



MEMORANDUM

HIPAA PRIVACY RULE AND LOCAL CHURCHES

In general, the HIPAA Privacy Rule does not apply to the traditional practices of local churches publicizing prayer lists and prayer requests. There are, however, some special circumstances where the HIPAA Privacy Rule or other federal or state laws may restrict these practices. In this memorandum we discuss these legal issues and provide some general guidelines for local churches to consider when disclosing health related information about parishioners and other individuals.

TABLE OF CONTENTS

Introduction	Page 2
Publicizing Prayer Lists and Requests	2
What is the HIPAA Privacy Rule?	3
Application of the HIPAA Privacy Rule to Local Churches	4
Special Situations And Privacy Concerns	5
Local Church Employees	5
Local Churches as Health Care Providers	6
State Privacy Laws	9
Summary	10
Additional Resources	12

Introduction

HIPAA. These five little letters have caused a great deal of confusion and anxiety lately. The purpose of this memorandum is to take some of the mystery out of HIPAA and address the most common questions concerning the impact of HIPAA on local churches.

It may be best to begin at the beginning. HIPAA is an acronym for the Health Insurance Portability and Accountability Act, a federal law passed in 1996. The first HIPAA rules to be implemented dealt with the portability of health insurance for individuals who changed health plans, typically, after a change in employment. The subject of this memorandum is another set of HIPAA rules – those dealing with protecting the privacy of individuals' health related information. The final version of the so called HIPAA Privacy Rule ("privacy rule") was issued by the U.S. Department of Health and Human Services ("HHS") on August 14, 2002, and became effective, in most circumstances, on April 14, 2003.

This probably comes as no surprise, but the privacy rule is both complex and astonishingly far-reaching. And because it is so vast and so new, health law professionals (and even the government) are still trying to figure out how it will apply in the myriad of situations where the privacy of an individual's health related information is an issue. Hence, it is also no surprise the general public is confused and, of course, confusion, misinformation, and fear travel much more quickly than the truth.

Perhaps you have seen some of the "scary" articles circulating around discussing the severe penalties for violating the privacy rule. Indeed there are serious civil and criminal penalties for violating the privacy rule, but not everything cited in these articles actually is a violation of the rule. Over time, most of this uncertainty and confusion will sort itself out and we will all become more familiar and comfortable with this new rule. While this memorandum can only begin to address the most basic aspects of this complex rule, we hope it can bring some clarity to the narrow issue of how it applies to local churches.

Publicizing Prayer Lists and Requests

By far, the most common questions about the impact of the new privacy rule on local churches concern a church's announcement or publication of health related information about its parishioners and other individuals. Typically, this occurs in the context of a request for prayers, or establishing a prayer list or prayer chain. After the privacy rule became effective, many churches expressed concern that these traditional practices would no longer be permitted. Fortunately, most of these concerns are unfounded:

In general, the HIPAA Privacy Rule does not apply to churches' disclosure of health related information about its parishioners or other individuals in the context of publicizing prayer requests and prayer lists.

We will discuss the legal basis for this statement in more detail below. But, as with life itself, there are few absolutes. Indeed, there are some exceptional circumstances where

the privacy rule and other federal and state laws may apply to these practices and we will discuss some of these special privacy concerns later in this memorandum.

Before we proceed with the technical legal discussion, this might be a good place to reflect on all the "chaos" caused by the privacy rule. As noted above, the privacy rule does not restrict traditional church practices in most circumstances. But all the discussion about the privacy rule has had an indirect benefit. For perhaps the first time, we have all been forced to think seriously about the issue of "privacy" - what it really means and how it should be respected. In the long run, that may be the most important legacy of this (painful) experience.

To begin understanding the legal ramifications of the privacy rule, we start with a brief overview of the rule itself.

What is the HIPAA Privacy Rule?

In the most simple terms:

The HIPAA Privacy Rule regulates the use and disclosure of "protected health information" by "covered entities."

Said another way, the privacy rule sets forth the circumstances and conditions under which a covered entity may use or disclose protected health information.

