022, through November 11, 2025, participants must:

1) Read the "learning objectives" and "author and planning team disclosures;"
2) Study the section entitled "educational activity;" and
3) Complete the Post-test and Evaluation form. The Post-test will be graded automatically. Following successful completion of the Post-test with a score of 70% or higher, a statement of participation will be made available immediately. (No partial credit will be given.)

Learning Objectives: Upon completion of this educational activity, participants should be able to:

1. **Identify** a pharmacist's role in HIPAA
2. **Describe** HIPAA Privacy and Security Rules
3. **Explain** pharmacy penalties for HIPAA violations
4. **Use** this information to answer questions about protected health information

Disclosures

The following individuals were involved in the development of this activity: Pamela Sardo, PharmD, B.S., and Susan DePasquale, MSN, PMHNP-BC. There are no financial relationships relevant to this activity to report or disclose by any of the individuals involved in the development of this activity.

Introduction

The Healthcare Insurance Portability and Accountability Act is a federal Act that protects sensitive patient health information. Sensitive patient health information may not be disclosed without the patient's consent. These rules apply to pharmacists and pharmacy staff. This course discusses the privacy and security rules, and the penalties for noncompliance. In the modern healthcare system, technology is advancing rapidly. Pharmacists and pharmacy staff need to keep pace with these changes.

Evolution of HIPAA

In 1996, President Clinton signed the Healthcare Insurance Portability and Accountability Act (HIPAA) into law. There were several purposes behind this legislation. The Act sought to improve the portability and accountability of health insurance coverage for employees between jobs, protect patients' private healthcare information, and combat waste, fraud, and abuse in health insurance and healthcare delivery. Surprisingly, medical savings accounts, tax breaks, pre-existing medical condition coverage, and simplifying the administration of health insurance are additional incorporated factors.[1,2] With respect to patient privacy, HIPAA protects sensitive patient health information from being disclosed without the patient's consent.

Health and Human Services (HHS) is the department that implements rules for HIPAA privacy and security. HHS also defines PHI (Protected Health Information).[2] The Code of Federal Regulations (CFR) is where HIPAA laws governing federal regulatory agency practices and procedures are located. Healthcare providers are defined, and covered entities (CE) are described, within the CFR.[3] A health care provider is described as a provider of medical or health services, and a person or organization furnishing, billing, or being paid for health care.[4] Pharmacy teams create records, transmit patient health information, and are considered HIPAA CE in the CFR.

HIPAA Rules for Pharmacies

HIPAA Privacy Rule

All medical records and other individually identifiable health information, whether electronic, on paper, or oral, are covered and protected by the HIPAA rule.[5] The Privacy Rule details the process by which pharmacists and other healthcare providers handle and protect a patient's medical information. It also sets limits and conditions on how an individual can use and disclose sensitive information without the patient's prior authorization. It includes the right to obtain and review a copy of health records. Patients can also request providers to make corrections to records.[6]

Rigorous state legislation can take priority over federal HIPAA privacy legislation. For example, state laws may provide stronger confidentiality protections for individuals with certain conditions, such as mental health, HIV infection, and AIDS.[7]

Covered entities must follow HIPAA regulations. Health plans, healthcare providers, and clearinghouses are entities that must follow HIPAA. Health plans include health insurance companies, health maintenance organizations (HMOs), and government programs, such as Medicare and Medicaid, that pay for health care. Healthcare providers conducting business and billing electronically, include doctors, clinics, hospitals, psychologists, chiropractors, nursing homes, pharmacists, and dentists. Healthcare clearinghouse entities process health information they receive by transforming it into a standard electronic format.[6]

Business associates of covered entities must also follow required HIPAA regulations. These associates are contractors and are not employees of a CE; however, they may need access to health information. They include medical billing companies, lawyers, information technology (IT) specialists, food service employees, volunteers, and companies that store medical records.[6,7]

Security Rule

While the HIPAA Privacy Rule safeguards PHI, the Security Rule protects a subset of information covered by the Privacy Rule. This subset is identifiable health information that a covered entity creates, receives, maintains, or transmits in electronic form. This information is called electronic protected health information (e-PHI), and the Security Rule does not apply to protected health information (PHI) transmitted orally or in writing.[8]

