The Ethics of HIPAA in the Practice of Pharmacy

By:

Michael C. Behnam

The health care industry of the world today is ever-growing and ever-changing. Health information is passed on from physicians, insurance companies, and patients themselves at higher and higher rates. At the same time though, the incidence of health care fraud is increasing at a rapid pace while our overall health system is becoming more and more complex. Due to this complex nature of the health industry, there has become a need to protect the rights of patients, especially their privacy. Sometimes deemed the 'Privacy Rule', the Health Insurance Portability and Accountability Act of 1996 (HIPAA) was created into law for the purpose of protecting the patient. Under HIPAA, the patient is treated as an individual with privacy rights; in other words, HIPAA was designed to respect the autonomy of the patient. To afford the protection of each and every patient, the health care industry, under this act, is required to standardize patient transactions not only with the patient themselves, but also with independent insurance companies acting on behalf of payment for the patient. With the creation of HIPAA, it has become a requirement for health care professionals to act with a sense of nonmaleficence; they must be careful of what kind of patient information they share with other health professionals and independent third party payors. In the sense of nonmaleficence, the more the health care professional omits from the sharing of patient information, the better it is looked upon because the patient is deemed to have their privacy rights protected to a greater degree in this manner. The ethical implications of HIPAA come into the scope of the health care industry when physicians, pharmacists, third parties, and other health care providers attempt to implement the complex rules set by HIPAA. Like many laws, the implementation of HIPAA can be subject to interpretation. To understand these ethical issues, one must first understand the basic principles of HIPAA and how they are used in practice. The following evaluation is aimed at defining the basic principles of HIPAA, how these principles are used in practice, and what key ethical implications these principles carry with them in the practice of pharmacy.

There are many principles that serve as the foundation of HIPAA. The foundation of HIPAA can be dated back to as early as the 1970s to the Privacy Protection Study Commission, which helped to articulate the case for national privacy standards for a variety of records kept on citizens\(^1\). The Clinton Health Security Act introduced during the presidency of William Clinton contains a section entitled "Privacy of Information" that sets forth the framework for the national standards created by the HIPAA regulations\(^1\). Although HIPAA was conceived in 1996, compliance with HIPAA for the health industry and its entities was not phased in until April 14, 2003. The
enforcement of HIPAA is the responsibility of the Office for the Civil Rights (OCR) within the U.S. Department of Health and Human Services (HHS). It is this department that overlooks the voluntary compliance activities and monetary penalties issued with violations of HIPAA². As stated in the executive summary HIPAA by the OCR: “The major goal of the Privacy Rule is to assure that individuals’ health information is properly protected while allowing the flow of health information needed to provide and promote high quality health care and to protect the public’s health and well being”². This Privacy Rule not only applies to paper records for the patient, but also applies to electronic patient record information and any oral communication provided by covered entities. The core premises of HIPAA surround the idea of privacy of the patient and protection of health information sharing among entities of the health care industry. The entities of the health care industry that are covered by HIPAA are not only inclusive of health care professional, but also include health plans, health care clearinghouses, and also business associates of the patient (when they are themselves a covered entity). In totality, each of these health care entities must secure the privacy of protected health information (PHI) when dealing with each patient. Protected health information is any kind of information that can identify the patient and, thus, must be de-identified by covered entities to ensure that the patients’ privacy has not been breeched. An example of what is de-identified in PHI can be seen below in table 1.
Once PHI has been de-identified, each health care entity can use this information for one of three reasons. A covered entity may use the de-identified patient information for treatment which is identified as: the provision, coordination, or management of health care and related services for an individual by one or more health care providers, including consultation between providers regarding a patient and referral of a patient by one provider to another. Another activity that is regulated under HIPAA for covered entities is that of payment which is defined as: activities of a health plan to obtain premiums, determine or fulfill responsibilities for coverage and provision of benefits, and furnish or obtain reimbursement for health care delivered to an individual and activities of a health care provider to obtain payment or be reimbursed for the provision of health care to an individual. One last reason a covered entity may use de-identified information is for that of health care operations which is defined as: quality improvement and assessment activities, competency assurance activities, conducting medication reviews, audits, or legal services, specified insurance functions, business planning, development, management, administration, and business management and general administrative activities. Although the foundation of regulation has been defined for
It must be noted that “covered entities are permitted, but not required, to use and disclose PHI, without an individual’s authorization.”

