Review of HIPAA, Part 2: Limitations, Rights, Violations, and Role for the Imaging Technologist

Wilnellys Moore, RT (R)(N)(MR)(AART), CNMT, and Sarah Frye, MBA, CNMT, PET, NCT, CCRP

Doisy College of Health Sciences, Saint Louis University, St. Louis, Missouri

CE credit: For CE credit, you can access the test for this article, as well as additional *JNMT* CE tests, online at https://www.snmmilearningcenter.org. Complete the test online no later than March 2023. Your online test will be scored immediately. You may make 3 attempts to pass the test and must answer 80% of the questions correctly to receive 1.0 CEH (Continuing Education Hour) credit. SNMMI members will have their CEH credit added to their VOICE transcript automatically; nonmembers will be able to print out a CE certificate upon successfully completing the test. The online test is free to SNMMI members; nonmembers must pay $15.00 by credit card when logging onto the website to take the test.

This article is the second part of a continuing education series reviewing the Health Insurance Portability and Accountability Act (HIPAA) of 1996. The term *HIPAA* should be familiar to those who work in the medical profession, but this article includes details on its rules, patients' rights, violations, breaches, and penalties. To help administer these safeguards, HIPAA requires that every organization designate a HIPAA privacy and security officer. HIPAA violations can have serious repercussions when rules are not followed; these violations can be either negligent or willful. If breaches of unsecured protected health information occur, HIPAA requires covered entities to notify affected individuals, the Secretary of Health and Human Services, and in some cases the media. Violations in which the covered entity did not know of the violation are now punishable under the first tier of penalties. Unintended violations carry a minimum penalty of $100 per violation and a maximum of $50,000 per violation. All patients have a right to privacy and a right to confidential use of their medical records. The role of medical professionals includes understanding how and when to apply these HIPAA rules verbally and electronically.

Key Words: HIPAA; violation; privacy law; patient rights; health insurance

J Nucl Med Technol 2020; 48:17–23
DOI: 10.2967/jnmt.119.227827

In this 2-part continuing education series, part 1 reviewed the history of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and its rules, including delving into the specifics of the privacy rule and the security rule. Part 2 of this article addresses some limitations of HIPAA, patient's rights under the act, and privacy and security officers. This article will address today's most common causes for HIPAA violations, showcasing how today's privacy and security challenges differ from those of years past. Periodic HIPAA training is mandatory for employees who have access to, or manage, patient data, but HIPAA rule violations continue to occur at an alarming rate (*1,2*). Although violations are not always willfully committed, the imposed penalties amount to millions of dollars in fines each year and even result in criminal charges and prison sentences (*3*). Health-care professionals have the responsibility to protect patient data and help prevent HIPAA violations in order to maintain patient trust, avoid potential legal consequences, prevent termination of employment, and prevent loss of credentials.

Received Feb. 25, 2019; revision accepted Jul. 8, 2019.
For correspondence or reprints contact: Sarah Frye, Doisy College of Health Sciences, Saint Louis University, Allied Health Building, 3437 Caroline St., Ste. 3021, St. Louis, MO 63104.
E-mail: sarah.frye@health.slu.edu
Published online Oct. 11, 2019.

HIPAA LIMITATIONS

Rather than applying to types of information, HIPAA protection applies only to covered entities that the Department of Health and Human Services (DHHS) defines as health-care providers, health plans, and health-care clearinghouses and business associates, leaving some personal information at risk (*4*). Therefore, health-care data generated by noncovered entities are not protected by HIPAA. Think about purchases made online, posts made on social media, and even the automatic upload of fitness tracker data to the Internet. All of these "data collected and traded online. . .may eventually support more accurate predictions about health than a person's medical record" (*4*). Information that is collected and shared online may be linked to individuals as demonstrated by a recent report involving Facebook and Cambridge Analytica. This report detailed how Facebook "has been approaching healthcare organizations to try to obtain deidentified patient data to link those data to individual Facebook users" using mathematic algorithms (*5*). If Facebook or those using Facebook's datasets can reidentify private data, how secure is it? This could carry the risk that private information is used in ways that have not been authorized by the individual in question (*5*).