The privacy rule defines the critical terms "protected health information" and "covered entities" in great detail but the following definitions should suffice for most purposes:

Protected health information ("PHI"): Basically, any information that identifies an individual and relates to the past, present, or future: (i) physical or mental health or condition of that individual, (ii) health care provided to that individual, or (iii) payment of health care provided to that individual.

Covered entities: (i) health plans, (ii) health care providers (who electronically transmit certain health care related information), and (iii) health care clearinghouses.

It follows from the above definition that virtually all health related information will be PHI if it also identifies the individual that is the subject of the information. For example, a statement by a plastic surgeon to his next-door neighbor that "I performed cosmetic surgery on your friend, John Smith" would clearly be a disclosure of PHI (about John Smith). Furthermore, any health related information that just reasonably identifies the subject of the information will also be PHI. For example, the statement by the plastic surgeon that "I performed cosmetic surgery on a good friend of yours who lives just down the street" would probably also be PHI even though the statement does not explicitly name the individual.

In the above definition of covered entities, "health plans" include virtually all types of individual and group plans that provide or pay the cost of health care. Some examples are: health, dental, and prescription drug insurers, HMOs, Medicare, Medicaid, and employer sponsored group health plans like those typically offered by United Methodist annual conferences to clergy and church employees. (On the other hand, workers' compensation, life insurance, and short and long term disability plans are generally not "health plans" as defined by the privacy rule.)

Covered entities also include "health care providers" such as doctors, hospitals, clinics, and counseling centers, provided they transmit certain health care related information electronically. More specifically, health care providers will be covered entities if they electronically transmit health related information in connection with any of the so called "standard transactions" described in the privacy rule. These standard transactions include all the basic communications that are the "lifeblood" of third-party health care billing in America today, e.g., submitting health claims, paying health claims, inquiries about benefit eligibility, and referrals to other providers. In short, it would be a rare professional health care provider who is not a covered entity subject to the privacy rule. (Note that if a health care provider is a covered entity, it is subject to the requirements of the privacy rule when it discloses PHI in any form - oral, written, or electronic.)

Finally, "health care clearinghouses" are also covered entities. Health care clearinghouses are typically third-party billing services used by health plans and health care providers. Because these entities have little connection with the activities of local churches, they are not discussed further in this memorandum.

Application of the HIPAA Privacy Rule to Local Churches

We said earlier the privacy rule does not generally apply to a church's disclosure of health related information concerning an individual. This follows from the statement of the rule and the definitions given above. Simply put, because churches are not generally "health plans" or "health care providers" (or health care clearinghouses), they are not "covered entities" subject to the rule. Moreover, this is true whether or not the information disclosed by the church would otherwise be PHI.

What about disclosures made by individuals acting on their own, independent of the church? First, obviously nothing prohibits parishioners or other individuals from disclosing as much or as little of their own health related information to as few or as many people as they may choose - including the entire congregation. And taking this a step further, in most circumstances, it is not a violation of the privacy rule for an individual to disclose health related information about someone else. As was the case with churches, unless the individual making the disclosure is a covered entity, the privacy rule does not apply.

As an example, suppose Mary and Betty are members of First United Methodist Church. One Sunday, during the church service, Betty informs the congregation that Mary is in the hospital being treated for injuries she sustained during an assault earlier that week. Betty asks the congregation to pray for Mary's recovery. If Betty did not have Mary's

permission to inform the congregation, was the disclosure a violation of the privacy rule? No, except in the unusual case where Betty is a covered entity (or connected with a covered entity). For example, Betty (not the church) would have violated the privacy rule if Betty was Mary's doctor, a nurse at the hospital where Mary is a patient, or a claims processor for Mary's health insurance company. Otherwise, there is no violation of the privacy rule.

In summary, the privacy rule does not have the wide-ranging effect on church practices that many had feared. But there are some special circumstances where the privacy rule and other federal and state laws can be a significant concern. These special privacy issues are discussed in the next section.

