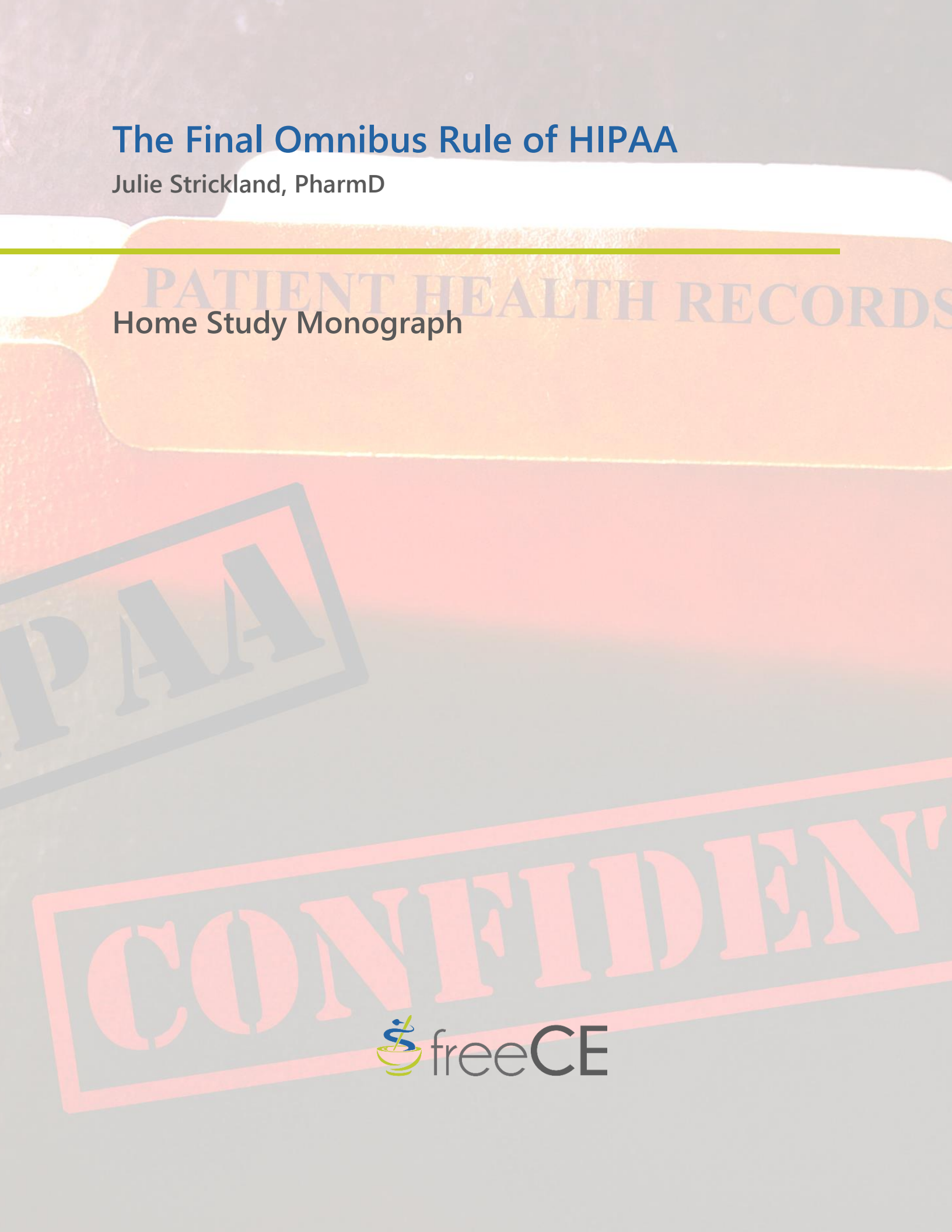
The Final Omnibus Rule of HIPAA

Julie Strickland, PharmD

Home Study Monograph



freeCE

The Final Omnibus Rule of HIPAA

ACTIVITY DESCRIPTION

The Health Insurance Portability and Accountability Act (HIPAA) is an important legal protection of an individual's rights to privacy and security of their health information. The Final Omnibus Rule posed important modifications to the existing rule to strengthen and simplify many aspects of HIPAA. This knowledge based activity will serve as a summary of the major modifications to HIPAA following adoption of the Final Omnibus Rule and highlight key enforcement issues reported by the Department of Health and Human Services.

TARGET AUDIENCE

The target audience for this activity is **pharmacists, pharmacy technicians,** and **nurses** in hospital, community, and retail pharmacy settings.