It is also important to note that HIPAA regulations do not impose strict timelines on the release of patient records to

other health-care providers for treatment purposes or on unlawful refusal to disclose, even though a health-care provider has 30 days to provide a copy of requested information to an individual (*6*). Misinterpretation of policies might be creating treatment delays that compromise patient care (*5*). For example, physicians requesting medical records for treatment of a new patient may face unnecessary roadblocks if asked to mail or fax authorizations not required by HIPAA (*6*). Dr. Monya De, an outspoken physician and journalist, declares that HIPAA is often misused because of a lack of understanding and that "patients and their treating doctors have a right to their medical information—immediately, and without the need for any signatures or faxes" (*7*).

PATIENTS' RIGHTS

HIPAA guarantees all patients a right to privacy, a right to confidential use of their medical information, a right to access and amend their own health information on request, and a right to provide specific authorization for use of their health information for purposes other than treatment and billing. Additionally, patients have the right to have their name withheld from patient directories or account lists (*6*). HIPAA also requires that every patient receive a document, called the Notice of Privacy Practices, describing these and other patients' rights. The Notice of Privacy Practices must inform patients of the uses and disclosures of protected health information (PHI) that the facility may make and must describe patients' right to access and amend their medical information (*8*). Facilities may impose reasonable fees for the cost of copying medical records to fulfill the patient's request. The Missouri Department of Health and Senior Services updates the recommended fees based on Office for Civil Rights (OCR) guidance. Effective February 2019, the new maximum fee covering labor and supplies is $25.34 plus $0.58 per page for either paper or electronic copies, with a cap of $111.03 for electronic copies (*9*). In addition, the privacy rule requires that every patient sign an authorization form for the use or disclosure of PHI for purposes not otherwise allowed by the rule (*8*). Patients also have the right to register a complaint with the federal government or the facility if they feel that their privacy has been violated (*8*).

PRIVACY AND SECURITY OFFICERS

Proper administrative processes include having written policies and procedures that address the patient's rights, the HIPAA rules, and (previously discussed in part 1 of this series) the privacy and security rules of each facility. To help administer these safeguards, HIPAA requires that every facility designate a HIPAA privacy officer and a HIPAA security officer. The designee can be the same person, if appropriate (*2*). *Security* refers to preventing unauthorized individuals from accessing PHI, whereas *privacy* refers to the obligation to keep PHI confidential. Because no single standardized program could appropriately train employees of all entities, the HIPAA officers must tailor policies and procedures to the specific needs of the facility. The HIPAA privacy and security officers also play critical roles in implementation of, and training on, the HIPAA requirements for the facility. The HIPAA officers must also develop processes to handle privacy-related complaints and must ensure that no retaliation occurs against someone who reports a violation. The HIPAA officers must also identify the appropriate action to minimize any harm that may have resulted from a breach of privacy and must include measures (reactive to those involved or proactive to help avoid future occurrences) to be considered for employees who do not follow the policies and rules (*10*).

ENFORCEMENT, COMPLIANCE, AND AUDITING

The OCR of the DHHS is responsible for enforcing the HIPAA privacy and security rules and may act on a complaint under the following 4 circumstances: if the alleged action took place after the dates the rules took effect, if the filed complaint is against an entity required by law to comply, if the complaint describes an unlawful activity that violates HIPAA rules, and if the complaint was filed promptly (usually within 180 d of the violation) (*11*).

If the OCR initiates an investigation of a complaint, both the complainant and the covered entity are notified and asked to cooperate by presenting information about the incident in question. The Department of Justice may get involved if the complaint describes an action that violates the criminal provision of HIPAA (*11*). If the evidence indicates that a violation has taken place, the OCR will attempt to resolve the case by obtaining voluntary compliance, corrective action, or a resolution agreement (*9*). A resolution agreement is defined as a "settlement agreement signed by HHS and a covered entity or business associate in which the covered entity or business associate agrees to perform certain obligations and make reports to HHS" (*12*). Most investigations are resolved through one of these resolutions; however, the OCR may impose civil money penalties in some cases (Table 1). Before the Health Information Technology for Economic and Clinical Health (HITECH) Act, all collected penalties were deposited in the U.S. Treasury; currently, the law requires that all settlements be paid to and used by the OCR for enhancing enforcement of HIPAA rules (*11*).