To comply with the HIPAA Security Rule, all covered entities must:[9]

- Ensure the confidentiality, integrity, and availability of e-PHI
- Detect and safeguard against threats to the security of the information
- Protect against anticipated unauthorized uses
- Certify compliance by their workforce

Every organization is responsible for determining what their security needs are, and how they will accomplish their security-related goals. The Security Rule leaves it up to the facility, as long as they adhere to the rule.[10]

HIPAA Breach Notification Rule

In 2021, a report revealed PHI data breaches occurred in almost 50 million people in the U.S.[11] The most commonly reported category of breaches is hacking, and the largest breach involves approximately 3,500,000 individuals.[12] A breach is unauthorized use or disclosure under the Privacy Rule that compromises the security or privacy of the protected health information. The HIPAA Breach Notification Rule requires HIPAA CE and their business associates to provide notification following an infringement of unsecured protected health information.[13]

Following a breach, entities must provide notification of the occurrence to affected individuals and the Secretary of HHS, through the online Office for Civil Rights (OCR) breach reporting tool, first class mail, or e-mail.[14,15]

If there is insufficient or out-of-date contact information for 10 or more impacted individuals, the business must post the breach notice on its website for at least 90 days or in print or broadcast media. A toll-free phone number must remain active for at least 90 days so individuals may learn if their information was involved in the breach. Notifications must be provided without delay and not later than 60 days following the discovery of a breach.[14]

Notifications must include a brief description of the breach, a description of the types of information involved, and steps affected individuals should take to protect themselves from potential harm. A brief description of what the CE is doing to investigate, mitigate harm, and prevent further breaches, and contact information are required.[14]

On a larger scale than a website posting, a media notice is required for any breach that affects more than 500 individuals. It will likely occur in the form of a press release. Media notification must be provided within 60 days and include the same information required for the individual notice.[14]

HITECH

The Health Information Technology for Economic and Clinical Health (HITECH) Act requires information technology and methods that make PHI unusable or unreadable. It is required as part of the American Recovery and Reinvestment Act of 2009 (ARRA). HITECH is a joint undertaking by the OCR, the Office of the National Coordinator for Health Information Technology (ONC), and the Centers for Medicare and Medicaid Services (CMS).[16,17]

Electronic PHI exists in pharmacy practices in a variety of systems, including electronic health records (EHR). Electronic systems are vulnerable to cyber-attacks, so all facility systems and technologies must undergo security efforts.[18]

Unexpectedly, the HITECH Act revises the Social Security Act. It establishes multiple categories of violations, multiple tiers of penalty amounts, and a maximum penalty of $1.5 million for all violations of an identical

provision.[17] Table 1 advises multiple steps for implementing security management to reduce the risk of unintended access and to reduce violations.[19]

TABLE 1: Recommended Steps and Actions for Implementing Security Management

SECURITY STEP	ACTION
Step 1: Lead the Culture, Select the Team, and Learn	Promote a culture of protecting patient privacy and security
Step 2: Document Processes, Findings, and Actions	Document policies, training and electronic record audits
Step 3: Review Existing Security of ePHI (Perform Security Risk Analysis)	Have an action plan that assigns responsibility for each risk finding
Step 4: Develop an Action Plan	Do not email PHI unless encrypted and check servers for phishing and malware
Step 5: Manage and Mitigate Risks	Establish protocols for administrative, physical, and technical safeguards; organizational standards; and policies and procedures
Step 6: Attest Meaningful Use Security-Related Objectives	Attesting is a legal statement that standards are met, including electronic health information
Step 7: Monitor, Audit, and Update Security on an Ongoing Basis	Determine what to audit and how the audit process will occur

Protected Health Information

Protected health information is any identifiable information that appears in medical records or discussions between healthcare staff (such as doctors and pharmacists) regarding a patient's treatment. It also includes billing information and any information that could be used to identify an individual in a company's health insurance records. Other unique identifying numbers, characteristics, or codes also apply.[20] Table 2 lists important identifiers that cause the information to be protected.[20,21]