LEARNING OBJECTIVES

After completing this activity, the **pharmacist, pharmacy technician** and **nurse** will be able to:

- Describe how business associates and marketing/fundraising communications are affected by the Final Omnibus Rule
- Identify the strengths that the modifications add to the Notice of Privacy Practices
- Recognize the modification of breach notifications regarding the utilization of risk assessment rather than the risk of harm standard
- Utilizing enforcement data, recognize the most commonly investigated compliance issues and the most common types of covered entities requiring corrective action

ACCREDITATION

Pharmacy

PharmCon, Inc. is accredited by the Accreditation Council for Pharmacy Education as a provider of continuing pharmacy education.

Nursing

PharmCon, Inc. is approved by the California Board of Registered Nursing (Provider Number CEP 13649) and the Florida Board of Nursing (Provider Number 50-3515). Activities approved by the CA BRN and the FL BN are accepted by most State Boards of Nursing.

CE hours provided by PharmCon, Inc. meet the ANCC criteria for formally approved continuing education hours. The ACPE is listed by the AANP as an acceptable, accredited continuing education organization for applicants seeking renewal through continuing education credit. For additional information, please visit: http://www.nursecredentialing.org/RenewalRequirements.aspx

Universal Activity No.: 0798-0000-17-174-H03-P&T
Credits: 1.0 contact hour (0.1 CEU)

Release Date: 8/1/2017
freeCE Expiration Date: 8/1/2019
ACPE Expiration Date: 8/1/2020

ACTIVITY TYPE

Knowledge-Based Home Study Monograph

FINANCIAL SUPPORT BY

Pharmaceutical Education Consultants, Inc.

Julie Strickland, PharmD

Pharmcon

ABOUT THE AUTHOR

Dr. Julie Strickland is a PharmD graduate of the University of South Carolina College of Pharmacy. She has experience in both chain and independent pharmacy practice, including ownership, with specific interests in patient safety and promoting positive patient outcomes. She now serves in Conway, SC as the Director of Continuing Education here at PharmCon.

FACULTY DISCLOSURE

It is the policy of PharmCon, Inc. to require the disclosure of the existence of any significant financial interest or any other relationship a faculty member or a sponsor has with the manufacturer of any commercial product(s) and/or service(s) discussed in an educational activity. Julie Strickland reports no actual or potential conflict of interest in relation to this activity.

Peer review of the material in this CE activity was conducted to assess and resolve potential conflict of interest. Reviewers unanimously found that the activity is fair balanced and lacks commercial bias.

Please Note: PharmCon, Inc. does not view the existence of relationships as an implication of bias or that the value of the material is decreased. The content of the activity was planned to be balanced and objective. Occasionally, faculty may express opinions that represent their own viewpoint. Participants have an implied responsibility to use the newly acquired information to enhance patient outcomes and their own professional development. The information presented in this activity is not intended as a substitute for the participant's own research, or for the participant's own professional judgement or advice for a specific problem or situation. Conclusions drawn by participants should be derived from objective analysis of scientific data presented from this activity and other unrelated sources.

Neither freeCE/PharmCon nor any content provider intends to or should be considered to be rendering medical, pharmaceutical, or other professional advice. While freeCE/PharmCon and its content providers have exercised care in providing information, no guarantee of it's accuracy, timeliness or applicability can be or is made. You assume all risks and responsibilities with respect to any decisions or advice made or given as a result of the use of the content of this activity.

The Final Omnibus Rule of HIPAA

HIPAA Overview

By now, the Health Insurance Portability and Accountability Act (HIPAA) is familiar to all health care workers and professionals. In the pharmacy setting, every workplace environment has implemented a policy of distributing the Notice of Privacy Practices (NPP), and keeping an acknowledgement of receipt of distribution on file. All too often, HIPAA is thought of as an administrative process of paperwork that must be distributed, signed, and filed. It is not uncommon during a physician office visit, hospital visit or pharmacy encounter to hear, "Sign this Notice of Privacy Practice…it's full of legal lingo that tells all about your privacy". And most people just sign it without ever reading it and go on with their lives. That's ok for those who are not concerned with how their protected health information (PHI) is used and disclosed, but for those who may care it is an important document. If a patient has reviewed an organization's NPP and would like to request a more stringent use of their own information, they have the right to do so.