Special Situations And Privacy Concerns

Local Church Employees — Disclosure of health related information about church employees can raise several privacy issues. And these issues are the same for all church employees, regardless of whether they are also parishioners of their church-employer. First, many church employees and their dependents are covered by group health plans sponsored by their church or other church organizations. While the church, in its role as employer or plan sponsor, is generally not a covered entity subject to the privacy rule, the health plan that covers the church employee is a covered entity. As discussed below, what this means is that the privacy rule will, indirectly, govern a church's disclosure of PHI about its employees and their dependents who are covered under the church's health plan.

Because they are covered entities, the privacy rule regulates the disclosure of PHI by employer sponsored health plans. But depending on the structure of the health plan and the degree of the employer's involvement in the administration of the plan, the employer may need a great deal of information from the plan, including PHI. The privacy rule permits this type of disclosure from the health plan to the employer under certain conditions.

The privacy rule permits health plans to disclose PHI to the plan's employer-sponsor for plan administration purposes, provided the employer implements specific safeguards to protect the PHI it receives from the plan. In particular, the plan sponsor must amend its health plan documents to specify which of its employees will have access to PHI and restrict those employees' access and use of PHI to plan administration functions only. Therefore, an employer's improper use or disclosure of PHI it obtained from the health plan would constitute a failure to follow the terms of the plan document and thus, could subject the employer to potential civil liability for breach of fiduciary duty or breach of contract. (It is in this way that the privacy rule indirectly regulates the disclosure of PHI by the employer who is generally not a covered entity subject to the rule.)

As an example, suppose Betty is the office manager of Metropolitan United Methodist Church. Metropolitan UMC is a very large church with many employees. Like most churches, Metropolitan UMC is not a covered entity subject to the privacy rule but it does sponsor a group health plan for its employees and their dependents through a policy written by First Insurance Company. In fact, one of Betty's duties at Metropolitan UMC

is to assist with the administration of the church's health plan. The church has amended its plan documents (as described earlier) to permit First Insurance Company to share PHI with the church for plan administration purposes. But Betty also has several other duties at the church, including, supervising the office staff and preparing the prayer requests for publication in the church bulletin.

One day, Betty gets a call from Mary, one of the church's secretaries, saying that she won't be able to come in to work for the next few days because her doctor wants her to be in the hospital while she undergoes some tests. Later that same day, while reviewing some claims for the church's health plan, Betty notices a claim for Jane, one of the assistant pastors. The claim is for cancer treatments Jane began last week before she went out of town for a church meeting. Until that day, Betty knew nothing about either Mary or Jane's medical conditions. With the best of intentions, but without asking permission from either Mary or Jane, Betty puts everything she knows about Mary and Jane in the church bulletin requesting the congregation pray for them both. How does the privacy rule apply in these two situations?

Because the church is not a covered entity, there can be no violation of the privacy rule. However, Betty's disclosure of Jane's PHI could potentially expose the church to civil liability. When Betty learned the information about Jane, Betty was wearing her plan administrator's "hat," and hence, she failed to follow the terms of the plan document by using this information for purposes other than plan administration functions. On the other hand, when Betty learned the information about Mary, Betty was wearing her "employer/employee" hat, fulfilling her duties of supervising the office staff. Because Betty did not learn the information about Mary from the plan, the disclosure did not violate the terms of the plan document. (In general, "employment records," held by the employer in its role as employer, are not considered PHI under the privacy rule. Thus, for example, the record of Mary and Jane's accumulated days of sick leave in the church's personnel files would not be PHI.) It is also important to note that we have discussed this example solely in the context of what would be "legal" and whether the church has any potential liability for Betty's actions. But there is a larger view that also considers what Betty should have done and we will return to that point in the last section of the memorandum.

Before leaving the issue of church employees, churches need to be aware that there are numerous other laws, besides the HIPAA Privacy Rule, that may restrict the disclosure of health related information about employees. For example, the Americans with Disabilities Act ("ADA") and the Family and Medical Leave Act ("FMLA") require that certain employee medical records be kept confidential. Moreover, many states also have laws regulating the disclosure of health related information about employees. In general, the law provides a great deal of protection for health related information concerning employees and churches should be extremely cautious about disclosing such information without their employees' explicit consent.