HITECH requires that the OCR conduct periodic audits of covered entities and their business associates to assess compliance efforts (*11*). The OCR analyzes the policies and procedures of a facility to ensure adequate safeguarding of PHI. Compliance issues frequently investigated by the OCR include impermissible use or disclosure of PHI, lack of safeguards for PHI, denial of individuals' access to their PHI, and uses and disclosures of information that are more than minimally necessary to the medical situation (*11*).

VIOLATIONS

HIPAA violations can be classified as either negligent or willful. All health-care providers are required to receive

TABLE 1
HIPAA Civil Penalties by Type of Violation (*35*)

Violation category	Each violation	Maximum (all violations)
Did not know	$100–$50,000	$1.5 million
Should have known	$1,000–$50,000	$1.5 million
Willful neglect (corrected within 30 d)	$10,000–$50,000	$1.5 million
Willful neglect (not corrected)	$50,000	$1.5 million

periodic HIPAA training and should be familiar with privacy policies and the steps that must be taken to safeguard confidential information. Training is mandatory when regulations change, but many employers also perform training yearly or every other year (*13*). Unfortunately, mistakes happen and errors in judgment can occur.

Negligent Violations

Some examples of negligent violations include failure to protect passwords, improper disposal of PHI, failure to verify a person's identity before releasing protected information, and sharing (e.g., cellular phone messaging or social media) of insufficiently deidentified information. Because covered entities have 30 d to correct violations to avoid fines, some have adopted zero-tolerance policies that result in the termination of employees who commit unintentional or negligent violations (*11*). In April 2016, the OCR announced that it reached a $2.2 million settlement with New York Presbyterian Hospital for the egregious disclosure of 2 patients' PHI to film crews and medical staff during the filming of a television series without first obtaining authorization from the patients. In this breach, the OCR found that New York Presbyterian Hospital allowed the crew to film a patient who was dying and another patient in significant distress, even after a medical professional urged the crew to stop (*14*).

It is also important to beware of accidental social violation. An accidental violation may occur when a friend or a neighbor makes an innocent inquiry to a health-care worker about a patient. One should take the opportunity to educate the person making the inquiry that because of privacy laws, patient information cannot be disclosed. The person should be encouraged to seek information directly from the patient's family member, if possible.

Willful Violations

Willful violations often result when curiosity takes over and health-care providers access records of celebrities, coworkers, friends, relatives, or neighbors. In May 2011, 32 employees in a Minnesota hospital were terminated for inappropriately accessing medical records of patients who overdosed at a local party (*15*). Willful violations may also include providing a personal password to others, selling or using PHI for personal gain, intentionally violating security standards, and providing PHI to an individual who does not need to know the information. In August 2018, Texas Children's Hospital confirmed that a nurse was fired after she posted to Facebook information about a child who tested positive for measles (*16*). In another case, a former respiratory therapist could serve up to 1 y in jail for a conviction of criminal HIPAA violations; in this case, "the jury agreed with prosecutors that the protected health information of patients was wrongly obtained and that PHI was used to seek and obtain intravenous prescription drugs" (*17*). These examples of willful violations go directly against the rules stated in HIPAA.

BREACHES

HITECH requires that covered entities and business associates notify affected individuals, the Secretary of Health and Human Services, and in some cases the media of breaches of unsecured PHI. *Unsecured PHI* refers to "PHI that is not secure through the use of technology or methodology specified" by guidance of the law (*11*). The guidance specifies that encryption and destruction are the 2 technologies and methodologies for rendering PHI unusable and unreadable to unauthorized individuals (*18*). Any situation involving an impermissible access, acquisition, use, or disclosure of PHI that compromises the security or privacy of the PHI is presumed to be a breach unless the covered entity can demonstrate that there is a low probability that the PHI has been compromised (*17,19,20*). If at the time of the attack PHI was encrypted or indecipherable to unauthorized persons, there is a low probability that there might have been a HIPAA breach (*20*).