This is exactly why we need HIPAA and the Notice of Privacy Practices…so patients can be informed as to exactly how their providers will use and disclose their protected health information. And if they disagree with how it will be used, an individual can express objection or even request modification of the use of their own information. HIPAA is, and was always intended to be, so much more than simply describing the privacy of your health information. HIPAA identifies that a covered entity should never release more information than the minimum necessary to function in routine business. This includes treatment collaboration, as well as obtaining payment for services. HIPAA was created and designed to provide privacy standards to protect patients' health and medical information. Remember that prior to HIPAA, an employer could use what we now call protected health information to determine if they would employ or insure an individual. Because of individual protections of HIPAA, personal health details (such as pregnancy status, desire for additional children, financially catastrophic medical conditions, and other health information) cannot be used for employment decisions or for determination of insurance through an employer provided health insurance plan. It does not mean that premiums cannot be higher for individuals on the plan who smoke for instance, just that plan eligibility cannot be determined by asking for health information.

The Department of Health and Human Services is in charge of adopting the standards within HIPAA. Within these standards are several rules that allow for the protection and enforcement of breaches of PHI. The Office for Civil Rights enforces the HIPAA Privacy Rule, which protects the privacy of individually identifiable health information; the HIPAA Security Rule, which sets national standards for the security of electronic protected health information; the HIPAA Breach Notification Rule, which requires covered entities and business associates to provide notification following a breach of unsecured protected health information; and the confidentiality provisions of the Patient Safety Rule, which protects identifiable information

being used to analyze patient safety events and improve patient safety. That being said, so much has changed since 1996 when HIPAA was signed into law and even since 2009 when the Health Information Technology for Economic and Clinical Health (HITECH) Act was enacted. HITECH works hand in hand with HIPAA and in part addresses privacy and security concerns associated with the electronic transmission of health information, breach notification, as well as strengthened existing civil and criminal enforcement of the HIPAA rules.

Information technology advances every day, and with these advancements come reasons and new ways for protected health information to be used, disclosed or even sold. For example, in 1996 social media was almost non-existent and now a plethora of information can be spread with one click (or touch) to literally millions of people instantly. With so many new ways of transmitting and moving information, even when for legitimate purposes like e-prescribing, cloud based sharing systems and electronic records, it is essential for modifications to HIPAA/HITECH to attempt to keep up with the developing digital world. The latest modifications are named the Final Omnibus Rule. They are called the Final Rule, not because it will be the last modification, but rather because it represents a final decision of the previously written Interim Rule. This monograph will serve as a summary of the major modifications to HIPAA from the Final Omnibus Rule and highlight several situations these modifications may impact the practice of pharmacy. The Final Omnibus Rule primarily addresses strengthening rights and access to an individual's PHI and also attempts to tie up loose ends of HIPAA, especially regarding enforcement of HIPAA. The Final Omnibus Rule contains several modifications to the HIPAA Privacy, Security, and Enforcement Rules. These modifications are meant to improve existing rules and in some instances, simplify nuisance issues that have arisen from former versions of HIPAA. This monograph will address some of the major modifications to the standards and highlight situations that may affect the practice of pharmacy in various settings.

Business Associates

One major change is that business associates of covered entities are now directly liable for compliance with certain requirements of both the HIPAA Privacy and Security Rules. Including business associates under HIPAA is huge, because it means enforcement of HIPAA can occur with both the covered entity and any business associates involved. Remember that covered entities include providers of direct patient care, health plans, and health care clearinghouses (receives or transmits PHI in a nonstandard form). Business associates are persons or entities that do not have a direct relationship with the patient, but do perform functions for a covered entity that require disclosure to conduct business. Examples of business associates include third party administrators assisting with claims processing, CPA firms, legal services, consultants, document shredding/disposal businesses, and cloud service providers just to name a few.

Prior to the Final Omnibus Rule, holding business associates accountable in situations of privacy breaches was much more difficult. This should make any covered entity that needs to disclose PHI in order to conduct business, such as in the case of a document/vial disposal company, breathe a little easier knowing that a signed business associate contract binds the business associate to the same level of protection of PHI as the covered entity is held.

When conducting business with any outside vendors, be sure that business associate contracts are in place *prior* to disclosing any health information needed to conduct business. A complaint filed with the U.S. Department of Health and Human Services claimed that a chain pharmacy impermissibly disclosed the PHI of a customer to a law firm in an administrative hearing. Upon investigation, the Office of Civil Rights did not find that the law firm had disclosed the customers PHI in any impermissible way. They did, however, discover that there was not a business associate contract between the law firm and the chain pharmacy to ensure the PHI was safeguarded. If a pharmacy needs to disclose PHI to a law firm, it is the responsibility of those acting on behalf of a pharmacy to ensure that PHI is safeguarded until *after* executing a business contract with the firm. The Office of Civil Rights acknowledges that disclosure of PHI is essential to operating a business, however, safeguarding PHI is a top priority.