Table 2: Defined PHI Identifiers

Patient Name	Birthdate	Address (anything more specific than the state)
Social security number	Phone or fax number	E-mail address
MAC* address of the network card	IP^ address	Driver license number
Vehicle identifier (license plate or VIN)	Biometric data (fingerprint, retina scan)	Medical record number
Medical device serial number	Dates of visits, admission, or discharge	Payments, bills
Photographs	Diagnostic codes	Health plan account number

*Media Access Control (MAC) address can be used by routers and switches to control access to a network
^Internet Protocol (IP) address is an identifying number for network hardware connected to a network

Protected Health Information can be disclosed in several circumstances. Public health agencies are authorized to collect health information for the purpose of preventing or controlling disease, injury, or disability. These agencies report on diseases and conduct public health surveillance, investigations, and interventions.[5]

Protected Health Information disclosure may occur from a public health agency to a foreign government agency collaborating with a US public health authority. These US authorities include the Food and Drug Administration, the Occupational Safety and Health Administration, the Centers for Disease Control and Prevention, and state and local public health departments.[5] An example of an allowed disclosure under state law includes a patient diagnosed with certain infectious diseases of public health importance that are mandated to be reported by a state or nationally (*e.g.*, monkeypox, legionellosis, tuberculosis, or Lyme disease).[22]

Protected Health Information may be disclosed, without a patient's permission, for payment, certain health care operations, ongoing treatment, and consultation between providers regarding a patient's care and referral of a patient by one provider to another.[23] Another permissible disclosure occurs when a patient begins discussing their health information while family or friends are present.[24] PHI disclosure to law enforcement is permissible if the information is needed to identify or apprehend an escapee or violent criminal.[25] Health information is no longer considered PHI if an individual has been deceased for more than 50 years.[3]

Pharmacists are actively involved with immunizations. Student immunization records can be disclosed to a school without written authorization as long as a practice setting has a parent or guardian's agreement. The practice setting must document that agreement, and state law must require the school to have such information before admitting the student. In addition, the PHI disclosed, in this case, must be limited to proof of immunization.[26]

There are no restrictions on the use or disclosure of de-identified health information. Two ways to de-identify information are either by a qualified statistician or the removal of identifiers of the individual, relatives, household members, and employers.[27]

HIPAA Compliance

A CE must make a PHI notice available to any person who asks for it, prominently post it and make it available on a website. Health plans must also provide the notice to individuals covered by a plan, must provide a notice of revisions to PHI within 60 days, and notify individuals at least once every three years.[27] The notice must include a point of contact for further information and for making complaints. The HHS OCR enforces HIPAA rules.[28] All complaints should be reported to the OCR. HIPAA violations may result in civil monetary or criminal penalties.[8]

Risk Assessment

Pharmacists' operations include awareness of cybersecurity and the clinical significance and legal implications of HIPAA violations. HHS reports receiving over 100,000 HIPAA complaints.[29] In response to a 2018 report revealing 83 percent of all breached healthcare records are caused by hackers or other IT-related issues, facilities should perform a risk assessment.[30,31]

Patients legally own their medical records. Pharmacy receipts and medication counseling are considered to be a part of a patient's medical records. Their release should be covered in a pharmacy's policies and procedures manual.[32] Data masking, encryption, and de-identification processes must be included.[33]

Compliance requires pharmacy data backup plans and contingency plans as described in the Security Rule. Contingencies should include analyzing applications, assuring data is accounted for, disaster recovery plans, emergency operations plans, and periodic testing to ensure readiness.[34]

Penalties

HHS may impose civil penalties on a covered entity of $100 per failure to comply with a Privacy Rule requirement, up to $25,000 per year for multiple violations of the same Privacy Rule.[28]

Beyond civil penalties, HHS may impose criminal penalties when a person knowingly obtains or discloses information in violation of HIPAA. The possible penalties are $50,000 and up to one-year imprisonment. The criminal penalties increase to $100,000 and up to five years imprisonment if the wrongful conduct involves false pretenses. The penalty increases to $250,000 and up to ten years imprisonment if the conduct involves the intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm. State attorneys general can also impose penalties, and criminal sanctions are enforced by the Department of Justice.[4,28]

Pharmacists are leaders on healthcare teams, providing safe and effective care. Pharmacists are also leaders in supporting policies and procedures to establish compliance and to learn from historical published violations below to maintain a strong professional reputation and avoid government investigations.