The most recent HITECH Act required an annual report to Congress (2013–2014) and categorized breaches by 6 different causes: theft, loss, unauthorized access or disclosure, improper disposal, a hacking or information technology incident, and unknown or other causes (*20*). In 2014, the OCR received a total of 87,278 breach reports, with 277 of these reports affecting 500 or more individuals and accounting for 98% of the individuals affected. Health-care providers involved in breaches accounted for 63% of those reports, whereas 23% involved business associates and 14% were breaches at health plans. The total number of individuals affected by these breaches in 2014 alone adds up to over 21 million (*20*). Theft incidents are the most common type of breach and were the leading cause of breaches in 2014, with over 6 million individuals affected (*1*). However, hacking or information technology breaches tend to affect a significant number of individuals, with over 7 million individuals affected in 2014 (*1,20,21*). Viruses, malware, and cyberattacks of health-care networks have resulted in anonymous, unauthorized access to systems where PHI was contained. Other reported breaches consisted of missing unencrypted backup tapes and universal serial bus (USB) drives, PHI records discarded in trash bins rather than shredded, PHI mailed to wrong addresses, and improper disposal of imaging films. One breach report alone can result

in a cascade of investigations into the covered entities involved and their associates.

Breach Cases

Breaches of HIPAA can have lasting effects on the patients affected and lasting effects on those who caused the breach. The website HHS.gov contains many reports of violations, a few of which are described here. More than $10 million in settlements were negotiated as part of corrective action plans and resolution agreements for 10 cases resulting from a single breach report for 2013–2014 (*22*). Anthem, Inc., agreed to pay $16 million in 2018 to the OCR and take substantial corrective action to settle potential violations of the HIPAA privacy and security rules after a series of cyberattacks discovered in 2015 led to the largest U.S. health data breach in history and exposed the electronic PHI of almost 79 million people (*23*). Another example of a breach is from Advocate Healthcare Network. Advocate agreed to pay a settlement of $5.55 million and adopt a corrective action plan as a result of the extent and duration of alleged noncompliance (dating back to the inception of the security rule in some instances) involving electronic PHI (*24*).

In another example, the breached party ended up being awarded $1.8 million when a Walgreens pharmacist disclosed information to the former significant other of a patient on the medications the patient was currently taking, which included medication for a sexually transmitted disease (*25*). Another case had to do with celebrity PHI being accessed. Northwestern Memorial Hospital reviewed employee PHI access logs and took decisive action over the privacy violation of snooping on celebrity medical records in January 2019; employees found to have breached HIPAA were fired (*26*). In May 2019 in Tennessee, a diagnostic medical imaging services company agreed to pay $3 million to the OCR to settle a breach exposing over 300,000 patients' PHI and chose to "adopt a corrective action plan to settle potential violations of the HIPAA Security and Breach Notification Rules" (*27*). These cases are a few of many that occur because of theft, loss, unauthorized access or disclosure, improper disposal, hacking or information technology incidents, and other causes.

Breach Reporting Requirements

Covered entities must disclose to both the patient and the government the occurrence of a breach involving unauthorized use or disclosure of unsecured PHI. After the discovery of a breach, the covered entity must notify affected individuals within 60 d by first-class mail or by e-mail if the individual has agreed to electronic notices (*20*). The secretary of the DHHS must be notified of all breaches of unsecured PHI, and the reporting requirements to other parties is determined by the number of individuals affected. For breaches involving fewer than 500 individuals, reports may be sent annually. However, breaches that involve 500 or more individuals require that the DHHS secretary be notified at the same time as the affected individuals (*20*). If the breach involves 500 or more individuals, the covered entity also must notify media outlets servicing the state in which the breach occurred no later than 60 d after discovery of the breach (*20*).