Given the foundation of HIPAA, there are some key ways that this act may be used in practice. With the de-identifiers stated, each and every covered health care entity must disclose the ‘minimum necessary’ to carry out the three health care transactions mentioned. Along with the ‘minimum necessary’, covered entities must also supply a “Privacy Notice” that must be shown or given to the patients themselves. In essence, the privacy notice must tell the patient who will be able to see and use the patient’s medical records, what uses will require the patient’s specific authorization, and that patients have the right to inspect, copy, and amend their medical records and to obtain an accounting of disclosures. With the aforementioned, there are specific situations where patients may be denied access to their medical records. These situations include ones where: a licensed health care professional has determined, in the exercise of professional judgment, that the access requested is reasonably likely to endanger the life or physical safety of the individual or another person; the protected health information makes reference to another person and the access requested is reasonably likely to cause substantial harm to such person; or the request for access is made by the individual’s personal representative and access by that person is reasonably likely to cause substantial harm to the individual or another person.

The HIPAA privacy rules apply to patients of all ages including patients who are minors. In the case of the minor, the parent, under their individual state law, has the right to access their child’s medical records as long as their access is deemed to be in consent with their individual state law. However, the minor can be in charge of their own privacy if it is the minor who lawfully consents to treatment, the minor obtains care at the direction of a court or a person appointed by the court, or the parent has agreed in advance with the health care provider that the relationship between the child and the health care provider will be confidential. Another different situation of how HIPAA is used in practice is when it is used in emergency care situations. It is in these situations where the health care provider does not need to gain authorization from the patient (as would be stated on the provider’s privacy notice) until after the emergency has ended. Semi-analogous to the situation of an emergency is that of when the patient is not available to give authorization of consent. In this situation, HIPAA allows for a type of caregiver to take charge of the patient’s care and allows for them to give consent on behalf of the patient. In addition to patients and minors, health care professional students and residents must also abide by HIPAA regulations. The OCR has suggested that hospitals “can shape their policies and procedures for minimum necessary uses and disclosures to permit medical trainees access to patients’ medical information, including entire medical records.” Another key way in which HIPAA can be applied to health care practice is when medical research is conducted. In a basic manner, HIPAA allows the use of de-identified patient records in medical/pharmacy research without patient authorization. What is allowed in research is a ‘limited data set’, meaning that patient data are stripped of most, but not all, identifiers, and the recipient or research entity signs an agreement consenting to adhere to specific limitations on use and not to identify or contact the subjects. Lastly, with the advancement of technology of today’s society, some physicians and hospitals are beginning to use computerized physician order entry.
(CPOE) and electronic signatures in an attempt to speed up dispensing processes for the patient. Under HIPAA, these processes are covered as long as the electronic signature meets four requirements which include: intent-the electronic signature must be created and affixed to the information at the time the information is “signed”, message integrity-the transmission containing an electronic signature must be confirmed as having been received intact, user authentication-when a document is electronically signed, the identity of the user must have been positively confirmed, and non-repudiation-having electronically signed a document, a user may not reasonably challenge the authenticity of his or her electronic signature.

Given the key principles of HIPAA, there are many ethical implications when applying them to the practice of pharmacy. The ethical dilemmas that occur with the use of HIPAA in practice are most attributable to the stipulations within the law itself and its heterogeneous interpretation among health care professionals. Along with these problems, the complexity and ambiguity of HIPAA is very difficult for any entity to follow by on a strict ‘line-by-line’ basis. An overlying ethical issue of HIPAA comes from its principle of using the ‘minimum necessary’ patient information when carrying out health care transactions. According to the HHS ‘minimum necessary’ guidelines a covered entity must develop and implement ‘minimum necessary’ policies and procedures within its own organization. Also, in regards to PHI, the covered entities’ policies must define who needs access to this information, the types of information needed, and conditions to access. In regards to the practice of pharmacy, the ethical problem of ‘minimum necessary’ can occur from the heterogeneous definitions given to it form each different pharmacy organization. For example, two different community pharmacy organizations may have a different policy in place for disclosing patient information. If a patient decides to switch between these two pharmacies, the transfer of information may be limited by what is allowed by one pharmacy’s ‘minimum necessary’ policy compared to the other. This can become troublesome if the new pharmacist deems it necessary to look at the patient’s old pharmacy profile to make therapeutic decisions on their drug regimens. If the previous pharmacy does not allow transfer of the patient’s previous information or does not allow the patient the ability to obtain a copy of this information for security or other reasons, this may have detrimental effects to the patient’s health. It is here that the concept of nonmaleficence can act in way that goes against the patient’s favor; the pharmacist of one pharmacy may omit information about their patient when transferring the information to another pharmacist, which may be detrimental to the patient’s health. In addition to this idea, a patient’s autonomy may not be protected in the sense that they are not in charge of what is and is not transferred from one pharmacy to another in regards their PHI.