- A surgeon is fired after illegally accessing personal records of celebrities, fined $2000, and sentenced to 4 months in jail.[29,35]
- In *Hereford (Dianna)vs. Norton Healthcare Inc., et al.,* Hereford reportedly advises colleagues to wear gloves to avoid contracting hepatitis. The patient sues the hospital, stating sensitive medical information was loudly stated in the hearing range of other patients and staff.[10]
- A $1.4 million dollar verdict against Walgreens is levied when one of its pharmacists shared confidential medical information regarding a patient.[229,36]
- CVS agrees to pay $2.25 million to settle for HIPAA violations regarding the inappropriate disposal of prescription bottles and receipts.[36]
- A private practice loses an unencrypted flash drive containing protected health information, is fined $150,000, and is required to install a corrective action plan.[29]
- Malware compromises UMass Amherst data, resulting in a $650,000 fine.[30]
- In 2008, UCLA Health System was fined $865,000 after employees access medical records for celebrities like Farrah Fawcett, Britney Spears, and Maria Shriver.[29]

What's next?

Direct-to-Consumer Services and Research

Healthcare innovations, such as tests and analyses, are available directly to customers. One example is genetic testing. Large, searchable genetic databases are accessible for scientific research and consumer uses. There are poorly understood and diverse laws and rules surrounding liability,

consent, and privacy. Researchers are publishing proposals for new health information governance in the future.[38]

Health technology is advancing rapidly. Pharmacists are closely aligned with patients' right to access digital records. Data that separates from a HIPAA entity, and enters a different entity, such as a consumer software downloadable application (app), faces oversight from a different agency, the Federal Trade Commission. Regulation to address privacy protections for these apps is currently a patchwork of guidelines, and a uniform approach has not been created.[39] Pharmacists are ideally positioned as contributors to current HIPAA guidance and future new governance to ensure that PHI remains protected.

Course Test

1. Which of the following is not protected health information (PHI)?

a. Patient name
b. Telephone number
c. Biometric data
d. Temperature scan

2. Pharmacists should be aware that the Privacy Rule reveals PHI exists in _____ form.

a. electronic
b. verbal
c. written
d. All of the above

3. Which of the following is a penalty that pharmacists might encounter for failure to comply with HIPAA?

a. Criminal penalty of life imprisonment if the wrongful conduct involves false pretenses.
b. Civil penalties on a covered entity of $100 per failure to comply with a Privacy Rule requirement.
c. Twelve years imprisonment if the conduct involves the intent to sell information for commercial advantage.
d. The state Elderly Affairs Department can enforce and impose HIPAA violation penalties and sanctions.

4. A pharmacist's role is to protect identifiable patient information from inadvertent disclosure. Which of the following is PHI?

a. A brochure in the waiting area about smoking cessation programs
b. Billing information from last month's new and refill prescriptions
c. A letter to residents with a photograph of a healthy heart and exercise tips
d. Billing information from the wholesaler to the pharmacy department

5. **A patient comes to the pharmacy after being discharged from the hospital where the patient was treated for a *Legionella* infection. The patient tells you they believe HIPAA has been violated because the State Health Department called them at home asking how they contracted Legionnaires' disease. How do you respond?**

    a. Ask if they are taking university classes because health records can always be disclosed to a school without written authorization as long as the individual is actively enrolled in the university.
    b. Advise the patient to call the police because PHI about Legionella may not be disclosed without a patient's permission and someone improperly shared information after their discharge.
    c. Advise that public health agencies can collect health information for the purpose of preventing or controlling disease, and Legionella infection at extrapulmonary sites is a nationally notifiable disease that the CDC monitors.
    d. Tell the patient that everything is OK because protected health information is available to any person who asks for it, and the notice that data sharing will occur is prominently posted in hospitals and on hospital websites.