PENALTIES

The enactment of the HITECH Act resulted in increased civil penalties for HIPAA violations based on the level of willful neglect and whether the offense was corrected within the allowed 30 d (*19*). In the past, a covered entity with reasonable lack of knowledge of a violation could claim affirmative defense; however, unawareness is no longer a viable defense under the HITECH Act. Violations in which the covered entity did not know or by reasonable diligence would not have known of the violation are now punishable under the first tier of penalties. Unintended violations carry a minimum penalty of $100 per violation and a maximum $50,000 per violation. Delaying compliance carries vast risks since there are fines for willful neglect of compliance (including ignorance of the rules) that begin at $50,000 for severe infractions with a maximum annual cap of $1.5 million (*7*). Criminal penalties have not changed under the new laws (Table 2). Willful violators who obtain or disclose PHI may be fined up to $50,000 and incarcerated for up to 1 y. Violations committed under false pretenses carry up to $100,000 in penalties and 5 y in prison. Violations committed with the intent to sell PHI or cause harm to an individual carry a fine of $250,000 and incarceration up to 10 y (*7*).

NEW THREATS

The increasing availability and exchange of digitized health information support advancements in health care and public health but also increase the vulnerability of PHI. Ransomware is a type of malware that infects electronic systems and encrypts data until a ransom is paid (*28*). However, the presence of ransomware alone is not indicative of a breach of PHI. The facility must conduct a breach risk assessment to evaluate the extent to which PHI has been compromised. A thorough risk analysis can help identify potential risks and vulnerabilities of the electronic PHI that is created, saved, sent, and received by a facility.

In October 2017, the DHHS issued a clarification with guidance on how best to protect PHI when mobile devices are used (*29*). Although the DHHS recognizes the convenience and practicality of such devices, it recommends that the devices be included in the facility's risk analysis. The primary risk is that such devices might be lost or stolen

TABLE 2
HIPAA Criminal Penalties by Type of Violation (*36*)

Violation category	Fine	Incarceration
Knowingly obtain or disclose PHI	Up to $50,000	Up to 1 y
Under false pretenses	Up to $100,000	Up to 5 y
Use PHI for personal or commercial gain or to cause harm	Up to $250,000	Up to 10 y

because of their small size and portability (*30*). An example of this type of attack was first identified in 2015 when a cybersecurity company identified a previously unknown group called Orangeworm that had been observed installing a custom backdoor access into large international corporations that operate within the health-care sector in the United States, Europe, and Asia (*31*). "Known victims include healthcare providers, pharmaceuticals, [information technology] solution providers for healthcare and equipment manufacturers that serve the healthcare industry, likely for the purpose of corporate espionage" (*31*). The malware from this attack was found on machines that had software installed for the use and control of high-tech imaging devices such as radiography and MRI machines (*31*). Cybersecurity companies try to prevent attacks such as this from happening again and make efforts to notify identified targets against Orangeworm and similar operations (*31*).

THE ROLE OF TECHNOLOGISTS

Watch What Is Said and Where It Is Said

To prevent complaints of not observing privacy, avoid discussing a case in a location where other patients or visitors may hear. Do not discuss patient information in public elevators or other public areas such as hallways and cafeterias. When sharing PHI near unauthorized individuals, reasonable precautions must be taken such as lowering voices, turning backs toward others in common areas, or talking away from others (*28*). Also, remember that only the minimum health information necessary to conduct business is to be used or shared. Medical information must never be used as a form of amusement or gossip. Do not share patient information with family members, friends, news reporters, or the public without authorization. A patient must consent to discussing health information in the presence of family members or friends (*28*). A patient's verbal consent allows permission to speak with a spouse, a child, or a parent (*28*).

Do Not Mishandle Medical Records

Do not remove PHI from the medical facility. Do not give medical records to others who are not authorized to have them. Do not leave patient records, whether paper or electronic, where unauthorized people can see them. If using a whiteboard calendar for organizational purposes, do not place it in an area where it is visible to the general public. If there is a chance that someone might see it, do not write patient identifiers on the board, but list the types of studies to be performed instead.