Local Churches as Health Care Providers — In some circumstances churches can be covered entities subject to the privacy rule. Recall that health care providers who transmit claims, billing, referral, or certain other types of health care related information

electronically will be covered entities subject to the privacy rule. The same is true for churches that provide health care.

For example, suppose a local church operates an inner city health clinic (which is not a distinct legal entity separate from the church). Further suppose that the clinic electronically bills Medicaid, Medicare, private insurance companies, or patients' credit cards for their services. Then the church (not just the health clinic) will be a covered health care provider subject to the privacy rule in all respects. In particular, such a church could not disclose PHI about its parishioners or other individuals in its prayer lists or church bulletin without their prior written authorization. Moreover, under a literal reading of the privacy rule, the church could not disclose such information regardless of whether it acquired it through its health care activities or from some other independent source, e.g., from a relative or a friend.

As discussed in the above example, if a local church engages in health care activities or functions that make it a covered entity, the entire church is subject to the requirements of the privacy rule, not just the part of the church that engages in the covered activities or functions. There is, however, some relief available in these circumstances. Under certain conditions, the privacy rule permits a single legal entity that is a covered entity whose activities include both covered and non-covered functions to elect to become a "hybrid entity." This election to become a hybrid entity basically frees the non-covered functions of the entity from being subject to the privacy rule.

To become a hybrid entity in accordance with the privacy rule, a covered entity must, in effect, partition itself into "components" - those that perform the functions that make the entity a covered entity (the "health care components") and those that don't perform such functions. It is not necessary to make the components themselves distinct legal entities but the covered entity must designate its various components in writing. Furthermore, the covered entity must put in place safeguards to insure that PHI does not "leak" from a health care component to its other components. If the hybrid entity is created properly, then basically, the health care components will be treated as covered entities subject to the privacy rule and the other components will not be subject to the rule.

Note that even after a covered entity becomes a hybrid entity, the covered entity is still responsible for insuring that its health care components comply with the privacy rule in all respects. For example, the health care component will need to comply with the privacy rule's administrative requirements. In the case of a covered health care provider, these requirements include developing and implementing written privacy policies and procedures, designating a privacy official, training members of its workforce on the privacy policies, and implementing safeguards to protect its data. Because of the complexity of creating a hybrid entity, we recommend churches seek professional legal advice to assist with this process.

In the example discussed earlier in this section, suppose the church designated itself as a hybrid entity with the inner city health clinic as its health care component. If there were sufficient safeguards in place to protect against disclosure of PHI by the clinic, then the customary activities of the church, including publicizing prayer lists and requests, could proceed unaffected by the privacy rule.

As an aside, a church can perform functions or services for a (legally separate) covered entity (e.g., a separately incorporated health clinic) without the church itself becoming a covered entity. However, if those functions or services require access to or use of PHI from the covered entity, the church must enter into a "business associate contract" with the covered entity. As set forth in the privacy rule, a business associate contract requires, among other things, that the business associate (i.e., the church) not make any unauthorized use or disclosure of the PHI it receives from the covered entity and to implement safeguards to insure that this does not occur. (Hence, for example, the church could not disclose any PHI it received from the covered entity in a prayer list or prayer request.) Again, a church should consult with an attorney if it provides any such services to a covered entity.

Finally, in determining whether a church is a health care provider subject to the privacy rule, it may be important to first examine whether the activities conducted or performed by the church are actually "health care" as defined by the rule. For example, the preamble to the privacy rule states:

"[H]ealth care" as defined under the rule does not include methods of healing that are solely spiritual. Therefore, clergy or other religious practitioners that provide solely religious healing services are not health care providers within the meaning of this rule, and consequently not covered entities for the purposes of this rule.