A sample business associate agreement is available on the U.S. Department of Health and Human Services webpage for Health Information Privacy. Simply perform a search on the website for "business associate contracts" to locate the sample on the site. This sample includes a 10-step outline to make sure that all required provisions are included in the contract. The sample also includes a sample of the language appropriate to cover each of these 10 provisions so that a covered entity and a business associate are in compliance with HIPAA rules.

One important note about disclosing PHI is that these rules are in no way meant to keep patient safety information from being reported. In the case of adverse reactions, error reporting, and any other form of patient safety, HIPAA and its modifications should never be used as a reason to refrain from reporting through proper reporting systems. Patient safety organizations that evaluate methods and procedures for covered entities, however, are considered business associates and should not be confused with error and adverse event reporting systems.

Marketing and Fundraising

Another part of the Final Omnibus Rule strengthens and limits the use and disclosure of PHI for marketing and fundraising purposes. The new rule strictly prohibits the sale of PHI without individual authorization from the individual. This means there cannot be any kind of blanket authorizations described in the Notice of Privacy Practice that would allow a covered entity to use or disclose PHI for marketing purposes.

Marketing includes communications that encourage the purchase of a product or service, where the covered entity would financially benefit from the communication. There are a few exceptions to the final rule regarding marketing communications where the covered entity can

receive financial remuneration (compensation). The first exception is marketing that involves the following: describing a health-related product or service provided by the covered entity; case management and coordination; or contact regarding alternative therapies. In these cases there is no compensation for the communication or the communication is face-to-face. For example, it is within the limits of the Final Rule for a pharmacist or practitioner who operates a diabetes clinic to recommend the purchase of a diabetic cookbook or even an instructional class about cooking diabetic friendly meals, if the products or services are provided by the covered entity. The provider may be making money from carrying these products in the office, but this is not considered marketing. This type of communication does not directly deal with the patient's treatment, but the product or service could be of value to the patient and their condition. The second exception to the no marketing without authorization rule is communications regarding refill reminders for current therapy of drugs or biologic agents. Refill reminders are allowed as long as the payment (if there is any payment) for these communications is limited to reimbursement of the cost of the communication (not a profit). Because a patient's current medication regimen is part of their treatment, it makes sense that refill reminders about a drug or biologic agent should not require authorization. The third exception receiving compensation for communications involving government or government-sponsored programs.

Marketing should not be confused with treatment options. If a physician or pharmacist discusses various treatment options or suggests particular products to a patient during the treatment process of a condition, there is no marketing or financial gain taking place and, therefore, no authorizations are needed. However, if a health plan, physician, or pharmacy sold a list of insulin dependent patient names and addresses to a glucometer company, then individual authorizations need to be attained before this information could be disclosed. The difference is clear, in the course of treatment recommendations can be made without individual authorization and in the case of advertising for financial gain, individual authorizations must be obtained.

Fundraising encompasses a large part of the funds available for medical care and advancements for many organizations. Just to name a few large organizations, The Ronald McDonald House, The American Red Cross, and St. Jude's Research Hospital depend heavily on contributions from donors. On a smaller scale, fundraising is even used to raise money for new technology to be purchased for a hospital. There are several ways that fundraising has been affected by the Final Rule. The changes in the Rule require that a covered entity provide a clear, simple way for an individual to opt out of any future fundraising communications and that a reasonable effort will be made on the part of the covered entity to ensure the individual does not receive any further fundraising communications. The Final Rule also states that a covered entity may not condition treatment based on an individual's desire to participate or opt out of fundraising communication.

Another change to the Final Rule regarding fundraising allows non-profit organizations to target donors more specifically if the donor has not chosen to opt out of fundraising communications. Before, HIPAA limited the information a covered entity could provide to "target" communications. In the past, non-profit organizations may have had access to names and zip codes of patients and former patients, but not what department of the hospital the patient was treated in. Now the Rule is more lenient allowing somewhat more of a target recipient. For example, a hospital raising money for their cancer center could target communications to patients and former patients of the oncology department where, again, prior to the Final Rule the communications could not be targeted by department. Fundraising efforts tend to be more successful when aimed at potential donors with an interest in the topic of the fundraising event.