6. **A patient with asthma tearfully informs you their doctor will soon close the practice to retire, and they are afraid all their medical records will disappear. How do you respond?**

    a. Advise the patient to ask the doctor where their records will go because records can be shared when coordinating ongoing treatment between providers
    b. Be sympathetic because the patient is correct. The OCR requires medical records to be incinerated, resulting in explaining the entire medical history with a new doctor
    c. Advise the patient that HHS recommends telling their neighbors that they have asthma to determine where to go next for their pulmonary care appointments
    d. Advise the patient that everything will be OK because their prescriptions will automatically renew for 1 more year when the doctor closes their practice.

7. Which of the following is a HIPAA-associated business associate?

a. A web designer is hired to maintain the facility's website view and hours of operation, and list the services provided.
b. A company is hired to clean the practice location nightly, including vacuuming and cleaning the back rooms.
c. A company is hired to convert prescription payments into coded claims for submission to insurance.
d. A company is hired to collect parking fees from a booth for anyone visiting a university medical center.

8. Which of the following is a HIPAA violation subject to penalty?

a. Inappropriate disposal of prescription bottles and receipts
b. A private practice loses a flash drive containing total copay sales
c. Malware compromises a university team's workout documents.
d. The invoice of wholesaler items purchased is visible at the 'in' window.

9. Which of the following is not a security management step?

a. Document processes, findings, and actions
b. Attest meaningful use of security-related objectives
c. Review existing security of ePHI with risk analysis
d. Promote a culture of diversity and teamwork

10. Which of the following is permissible for de-identified data communication?

a. Pharmacy receipts and medication counseling paperwork are considered de-identified.
b. Protected health information can be de-identified with the help of a qualified statistician.
c. Searchable genetic databases are accessible for scientific use and always de-identified.
d. Federal Trade Commission regulates de-identified data in medical records and consumer apps.

References

1. Why was HIPAA created? A brief history of the HIPAA law. HIPAA Security Suite. Updated April 1, 2019. https://hipaasecuritysuite.com/why-was-hipaa-created-a-brief-history-of-the-hipaa-law/. Accessed October 8, 2022.
2. Health Insurance Portability and Accountability Act of 1996 (HIPAA). Centers for Disease Control and Prevention Public Health Professionals Gateway. Updated June 27, 2022. https://www.cdc.gov/phlp/publications/topic/hipaa.html#print. Accessed October 9, 2022.
3. 45 CFR § 160.103. 2022.
4. HIPAA compliance for pharmacies. *HIPAA Journal*. Updated April 6, 2022. https://www.hipaajournal.com/hipaa-compliance-for-pharmacies/**.** Accessed October 8, 2022.
5. FAQs about HIPAA Privacy Rule. National Healthcare Safety Network (NHSN). Centers for Disease Control and Prevention. Updated January 27, 2015. https://www.cdc.gov/nhsn/hipaa/index.html. Accessed October 10, 2022.
6. Your rights under HIPAA. HHS.gov. Updated January 19, 2022. https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html. Accessed October 8, 2022.
7. Mello MM, Adler-Milstein J, Ding KL, Savage L. Legal Barriers to the Growth of Health Information Exchange-Boulders or Pebbles? *Milbank Q.* 2018 Mar;96(1):110-143. doi: 10.1111/1468-0009.12313. PMID: 29504197; PMCID: PMC5835678.
8. Guide to privacy and security of electronic health information version 2. The Office of the National Coordinator for Health Information Technology. Updated April 2015. https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf. Accessed October 8, 2022.
9. Health Insurance Portability and Accountability Act of 1996 (HIPAA). Public Health Professionals Gateway Public Health Law. Centers for Disease Control and Prevention. Updated June 27, 2022. https://www.cdc.gov/phlp/publications/topic/hipaa.html#print. Accessed October 8, 2022.
10. HIPAA Law-definition, examples, cases, processes. Legal Dictionary. Updated April 11, 2019. https://legaldictionary.net/hipaa-law/. Accessed October 9, 2022.
11. Leonard B. Health data breaches swell in 2021 amid hacking surge POLITICO analysis finds Politico. March 23 2022. https://www.politico.com/news/2022/03/23/health-data-breaches-2021-hacking-surge-politico-00019283. Accessed October 14, 2022.