Thus, it would appear that the sole acts of placing names on prayer lists and requesting prayers for individuals cannot make a church a health care provider as defined under the privacy rule. And while this statement in the preamble about spiritual healing is helpful and important, some ambiguities remain. For example, when clergy assist individuals suffering from depression it may be difficult in some cases to clearly classify their assistance as either spiritual healing or mental health counseling. The distinction is important because spiritual healing is not covered by the privacy rule and mental health counseling is covered. But in any event, it is essential to remember that health care providers will not be covered entities unless they also transmit certain health care related information electronically. As it turns out, this electronic transmission requirement is a rough proxy for identifying entities that are fairly involved in the "business" of providing health care which excludes most (but not all) local churches. For example:

Traditional pastoral counseling provided by churches at no charge to their parishioners does not make the church a covered health care provider subject to the privacy rule.

At the other extreme would be churches that operate counseling centers with professional psychologists on staff providing services to mentally ill patients and also (electronically) billing their patients' insurance carriers for their services. These churches are almost certainly covered health care providers subject to the privacy rule.

In between these two extremes there is a lot of room and the line that separates them can be hard to find. Therefore, if you have a concern that your church may be a covered

health care provider subject to the privacy rule, we suggest you consult with an attorney who can advise you on your particular situation.

State Privacy Laws — As discussed earlier, the federal HIPAA Privacy Rule is not the only law regulating the disclosure of an individual's health related information. We noted in our discussion of church employees that the ADA and FMLA may apply in some circumstances. In addition, there are numerous state privacy laws addressing a variety of issues. For example, some states have laws restricting the disclosure of health related information about individuals with AIDS and other communicable diseases. In this section, however, we will focus on claims (lawsuits) that individuals (plaintiffs) may bring against defendants based on "invasion of privacy" or more precisely, "public disclosure of private facts." Many states recognize this type of claim in one form or another. Generally speaking, for plaintiffs to prevail on an invasion of privacy claim, they must show that the defendant publicized private facts about the plaintiff and that the defendant's actions would be offensive or objectionable to a reasonable person. (Thus, the plaintiff cannot prevail if the information disclosed was already public knowledge or if the disclosed information was insignificant or benign.)

An illustrative case is *Mitnaul v. Fairmount Presbyterian Church* decided by the Ohio Court of Appeals in 2002. (Note that this case was decided before the HIPAA Privacy Rule became effective.) The plaintiff in *Mitnaul* was at one time the Director of Music Ministries for the defendant church. While serving in that position, plaintiff was hospitalized for treatment of depression and during his hospitalization, the church placed the plaintiff on a medical leave of absence. After his release from the hospital, plaintiff and the church became involved in a dispute about the plaintiff's return to work. Ultimately, plaintiff sued the church alleging, among other things, discrimination based upon disability, retaliatory discharge, breach of contract, and invasion of privacy. The trial court granted summary judgment for the church, rejecting all of plaintiff's claims. On appeal, however, the appeals court remanded some of plaintiff's claims back to the trial court for further proceedings. One of those remanded claims was the invasion of privacy claim.

The basis of plaintiff's invasion of privacy claim was the following statement posted on the church's web site following plaintiff's release from the hospital:

We have good news for you! [Plaintiff] is returning to Fairmount after a long medical leave of absence. Since the summer of last year, [plaintiff] has been treated for bi-polar illness, a condition which at times has resulted in serious depression for him. Various therapies and medications have been tried, and finally, after much experimentation, his health has improved considerably. For that we are all very happy.

In remanding the invasion of privacy claim back to the trial court, the appeals court stated:

[W]hile the church's publication could be based upon informing the congregation of [plaintiff's] return to the church, the inclusion of the

additional personal information about his bi-polar illness could be viewed as offensive or objectionable to a reasonable person.

Obviously, this was an unfortunate case where well-meaning people unintentionally exposed their church to legal liability. While this case did not involve the HIPAA Privacy Rule, it illustrates very clearly many of the issues churches need to consider whenever they disclose health related information about an individual. In the next section, we highlight these issues.