Notice of Privacy Practices (NPP)

The Notice of Privacy Practices (NPP) serves to inform individuals as to how a covered entity will use and disclose PHI, simplify how an individual may access and restrict use and disclosure of PHI, and identify to whom and how an individual can make complaints. The NPP should be distributed to the individual at the time of first encounter, or as soon as possible following the first encounter in circumstances such as phone encounters and emergency encounters. Although much of the requirements of the NPP are familiar to healthcare professionals, the Final Omnibus Rule brings some changes to the wording, requirements, and availability of the NPP. To begin, the Final Rule requires the NPP to be predominantly posted and readily available upon request and also be available electronically in an easy to find manner on any website that the covered entity hosts. A covered entity may now email the NPP to an individual rather than provide a paper copy, with permission from the individual. Although an individual is not required to sign a NPP, it is the responsibility of the covered entity to retain acknowledgment receipts or documentation of refusal to sign for acknowledgment of receipt. It is important to note that refusal of an individual to sign an acknowledgment of receipt does not change the rights of the individual described in the NPP. In other words, not signing does not mean rejection of the content. The notice itself describes how the patient can request modification of how their PHI will be used or disclosed in a manner that is different from what is described in the NPP.

There are several changes to statements that are now required, if applicable, within the NPP. The first is that if a covered entity intends to contact an individual for fundraising purposes, it must be stated in its NPP. Another important change to the statements made in the NPP is that now an NPP must state the right of an individual to be notified following a known breach of PHI. In the past there have also been questions regarding what will or will not require an individual authorization. To elaborate and simplify the explanation of what *will* require individual authorization from the individual, the Final Omnibus Rule requires the NPP to contain a statement describing the 3 instances that require individual authorization, if these instances are applicable to the practice of the covered entity. These 3 instances are: (1) uses and disclosures

of psychotherapy notes; (2) uses and disclosures of PHI for marketing purposes; and (3) uses and disclosures not described in the NPP will require authorization from the individual. The third instance is included to allow a process for use and disclosures of PHI for situations that come up in the course of business that may not be described in a NPP of a covered entity.

The Final Omnibus Rule now requires a NPP to state that an individual has the ability to restrict healthcare providers from disclosing personal health information to their health plan concerning treatment, *if* the individual paid for the treatment out of pocket in full. This means that the money paid for treatment or service is not funded by an insurer and did not go toward any deductible for the health plan. This is a major modification from the former HIPAA standard. How does this affect a covered entity? The provider must have a procedure in place to mark or know which information has been restricted by an individual so that that health information is not disclosed to a health plan. For example, an individual is treated by a physician for a condition that the individual does not wish to be shared with his/her insurance plan. The individual pays in full for the treatment and requests that any information about the visit and treatment not be disclosed to his/her insurance plan. The physician may need to consider writing a paper prescription rather than an e-script so that the patient can take the prescription to the pharmacy and request for the medicine to not be submitted through insurance. Otherwise, the pharmacy may have received the e-script and filled it using insurance before the patient arrived. Then the individual goes to the pharmacy and pays for his/her medication out of pocket and requests the same restriction there as well. If there is not a way to "flag" the restricted information, it would be very difficult for a pharmacy, for instance, to know not to submit the claim for his/her future refill to the health plan for payment. Submitting the claim to the individual's health plan for payment, even if by accident, would be a breach of the individual's rights.

The last major modification to the content of the NPP is that the NPP must specify to whom and how an individual would file a complaint. A complaint can be filed with either a covered entity's designated HIPAA Compliance (Privacy) Officer or with the Office of Civil Rights themselves. Who and how to contact a Covered Entities HIPAA Compliance (Privacy) Officer must be stated in the NPP and it must also include that complaints may be made directly to the Office of Civil Rights. There is a complaint packet that anyone can fill out on their website.

Miscellaneous Modifications

There are several clarifications brought about with the Final Omnibus Rule that do not fall well under another category, but do affect how we handle PHI and for that reason, deserve attention.

As physicians and healthcare operations complete the move to electronic health records instead of paper charts, it becomes increasingly important to expand the access of an individual to their electronic PHI. With the adoption of the Final Omnibus Rule, an individual now has the ability to request electronic copies of records to be transmitted directly to the individual or the

individual's designee. For those records that will be partially help in chart form and partially in electronic form, the covered entity is not required, however, to produce non-electronic record in an electronic format. Allowing these records to be delivered to the patient in an electronic format should reduce cost and time associated with these requests. There are certain safeguards that the covered entity should still take to ensure that PHI is protected. The covered entity is still allowed to require requests for records to be made in writing and, if they choose, charge a fee for records. This fee is limited to the labor costs in responding to record requests. The covered entity must also make a reasonable effort to identify the individual requesting records and safeguard the PHI, which further strengthens the privacy of the individual.