Another ethical dilemma can be seen with the use of the ‘privacy notice’ and written consent by the patient authorizing the use of their PHI for health care operation purposes. In this situation, HIPAA mandates that each health care provider (including pharmacies) make a “good faith effort to obtain a written acknowledgment of receipt” that the patient has received the health care provider’s written notice of privacy practices. Also, pharmacists will be required to obtain a “written acknowledgment” from their patients evidencing their receipt of the pharmacy’s “notice” along with the
opportunity for patients to ask questions and make requests as to how the pharmacy should handle their PHI. A patient may refuse to sign a “written acknowledgment” that he or she has received the pharmacy’s written notice. In that case, the pharmacist may fill prescriptions for that patient, but the pharmacist must document the patient’s refusal to receive the notice and provide in writing the reason why the patient refused. The ethical problem that arises in this case is two fold. One ethical issue that arises is how well do pharmacists implement counseling of privacy practices in their practice on a day-to-day basis? Based on personal experience, our pharmacy only hands over a statement of the company’s privacy policy to the patient on a one-time basis (when the patient has a new prescription). The extent of counseling about our company’s privacy policy is almost absolute zero. In this case, the pharmacist technician or pharmacist sometimes (not a lot of times) will ask the patient to sign the company’s log book in a separate space to show a ‘proof’ to auditors that the patient has received the company’s privacy policy (not necessarily counseling about it). In this case, the pharmacist can be seen to be in violation of the normative principle of beneficence. Ideally, the pharmacist should explain what the key components of the company’s privacy policy are to the patient and ask them if they have any questions regarding the privacy policy. Omitting these activities would be regarded as the violation of beneficence. Another issue that adds on to this ethical dilemma is the privacy statement, itself, that the patient gives written consent to by signing the logbook. For example, our company’s privacy policy statement is as follows: “I have received the medication described and authorize the release of all of the information on this log and the prescription to which it corresponds to my third party plan, the underwriter, the policy holder, plan sponsor, or employer, as appropriate”. The problem with this statement is that the patient, without noticing (because the pharmacist does not advise the patient of the ‘fine print’ at the bottom of the log book), authorizes the release of all of the information in the logbook. This information cannot be considered PHI because the patient’s prescription number is included in the logbook. With this said, the patient has basically allowed for their third party or other entities (not necessarily covered by HIPAA) to look at any medication they have without them knowing even though the patient has given consent for it by signing the log book. This is an issue because the patient’s autonomy is not fully protected in this case. Even though third parties may look at what prescriptions their patients are taking without penalty, the patient may not want to waive the right for other entities (that are, again, not necessarily covered by HIPAA) to willingly do the same. This ethical issue also, again, goes back to the idea that the pharmacist is in violation of the normative principle of beneficence. In this case, the pharmacist, ideally, needs to ensure that each patient is aware of what rights they are signing away in the logbook; otherwise, if they omit this information to each patient, they are in violation of beneficence. The overall problem with the two aforementioned privacy issues is that the pharmacy environment is very fast paced and it is almost completely unrealistic for the pharmacist to counsel each patient about their HIPAA rights. The ethical issue of incomplete implementation of HIPAA rules, in this case, will be a difficult issue for pharmacists to overcome in the future unless the law is modified in some way.

The ethical nature of the pharmacy profession also comes into effect when dealing with the rights of minors under HIPAA regulations. According to the 1994 APhA
Code of Ethics\textsuperscript{7} “A pharmacist promotes the right of self-determination and recognizes individual self-worth by encouraging patients to participate in decisions about their health. In all cases, a pharmacist respects personal and cultural differences among patients.” With this statement, the pharmacist is obligated to be ideological in their practice. This may become a problem, though, when a minor asks for a pharmacist to be confidential about certain medications. For example, if the minor is obtaining birth control pills, under HIPAA, the minor is lawfully protected from parental intervention and can keep this situation secretive from their parents (if they consent to obtaining the birth control pills from the doctor and the pharmacist, they can be protected under HIPAA). In this situation, the pharmacist must oblige to keep the minor’s autonomy protected and technically can be held liable under HIPAA if they do not keep the minor’s medication purchasing record confidential from the minor’s parents. Overall, under HIPAA, the pharmacist must practice with fidelity when dealing with minors; they must oblige to the confidentiality of the minor regardless of their ethical views on the situation.