Use Computers Wisely

Computers are to be used for business purposes only, and the monitors should not be facing the public. Do not leave computers unattended when PHI has been accessed. The employee who leaves an unattended computer with patient records visible and accessible is responsible for what others see. It is not a good idea to save PHI on USB drives or even the local hard drive; instead, it should be saved in a secure network location. "In one HIPAA violation case, a dermatology practice lost an unencrypted flash drive that contained protected health information [and] the group was fined $150,000 and was required to install a corrective action plan" (*32*).

Login information and passwords are never to be shared or displayed publicly. Hackers have been known to use computer software that guesses passwords to break into systems and steal sensitive data to use or to sell for malicious intent. Strong and complex passwords must be used and should be changed routinely. Never continue to use a default or temporary password. To maintain the security of the network, open e-mail attachments only if they are from known sources. Unsolicited e-mails might contain viruses, malware, or other harmful computer code. The use of electronic messaging, e-mail, and Internet browsers should ideally be monitored and reviewed at any time and without prior notification.

Control Access to Secure Areas

Access keys and badges should not be accessible to the public. Do not lend an access badge to unauthorized individuals. An employee might be held responsible for unlawful activities that occur in an area if that employee's badge was used to access it. Report a lost or stolen badge as soon as possible. Additionally, desks and file cabinets that contain PHI and are in public or accessible areas are always to be locked when not being used.

Beware of Social Media

Never post patient data or situational information on social media. People are often able to trace the situation to a news article or narrow down the possibilities. Even if an image has been deidentified, HIPAA is violated if the posted image can be traced to an individual's identity. An example of this occurred when a nurse in a New York clinic violated HIPAA when her sister-in-law's boyfriend was diagnosed with a sexually transmitted disease (*32*). "The nurse sent 6 text messages, warning the man's girlfriend about the disease" (*32*). The man sued the clinic and the "trial court judge dismissed the claim on the grounds that the nurse's actions were both unforeseeable and based on personal reasons" (*32*).

Verify the Patient's Identity

Never assume a patient's identity. It is acceptable to address a patient by name in a physician's office, waiting room, or lobby; however, use only the first or the last name (not both) and limit the information heard by others in the area. Escort the patient to a secured area before continuing the conversation or before asking the patient to verify 2 patient identifiers (which often include full name and date of birth) before a study. The identity of the person requesting PHI must always be verified, and the facility must make sure to have a signed consent form on file. When copying medical images onto compact disks or digital video disks, ensure that

the information is readable, correct, and belongs to the appropriate patient. Treat compact disks and digital video disks like any other medical record (*33*).

Be Careful with Electronic Devices

All electronic devices used to create, receive, maintain, or transmit electronic PHI must be approved by the facility (*29*). Electronic devices are often used with default settings that may not be secure. Covered entities must ensure that these devices are properly configured and secured before using them to access or store PHI (*29*). Users must also be trained in the dangers of using unsecured networks such as public Wi-Fi, unsecure cloud storage, and file-sharing services (*29*).

Speak Up

HIPAA is also concerned with how the facility deals with individuals who report HIPAA violations. The facility must have a policy in place to protect the rights of any person who in good faith reports a privacy violation. This policy must prohibit retaliation against anyone who files a complaint, testifies in court, assists in an investigation, or believes that a violation has taken place (*34*). If you suspect a privacy violation or see any suspicious activity, contact the facility's privacy officer or supervisor.

CONCLUSION

If PHI were compromised at a facility, who would be held responsible—the facility or the employee who causes the compromise? The answer is both. Part 2 of this series has helped establish that a facility is responsible for using all necessary safeguards for HIPAA compliance and for ensuring that there is an updated and implemented HIPAA compliance plan. Individuals, practitioners, and business associates may independently face criminal charges for mishandling PHI. Remember that everyone who handles PHI is responsible for protecting it. The cost of noncompliance penalties is substantial, and violations can potentially damage an individual's and a facility's professional reputation. Part 1 of this series stressed the history of HIPAA, the rules associated with HIPAA, and PHI. Part 2 has continued the conversation on HIPAA to convey its limitations, enforcement, violations, and penalties. Hopefully, nothing new was learned in this series and all who read this always stay up to date with HIPAA policies and procedures. If you learned something new, spread the word and remind coworkers that HIPAA is not to be taken for granted.