Another change deals with records of deceased individuals. For many reasons, it is not uncommon for the family of a deceased individual to request medical records, medication history, etc. There is always concern as to whether it is permissible to release this PHI and to whom the PHI may be released. The Final Rule provides a standard to rely on in this case. The Final Rule specifies that PHI of a deceased individual must be protected the same as when alive for a period of 50 years. Family members, and others who were involved with the individuals care and payment *prior to death*, however, are given special leniencies to obtain the deceased individuals protected health information. This is only relevant if the deceased individual did not state or request, prior to death, wishes to not have their PHI released to anyone even if the family member was involved in the care or payment of care of the deceased. In a way, this should make it easier for a pharmacy or physician's office to answer questions or provide records to certain individuals involved in care.

Another common issue arises around students and immunization records. Prior to the Final Omnibus Rule, written authorization was required before immunization records could be sent to schools, daycares, or other facilities that, by law, are required to have the record. The Rule is now modified to allow verbal consent, which makes the hassle of obtaining these records much easier for parents and those facilities requesting immunization records. Even though the authorization no longer needs to be in writing, documentation of the authorization is still necessary.

One area of clarification that affects the operations of a pharmacy is that individuals *do* have the right to specify who can and cannot pick up their prescriptions. It is important for pharmacies to have a system in place to ensure that an individual's request is honored. This can be difficult in the typical pharmacy setting and requires planning and thought as to how to honor these requests. In most pharmacy systems, it is possible to include patient specific notes to alert the pharmacist and then the difficulty becomes alerting the other employees as to the special request.

Another miscellaneous modification to HIPAA is that health plans are prohibited from using genetic information for underwriting purposes. This includes using genetic information specific to the individual for purposes of eligibility, premiums, or pre- existing conditions. Whether considered an ethical issue or a privacy issue, it is pertinent to protect genetic information.

Breach Notification

First and foremost, breach notification requirements and penalties for violations have been in place for quite some time. The challenge is that there have been questions about who is responsible for enforcing the rules and to what extent can violations be pursued. For clarification, the Final Omnibus Rule names the U.S. Department of Health and Human Services (HHS) as the enforcing agency for covered entities and business associates. The Office of Civil Rights (within the department of HHS) leads any investigations into breach complaints. HHS defines "breach" as the "acquisition, access, use, or disclosure" of PHI that "compromises the security or privacy" of the PHI.

Of all of the areas of HIPAA modified or changed by the Final Omnibus Rule, breach notification represents the area of modification most changed from the Interim Final Rule. Prior to the Final Omnibus Rule, whenever a breach was discovered, a risk of harm assessment was the standard that a covered entity and/or their business associate would use to decide whether a breach occurred. This standard used wording that subjectively allowed a covered entity to decide whether an impermissible use or disclosure of PHI posed a *significant* risk of financial, reputational, or other harm to an individual. With the new Final Omnibus Rule, the standard has been changed to presume that a breach has occurred unless through a more objective evaluation, or risk assessment the covered entity can demonstrate a low probability that PHI has been compromised. Again, the change is that before the Final Rule the standard required evaluation to decide *if* a breach did occur and now the Risk of Harm standard is removed and replaced with a risk assessment which assumes the breach did occur unless proven otherwise. A risk assessment, at minimum, must consider each of four factors. 1) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification; 2) The unauthorized person who used the PHI or to whom the disclosure was made; 3) Whether the PHI was actually acquired or viewed; and 4) The extent to which the risk to the PHI has been mitigated. The conclusions of this evaluation must be reasonable to be used as a determination of the significance of a breach. It is important to note that risk assessments are only required if a covered entity wishes to demonstrate that a notification is not required.

The Final Omnibus Rule also clarifies some misconceptions regarding the minimum necessary principle. There has been some debate as to whether use or disclosure that violates the minimum necessary principle qualifies as a breach. The Final Omnibus Rule clarifies that violations should be evaluated just as any other security incident, but does not change the principle itself. When a covered entity is conducting business, only the minimum amount of PHI should be used or disclosed to accomplish the task. This requires a covered entity to always be conscious of what information is needed and what information they are providing. For example, if a covered entity is trying to obtain payment from an insurance company for a pain medication that requires a prior authorization, only information directly related to obtaining payment for that particular medication should be disclosed. Any other disease states or medications not directly related to the particular service should remain confidential. During the

course of trying to obtain payment, there would be no reason, for instance, to disclose that the individual also has a completely separate workers compensation plan that pays for medications related to a completely unrelated injury. Disclosing this information would be a violation of the minimum necessary principle and would be considered a breach.