12. Annual report to Congress on breaches of unsecured protected health information for calendar year 2020. US Department of Health and Human Services Office for Civil Rights. Updated April 7, 2022. https://www.hhs.gov/sites/default/files/breach-report-to-congress-2020.pdf. Accessed October 15, 2022.
13. 45 CFR §§ 164.400-414. 2022.
14. Breach Notification Rule. Health Information Privacy HHS.gov. Updated July 26, 2013. https://www.hhs.gov/hipaa/for-professionals/breach-notification/index.html. Accessed October 8, 2022.
15. Breach Portal: Notice to the Secretary of HHS breach of unsecured Protected Health Information. Form Approved: OMB No. 0945-0001. US Department of Health and Human Services Office for Civil Rights. Updated August 20, 2021. Accessed October 12, 2022. https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf. Accessed October 12, 2022.
16. HITECH Act breach notification guidance and request for public comment. HHS.gov Health Information Privacy. Updated July 26, 2013. https://www.hhs.gov/hipaa/for-professionals/security/guidance/hitech-act-breach-notification-guidance/index.html. Accessed October 8, 2022.
17. HITECH Act enforcement interim final rule. HHS.gov Health Information Privacy. Updated June 16, 2017. https://www.hhs.gov/hipaa/for-professionals/special-topics/hitech-act-enforcement-interim-final-rule/index.html. Accessed October 10, 2022.
18. Guide to privacy and security of electronic health information. HealthIT.gov. Updated April 9, 2015. https://www.healthit.gov/topic/health-it-resources/guide-privacy-security-electronic-health-information. Accessed October 9, 2022.
19. Chapter 6 Sample seven step approach for implementing a security management process. The Office of the National Coordinator for Health Information Technology HHS. Updated April 9, 2019. https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide-chapter-6.pdf. Accessed October 8, 2022.
20. 18 PHI (Protected Health Information) identifiers. HIPAA Secure Now. Updated May 16, 2022. https://www.hipaasecurenow.com/the-18-phi-protected-health-information-identifiers/. Accessed October 13, 2022.
21. 45 CFR § 164.514. 2022.
22. Infectious Disease Reporting and Regulations for Health Care Providers and Laboratories. Mass.gov. Updated 2022. https://www.mass.gov/lists/infectious-disease-reporting-and-regulations-for-health-care-providers-and-laboratories. Accessed November 14, 2022.
23. Mello M, Adler-Milstein J, Ding K, Savage L. Legal barriers to the growth of health information exchange-boulders or pebbles? *Milbank Q.* 2018;96(1):110-143. doi: 10.1111/1468-0009.12313

24. Chapter 2 Your practice and the HIPAA rules. The Office of the National Coordinator for Health Information Technology HHS.gov. Updated April 9, 2019. https://www.healthit.gov/sites/default/files/playbook/pdf/your-practice-and-the-hipaa-rules.pdf. Accessed October 10, 2022.
25. When does the Privacy Rule allow covered entities to disclose protected health information to law enforcement officials? Health Information Privacy HHS.gov. Updated June 30, 2022. https://www.hhs.gov/hipaa/for-professionals/faq/505/what-does-the-privacy-rule-allow-covered-entities-to-disclose-to-law-enforcement-officials/index.html. Accessed October 13, 2022.
26. \Student immunizations. 45 CFR 264.512(b)(1)(vi). Health Information Privacy HHS.gov. Updated September 19, 2013. https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/student-immunizations/index.html. Accessed October 13, 2022.
27. Guidance regarding methods for de-identification of protected health information in accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. Health Information Privacy HHS.gov. Updated May 31, 2022. https://www.hhs.gov/hipaa/for-professionals/privacy/special-topics/de-identification/index.html#:~:text=As%20discussed%20below%2C%20the%20Privacy,or%20in%20combination%20with%20other. Accessed October 13, 2022.
28. OCR privacy brief summary of the HIPAA Privacy Rule. US Dept Health and Human Services Guidance Portal. Updated May 2003. https://www.hhs.gov/guidance/sites/default/files/hhs-guidance-documents//privacysummary.pdf. Accessed October 8, 2022.
29. Hsieh R. Improving HIPAA Enforcement and Protecting Patient Privacy in a Digital Healthcare Environment. *Loy U Chi Law Journal.* 2014;46:175-223. https://www.luc.edu/media/lucedu/law/students/publications/llj/pdfs/vol46/Hsieh.pdf. Accessed November 10, 2022.
30. 7 Pharmacy HIPAA violations that might surprise you. PBA Health E Elements. Updated 2022. https://www.pbahealth.com/elements/5-hipaa-violations-you-might-not-know-about/. Accessed October 10, 2022.
31. Hacking responsible for 83% of breached healthcare records in January. *HIPAA Journal*. Updated March 1, 2018. https://www.hipaajournal.com/hacking-responsible-83-breached-healthcare-records-january/. Accessed October 15, 2022.
32. Pharmacy HIPAA compliance policies procedures. Healthcare Consultants. Updated October 2021. https://pharmacy-staffing.com/pharmacy-hipaa-compliance-policies-procedures/. Accessed October 9, 2022.