DISCLOSURE

No potential conflict of interest relevant to this article was reported.

REFERENCES

1. Solove DJ. HIPAA turns 10. *J AHIMA.* 2013;84:22–28.
2. 45 CFR 164.530. Government Publishing Office website. https://www.gpo.gov/fdsys/pkg/CFR-2017-title45-vol1/pdf/CFR-2017-title45-vol1-sec164-530.pdf. Accessed October 24, 2019.
3. 45 CFR 164.520. Government Publishing Office website. https://www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-sec164-520.pdf. Accessed October 24, 2019.
4. 45 CFR 164.104. Government Publishing Office website. https://www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-sec164-104.pdf. Accessed October 24, 2019.
5. Cohen IG, Mello MM. HIPAA and Protecting Health Information in the 21st Century. *JAMA.* 2018;320:231–232.
6. 45 CFR 164.502. Government Publishing Office website. https://www.gpo.gov/fdsys/pkg/CFR-2016-title45-vol1/pdf/CFR-2016-title45-vol1-sec164-502.pdf. Accessed October 24, 2019.
7. Edemekong P, Haydel M. Health Insurance Portability and Accountability Act (HIPAA). StatPearls website. https://www-ncbi-nlm-nih-gov.ezp.slu.edu/books/NBK500019/. Updated 2018 May 13. Accessed February 4, 2020.
8. De M. Understanding HIPAA, and how it can hurt health care. Center for Health Journalism website. https://www.centerforhealthjournalism.org/2016/03/29/when-misuse-hippa-hurts-health-care. Published April 9, 2016. Accessed October 24, 2019.
9. Fees for Medical Records. Missouri DHSS website. https://health.mo.gov/atoz/fees.php. Published February 1, 2019. Accessed October 24, 2019.
10. 45 CFR 164.308. Government Publishing Office website. https://www.gpo.gov/fdsys/pkg/CFR-2010-title45-vol1/pdf/CFR-2010-title45-vol1-sec164-308.pdf. Accessed October 24, 2019.
11. Annual report to Congress on HIPAA privacy, security, and breach notification rule compliance for calendar years 2013 and 2014. U.S. Department of Health and Human Services website. https://www.hhs.gov/sites/default/files/rtc-compliance-20132014.pdf. Accessed October 24, 2019.
12. Resolution agreements. HHS.gov website. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/index.html. Accessed October 24, 2019.
13. HIPAA training requirements. https://www.hipaajournal.com/hipaa-training-requirements/. Accessed. October 24, 2019.
14. Unauthorized filming for "NY Med" results in $2.2 million settlement with New York Presbyterian Hospital. HHS.gov website. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/new-york-presbyterian-hospital/index.html. Released April 21, 2016. Accessed October 24, 2019.
15. Lerner M. Allina hospitals fire 32 over privacy violation. Star Tribune. http://www.startribune.com/allina-hospitals-fire-32-over-privacy-violation/121402894/. Published May 6, 2011. Accessed October 24, 2019.
16. Leider N. Texas Children's Hospital fires nurse after posting about measles patient in anti-vaxxer Facebook group. HealthExec.com website. https://www.healthexec.com/topics/care-delivery/texas-hospital-nurse-measles-anti-vaxxer-facebook. Published August 30, 2018. Accessed October 24, 2019.
17. Criminal HIPAA case: conviction for respiratory therapist. HIPAA Journal website. https://www.hipaajournal.com/respiratory-therapist-convicted-criminal-hipaa-violations-3486/. Published June 28, 2016. Accessed October 24, 2019.
18. 45 CFR parts 160 and 164. Government Publishing Office website. https://www.gpo.gov/fdsys/pkg/FR-2009-08-24/pdf/E9-20169.pdf. Published August 24, 2009. Accessed October 24, 2019.
19. Morris K. Sing a song of HIPAA. *Ohio Nurses Rev.* 2013;88:12–14.
20. Annual report to Congress on breaches of unsecured protected health information for calendar years 2013 and 2014. HHS.gov website. https://www.hhs.gov/sites/default/files/rtc-breach-20132014.pdf. Accessed October 24, 2019.
21. Yaraghi N, Gopal RD. The role of HIPAA omnibus rules in reducing the frequency of medical data breaches: insights from an empirical study. *Milbank Q.* 2018;96:144–166.
22. Dresevic A, Mikel C. New HIPAA rules: a guide for radiology providers. *Radiol Manage.* 2013;35:34–39.
23. Anthem pays OCR $16 million in record HIPAA settlement following largest U.S. health data breach in history. HHS.gov website. https://www.hhs.gov/about/news/2018/10/15/anthem-pays-ocr-16-million-record-hipaa-settlement-following-largest-health-data-breach-history.html. Published October 15, 2018. Accessed October 24, 2019.
24. Advocate Health Care settles potential HIPAA penalties for $5.55 million. HHS.gov website. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/ahcn/index.html. Published August 4, 2016. Accessed October 24, 2019
25. Nelson J. $1.8M verdict against Walgreen for pharmacist's data breach stands. https://www.theindianalawyer.com/articles/36141-18m-verdict-against-walgreen-for-pharmacists-data-breach-stands. Published January 15, 2015. Accessed October 24, 2019.