Upon discovery of an impermissible use or disclosure of PHI, documentation is required to show proof of breach notification or that a risk assessment demonstrates that notification is not required. Both covered entities and business associates should have policies and procedures in place to handle notifications or risk assessments that must take place. Following a breach, training should be conducted to prevent recurrence.

In the event that it is determined that a breach has occurred, there are certain notices that must be provided. Although some of these are unchanged, there is a modification to the timing of notice. The affected individual(s) must be notified within 60 days of discovery. The media must be notified if the breach affects more than 500 individuals in one geographic area. The media outlet must be appropriate for the size of the location affected. In other words, a journal with a small area of circulation would not be sufficient for a breach in a large metropolis area. The Secretary of Health and Human Services is to be notified of breaches involving 500 or more individuals (regardless of geographic area) within 60 days after the end of the calendar year in which the breach is *discovered*. Previously, notification was required after the violation occurred. This was not always practical as discovery does not always occur in the same calendar year as the occurrence. It is also necessary for business associates to send a breach notification to affected covered entities no later than 60 days after the discovery of the breach, when the breach is within the operations of the business associate.

Enforcement of Violations

Not only is breach notification an important part of the strength that the Final Omnibus Rule adds to HIPAA, but the enforcement of violations is also strengthened. In general, the minimum penalty amount for each violation has been increased. When the Office of Civil Rights determines that there has been a violation, the violation is classified into one of four tiers. This tiered penalty scheme is adopted from the HITECH Act, with a few modifications to allow for penalty ranges per violation. Prior to the HITECH Act, the penalty was $100 per violation with a maximum yearly penalty of $25,000 for identical violations.

It is very important to note that there is *NO* maximum amount that a covered entity or business associate can be fined per year. If there are multiple violations of different provisions the maximum penalty could be applied to each differing violation. Violations of willful neglect that are not promptly corrected by the covered entity or business associate are penalized more harshly than violations that are promptly corrected or occurred unknowingly. A covered entity or business associate does have the right to appeal this civil money penalty in a hearing before an administrative law judge if they believe the penalty has been imposed unfairly.

Covered Entity / Business Associate	Penalty Per Violation	Annual Maximum Penalty*	Can Penalty be Waived by OCR?
Did Not Know	$100-50,000	$1.5 million	Yes
Reasonable Cause	$1000-50,000	$1.5 million	Yes**
Willful Neglect, Promptly Corrected**	$10,000-50,000	$1.5 million	No
Willful Neglect, Not Corrected	$50,000	$1.5 million	No

*Annual cap on all violations of an IDENTICAL provision is $1.5 million per year
**If the issue is corrected within 30 days of discovery

How violations are counted by the OCR for the purpose of calculating penalty can vary depending on the circumstances surrounding the noncompliance. For example, when multiple individuals are affected by a breach of unsecured PHI, it is expected that the number of identical violations be counted by the number of individuals involved. The major point is that by increasing the possible monetary amount and schematically arriving at a penalty amount, the Final Omnibus Rule has brought about stronger enforcement of HIPAA.

Since 2003, there have been over 158,000 HIPAA complaints. Over 25,000 of these complaints have been resolved through investigation and enforcement. These cases were resolved by The OCR requiring changes in privacy practices and other corrective actions, including monetary settlements. So far, 52 of the cases that the OCR have resulted in a settlement of over $72,929,000.00. In over 11,000 cases, the complaints have been investigated and no violations were found. In over 21,000 cases of complaints, the OCR has intervened early and provided technical assistance to covered entities and business associates, without an investigation, to address matters of HIPAA compliance. There have also been over 98,000 cases that were closed due to the complaint not being eligible for investigation. Reasons for ineligible cases include complaints alleging a violation prior to compliance date, complaints about entities not covered by HIPAA, complaints not pursued by the filer, or the activity described does not violate the Rules (such as permissible disclosures). From the data provided by HHS, only 1% of the cases are currently unresolved or being investigated.

According to data collected from the HHS from the compliance date to the present, the compliance issues investigated most are, compiled cumulatively, in order of frequency:

1. Impermissible uses and disclosures of protected health information;
2. Lack of safeguards of protected health information;
3. Lack of patient access to their protected health information;
4. Uses or disclosures of more than the minimum necessary protected health information; and
5. Lack of administrative safeguards of electronic protected health information.