The ethical line becomes hard to discern, under HIPAA, when dealing with the rights of patients to privacy in emergency situations and situations where the patient is absent to authorize consent. Under HIPAA regulations, emergency care providers are not required to provide patients with a privacy notice at the time of rendering emergency care (the rule in a medical emergency, “treat first and ask legal questions later,” still applies\textsuperscript{1}). This caveat to HIPAA brings up the ethical question: “what is the definition of an emergency where a patient is unable to authorize consent to the use of their PHI?” Along with this stipulation, HIPAA also gives the caveat that documentation of a good-faith effort to obtain the patient’s written acknowledgment of receipt of the privacy notice after the emergency is not required. In terms of pharmacy, for example, if an HIV patient were to walk into the pharmacy and become unconscious due to something unrelated to the HIV, the pharmacist may call the ambulance for the patient without consent. However, under HIPAA, when the paramedics arrive, the pharmacist may be obligated to not give all of the information to the paramedics regarding the patient’s health status due to fact that the pharmacist did not receive consent from the patient to do so. However, if the pharmacist deemed this situation to be an emergency, they may give the paramedics as much information on the patient as possible including the fact that the patient has HIV. Although this action by the pharmacist can be helpful for the patient, the patient might not have wished for the pharmacist to give all of their health information out to the paramedics without the patient’s consent. As shown in this case, the patient’s autonomy, in the case of this and any emergency, may not be protected by the pharmacist, although the pharmacist would be attempting to act with a notion of beneficence by trying to help the patient as much as they possibly can. Another angle to missing patient consent can be seen in the pharmacy when somebody picks up medication for a patient, when the patient is unable to pick up the medication himself or herself. In this situation, the HHS has revised the regulations to allow physicians to disclose to a family member or close friend information that is “directly relevant” to that person’s “involvement with the patient’s care”. If the patient is not present or is incapacitated, the physician may “in the exercise of professional judgment” determine that such disclosure is in the “best interests” of the patient\textsuperscript{8}. The ethical issues that are derived from this case come out of the ambiguity of the statements
presented by HIPAA. In a pharmacy, someone may be able to pick up a prescription for a patient who is not present. The problem presented is that it is the pharmacist’s duty to ensure the patient correctly understands how to take the medication and any of the side effects they may feel from taking the medication (minimally). Under HIPAA, the pharmacist may deem someone to be ‘directly relevant’ to the patient’s care, however for example, would a child, visiting cousin, or other unrelated person really be ‘directly relevant’ to the patient’s care? In addition to this, would a child, visiting cousin, or other unrelated person be capable of accurately authorizing disclosure of PHI to the pharmacy in the ‘best interests’ of the patient? It is this situation that HIPAA is not completely clear on and the pharmacist must use their own ethical, professional, and legal judgment as to whether the person picking up the medication for the patient is indeed capable of carrying out this function in a manner that is completely compliant to the patient’s privacy wishes.

Although pharmacy students and residents have access to patient chart data in hospitals for the benefit of learning, there is also an ethical implication that comes with this practice. Under HIPAA, pharmacy students and residents of the pharmacy profession, as well as all other health professions, have the ability to access patient data for the benefit of learning. The problem this practice holds is that there is no definition of what and how much patient information is allowed to be viewed by the student or resident. Again, HIPAA only states that the student or resident should view the ‘minimum necessary’ information for the purpose of learning or treating a patient. An ethical implication, again, then becomes what is the “minimum necessary?” Along with this, what about patients that are not assigned to the student or resident; how much is the student or resident allowed to see for the purpose of learning? One last ethical issue is how patient authorization to consent comes into play in these situations. Under HIPAA, hospitals are required to create policies, procedures, and protocols on how the student and resident may view a patient’s information. With such an ambiguous definition as ‘minimum necessary’, though, one can expect that each and every hospital has quite a varied policy, procedure, and protocol compared to other hospitals in regard to this. As a pharmacy student or resident, it may be difficult to define and narrow down what information is pertinent to the situation for each patient and following HIPAA regulations down the letter will be difficult to achieve.