26. 'Dozens' of Northwestern Memorial Hospital employees fired for accessing Jussie Smollett's medical records. HIPAA Journal website. www.hipaajournal.com/dozens-northwestern-memorial-hospital-employees-fired-medical-records-jussie-smollett/. Published March 8, 2019. Accessed October 24, 2019.
27. Tennessee diagnostic medical imaging services company pays $3,000,000 to settle breach exposing over 300,000 patients' protected health information. HHS.gov website. https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/tmi/index.html. Published May 6, 2019. Accessed October 24, 2019.
28. Marting R. HIPAA: Answers to your frequently asked questions. *Fam Pract Manag.* 2018;25:12–16.
29. Mobile devices and protected health information (PHI). HHS.gov website. https://www.hhs.gov/sites/default/files/october-2017-ocr-cybersecurity-newsletter.pdf. Published October 2017. Accessed October 24, 2019.
30. Freundlich RE, Freundlich KL, Drolet BC. Pagers, smartphones, and HIPAA: finding the best solution for electronic communication of protected health information. *J Med Syst.* 2017;42:9.
31. New Orangeworm attack group targets the healthcare sector in the U.S., Europe, and Asia. Symantec website. https://www.symantec.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia. Published April 23, 2018. Accessed October 24, 2019.
32. 20 catastrophic HIPAA violation cases to open your eyes. MedPro website. https://www.medprodisposal.com/20-catastrophic-hipaa-violation-cases-to-open-your-eyes. Published June 2, 2017. Accessed October 24, 2019.
33. HIPAA Compliance & Medical Imaging. Quest International website. https://www.questinc.com/company/blog-posts/hipaa-compliance-medical-imaging. Updated October 2018. Accessed October 29, 2019.
34. 45 CFR 160.316. Government Publishing Office website. https://www.gpo.gov/fdsys/pkg/CFR-2011-title45-vol1/pdf/CFR-2011-title45-vol1-sec160-316.pdf. Accessed October 24, 2019.
35. 45 CFR 160.404(b). Government Publishing Office website. https://www.gpo.gov/fdsys/pkg/FR-2009-10-30/pdf/E9-26203.pdf. Published October 30, 2009. Accessed October 24, 2019.
36. What are the penalties for HIPAA Violations? HIPAA Journal website. https://www.hipaajournal.com/what-are-the-penalties-for-hipaa-violations-7096/. Published June 24, 2015. Accessed October 31, 2019.