The most common types of covered entities that have been required to take corrective action to achieve voluntary compliance are, in order of frequency:

1. Private Practices;
2. General Hospitals;
3. Outpatient Facilities;
4. Pharmacies; and
5. Health Plans (group health plans and health insurance issuers).

Most healthcare professionals work in one or more of these five general areas, and given the data and the most commonly violated rules, it is essential to know the HIPAA Rules that govern our practice. It takes the commitment of every employee to ensure PHI is protected. This summary of the changes brought about by the Final Omnibus Rule are intended to facilitate compliance among covered entities and business associates. Between 2013 and 2015 pharmacies moved up on this list from the fifth most common covered entity to be required to take corrective action to the fourth most common. This reveals the need for pharmacy administration and staff to work diligently to improve how PHI is handled and safeguarded.

*reviewed and accurate as of 7/17/2017.

References

78 Fed. Reg. 5566-5702 (Jan. 25,2013). Department of Health and Human Services. Office of the Secretary. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule.

45 CFR 164.502(e), 164.504(e), 164.532(d) and (e). (April 3, 2003). Business Associates.

45 CFR 164.501, 164.508(a)(3). (April 3, 2003). Marketing.

45 CFR 164.520. (April 3, 2003). Notice of Privacy Practices for Protected Health Information.

HIPAA for Professionals. HHS.gov. Last reviewed June 16, 2017

U.S. Department of Health and Human Services. (2013). Business Associate Contracts. Available at https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html. Accessed on 7/12/2017.

Exam Questions:

1) Which statement most accurately describes how the Final Omnibus Rule affects business associates?

    A) The Final Omnibus Rule eliminates regulations that keep covered entities from sharing information with business associates
    B) The Final Omnibus Rule allows business associates to directly contact individuals
    C) The Final Omnibus Rule makes business associates directly liable for compliance with HIPAA Privacy and Security Rules
    D) Business associates are not affected by the Final Omnibus Rule

2) Which of the following is considered a business associate because they require disclosure of PHI in order to conduct business with a covered entity (such as a physician's office or pharmacy)?

    A) Mail/package delivery company
    B) Prior authorization assistance company
    C) After hours cleaning company
    D) Credit card processing company

3) Regarding marketing and fundraising, which statement is true?

    A) Fundraising communications are prohibited under the Final Omnibus Rule
    B) Fundraising communications are allowed, so long as no targeting of specific individuals takes place
    C) Refill reminders are considered marketing and require individual authorization
    D) Refill reminders are not considered marketing and do not require individual authorization

4) Marketing, or communications that encourage the purchase of a product or service for which the covered entity will benefit financially, may take place without individual authorization under all the following conditions EXCEPT:

    A) The product or service is not provided by the covered entity
    B) The product or service is part of case management and coordination
    C) The product or service is provided by covered entity face-to-face
    D) The product or service promoted will not benefit the covered entity financially

5) Which statement describes how the Notice of Privacy Practices have been modified?

A) A covered entity may send the NPP to new patients in an electronic format
B) The NPP now states that an individual can restrict disclosure of PHI to a health plan if they pay for the product or service themselves in full
C) The NPP must specify to whom and how an individual can file a complaint
D) B and C only
E) A, B, and C

6) Which of the following instances does not require individual authorization?

A) The use and disclosure of psychotherapy notes
B) The use and disclosure of PHI for billing purposes
C) The use and disclosure of PHI for marketing purposes
D) The use and disclosure of PHI not otherwise described in the NPP

7) A risk assessment must consider, at a minimum, all of the following factors EXCEPT:

A) The nature and extent of the PHI involved
B) Who received the unauthorized PHI
C) Whether the individual could discover the unauthorized breach
D) Whether the PHI was actually acquired or viewed
E) The extent to which the risk to the PHI has been mitigated

8) Risk assessments are required when _____.

A) A covered entity wants to demonstrate that a breach notification is not required
B) An unauthorized disclosure of PHI has taken place
C) A risk of harm assessment deems it necessary to follow up with a risk assessment
D) All breaches regardless of the circumstances surrounding the breach

9) The #1 most commonly investigated compliance issue reported by Health and Human Services is

A) Uses and disclosures of more than the minimum necessary
B) Lack of safeguards of protected health information
C) Impermissible uses and disclosures of protected health information
D) Lack of patient access to their protected health information

10) The #1 most common type of covered entity required to take corrective action to achieve voluntary compliance is _____.

A) Private practices
B) Outpatient facilities
C) Pharmacies
D) Hospitals