There is a growing amount of pharmacy research conducted in our society today and it is becoming more difficult to keep patient privacy at the utmost of priorities to the investigators conducting this research. In terms of privacy, uses and disclosures of individually identifiable health records for research without individual consent are permitted under the privacy regulations4. In addition to this, though, there must be an adequate plan to protect the identifiers from improper use and disclosure, and an adequate plan to destroy the identifiers at the earliest opportunity consistent with the conduct of the research4. The aforementioned terms may be ethically problematic when applying them to practice. The problem in this case, again, comes from the ambiguity of the HIPAA statement leading to heterogeneous practice in pharmacy research. Specifically, there is no clear meaning to the definition of what an ‘adequate plan’ should include to stop improper use and disclosure of patient information. There is also
no clear meaning of what an ‘adequate plan’ is to destroy the identifiers of each patient when the earliest opportunity during research would be. Under HIPAA, the investigators conducting pharmacy research would be responsible for creating their own definition of what an ‘adequate plan’ would be for protection of their patient’s privacy even though, as stated, uses and disclosures of individually identifiable health records for research without individual consent is permitted under the privacy regulations. Clearly, patient autonomy may be easily violated in this situation. However, HIPAA may also act in the opposite manner when conducting pharmacy or other medical research. For example, a three-year retrospective review of medical record data was conducted at the University of Wisconsin\(^9\). This study showed that when implementing HIPAA regulations to medical research applications to the Institutional Review Board, there was a significant drop in approval of medical research applications without revision (59%), while the number requiring revision (25%) and full IRB approval (16%) increased significantly. As a pharmaceutical research investigator, the complexity of compliance with HIPAA can possibly hinder research progress and it is up to the professional judgment of the investigator as to whether to keep ‘hold’ of their patients or tell their patients that there is no longer a study to be conducted when these complexities do hinder their research. This can become an ethical issue if a study is terminated due to complexities with HIPAA and the patient is forced miss out on a possible new disease relieving drug included in the study that they could desperately need.

Although computerized physician order entry and electronic signatures may help speed up dispensing practices in pharmacy, there is great controversy over its ethical use. Computerized physician order entry is growing with the technological advances of today’s society and, under HIPAA, physician’s are allowed to electronically sign prescriptions over to the pharmacy (community or hospital) as long as they meet the four specified requirements that were mentioned earlier. According to HIPAA, in the electronic environment, the same legal weight associated with an original signature on a paper document may be needed for electronic data\(^10\). It is the obligation of the pharmacist to act in a manner of beneficence and justice towards the patient; in this case, CPOE can make it easier for the pharmacist to make sure the patient is receiving the correct medication. However, the ethical difficulty in this case comes from the pharmacist’s perception as to whether the electronic signature meets the four specified requirements under HIPAA. If a physician electronically signs a prescription over to the pharmacy from their office, it might be difficult for the pharmacist to discern when the prescription was written which could violate HIPAA regulations. Of more concern, though, is that the pharmacist may not be in a position to verify the authenticity of the signature. Patients may easily get a hold of a physician’s DEA number and learn to mimic the physician’s signature and may fraudulently and successfully be able to send over their own prescription to the pharmacy without the pharmacist noticing the difference. It is this fact that leads to the ethical dilemma of whether pharmacists should even accept CPOE with electronic signatures or not. Under HIPAA, if the pharmacist deems the CPOE and electronic signature to be valid, then they may accept the prescription sent to them. However, the pharmacist may be partaking in an action that would be detrimental to the patient if it were the patient who was fraudulently sending the prescription to the pharmacist. The last question that remains unanswered until
Today is what kind of justice does CPOE and electronic signatures create for a patient when there is so much potential for fraud that surrounds it?

In essence, the foundation of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) is complex and ambiguous in nature. The ambiguity of HIPAA mainly derives from its less clear cut definitions. For example, HIPAA states that PHI must be used with the 'minimum necessary' patient information. Also, there are many instances where HIPAA leads hospitals and other organizations to come up with their own 'adequate policies' to ensure that HIPAA regulations are practiced in their institution and that the rights of their patients are protected. With its ambiguity and complex nature, one can expect that there is heterogeneous implementation of HIPAA in key areas of practice in pharmacy. Some key areas that HIPAA may affect in the practice of pharmacy are: privacy notices for patients and patients seeking to obtain a copy of their medical records, patients who are minors, emergency situations and situations where patients are not available to authorize consent, pharmacy students and residents' rights to access and view patient charts for the benefit of education or practice, pharmacy research, and CPOE with electronic signatures. With these key areas and many others, the pharmacist is faced with many, unique ethical dilemmas from which they must keep the patient's autonomy in tact when practicing under HIPAA regulations. Although the creation of HIPAA has helped to protect patient rights and privacy, it has also created barriers in pharmacy practice to overcome.


References