33. Jordan S, Fontaine C, Hendricks-Sturrup R. Selecting Privacy-Enhancing Technologies for Managing Health Data Use. *Front Public Health*. 2022 Mar 16;10:814163. doi: 10.3389/fpubh.2022.814163. PMID: 35372185; PMCID: PMC8967420.
34. 45 CFR § 164.308. 2022.
35. Doctor gets jail time for HIPAA violation. *MPR*. Updated May 2, 2017. https://www.empr.com/home/features/doctor-gets-jail-time-for-hipaa-violation/. Accessed October 12, 2022.
36. Indiana court upholds $1.44M HIPAA privacy breach award. *HIPAA Journal*. Updated November 14, 2014. https://www.hipaajournal.com/indiana-court-upholds-1-44m-hipaa-privacy-breach-award/. Accessed October 13, 2022.
37. CVS Caremark settles FTC charges: failed to protect medical and financial privacy of customers and employees; CVS Pharmacy also pays $2.25 million to settle allegations of HIPAA violations. Federal Trade Commission. Updated February 18, 2009. https://www.ftc.gov/news-events/news/press-releases/2009/02/cvs-caremark-settles-ftc-chargesfailed-protect-medical-financial-privacy-customers-employeescvs. Accessed October 13, 2022.
38. Wolf S, Ossorio P, Berry S, et al. Integrating rules for genomic research, clinical care, public health screening and DTC testing: creating translational law for translational genomics. *J Law Med Ethics*. 2020;48(1):69–86. doi: 10.1177/1073110520916996
39. Sayeed R, Jones J, Gottlieb D, Mandel JC, Mandl KD. A proposal for shoring up Federal Trade Commission protections for electronic health record-connected consumer apps under 21st Century Cures. *J Am Med Inform Assoc*. 2021;28(3):640-645. doi: 10.1093/jamia/ocaa227

DISCLAIMER

The information provided in this course is general in nature, and it is *solely designed to provide participants with continuing education credit(s)*. This course and materials are not meant to substitute for the independent, professional judgment of any participant regarding that participant's professional practice, including but not limited to patient assessment, diagnosis, treatment, and/or health management. Medical and pharmacy practices, rules, and laws vary from state to state, and this course does not cover the laws of each state; therefore, participants must consult the laws of their state as they relate to their professional practice.

Healthcare professionals, including pharmacists and pharmacy technicians, must consult with their employer, healthcare facility, hospital, or other organization, for guidelines, protocols, and procedures they are to follow. The information provided in this course does not replace those guidelines, protocols, and procedures but is for academic purposes only, and this course's limited purpose is for the completion of continuing education credits.

Participants are advised and acknowledge that information related to medications, their administration, dosing, contraindications, adverse reactions, interactions, warnings, precautions, or accepted uses are constantly changing, and any person taking this course understands that such person must make an independent review of medication information prior to any patient assessment, diagnosis, treatment and/or health management. Any discussion of off-label use of any medication, device, or procedure is informational only, and such uses are not endorsed hereby.

Nothing contained in this course represents the opinions, views, judgments, or conclusions of RxCe.com LLC. RxCe.com LLC is not liable or responsible to any person for any inaccuracy, error, or omission with respect to this course, or course material.