Summary

So, where does all this leave us?

As we have seen, the HIPAA Privacy Rule does not generally apply to a church's disclosure of health related information about its parishioners or other individuals. The two important exceptions where the privacy rule is still an issue are: (1) disclosures of certain health related information about church employees (and their dependents) who are covered by the church's health plan and (2) situations where the church itself is considered to be a covered health care provider. Also, besides the HIPAA Privacy Rule, there are other federal and state laws that may limit the disclosure of such information.

Are there any policies or procedures a church could implement with respect to publicizing prayer lists and prayer requests that would guarantee the church protection against any potential legal liability?

No. There are never any guarantees. But that is not a sufficient reason for discontinuing these practices, especially in light of the Church's spiritual mission and when there are so many things a church can do to minimize its legal exposure. Specifically, here are some general principles for churches to consider when publicizing health related information about parishioners and other individuals:

Consent, Consent, and Consent — In some sense, this entire memorandum is about how much churches can legally do without obtaining the consent of the affected individuals. As it turns out, consent is not legally required in most circumstances. But this is all backwards. ***If consent is easily and readily obtainable, why not obtain it?*** It could be something as simple as the church asking the individual "Would you mind if we shared this information with the congregation?" or "Would you like us to add you to our prayer list?" After all, not only is consent the best legal protection for the church, it is a respectful and courteous thing to do.

Certainly, there are situations where obtaining consent is impractical or impossible, e.g., in the case of incapacitated individuals. In these circumstances, the legal issues discussed in this memorandum need to be considered. But such cases are probably more often the exception rather than the rule.

As a routine practice, oral consent from the individual (or when that is not possible, from a close friend or relative) should be sufficient. But if the church is disclosing particularly

sensitive information or there is some other legal concern about the disclosure, the church should consider requiring more. Obviously, as a general matter, written consent is better than oral consent and consent directly from the affected individual is better than consent from a third party on behalf of that individual. An even weaker form of "consent" is an "opt-out" procedure. In an opt-out approach, the church would regularly publish a notice, e.g., in its church bulletin, that it compiles lists of members who are ill or hospitalized as well as information about their conditions and status. The notice would further state that the church will publish this information unless an individual objects to the disclosure. Clearly, this opt-out approach is less than perfect. But the point here about all these various forms of consent is that something is always better than nothing.

TMI ("Too Much Information") — When churches disclose health related information without the individual's consent, the general rule should be "less is best." There is a significant difference between a published notice that simply says "John Smith is hospitalized and we pray for his speedy recovery" and the type of notice published by the church in the *Mitnaul* case discussed earlier. With the best of intentions, churches can expose themselves to civil liability for invasion of privacy, among other things, when they disclose private information of a sensitive or potentially embarrassing nature. Common sense can go a long way here.

Some churches have adopted an approach that largely avoids this problem by letting someone else (besides the church) disclose the details about an individual's medical condition. In the absence of prior consent, these churches simply publicize a general notice and expression of concern for the health of the individual together with contact information for a relative or close friend. Parishioners can then contact those persons for more detailed information. In this way, the relative or friend controls what information is disclosed and to whom. Moreover, the relative or friend is probably in a better position than the church to make such decisions consistent with the wishes of individuals who may be incapacitated and unable to decide for themselves.

Church Employees — As a general rule, churches should be extremely cautious about disclosing health related information concerning their employees without their consent. This is true regardless of whether the employees are also parishioners. In particular, churches can be held legally liable for disclosing health related information about employees (or their dependents) obtained through the church's health plan.

Churches as Health Care Providers — As we discussed, this is a relatively rare situation but if it is the case, the privacy rule applies in full force and effect to the entire church. Such churches who are covered health care providers should consult with an attorney to assist them in complying with the requirements of the rule.

"The Golden Rule" — Sometimes we get so focused on the law and what we have the "right to do" we lose sight of the "right thing to do." Obviously, it is essential that we try to understand and comply with the law in all cases. But sometimes the law isn't clear and frequently it is silent on what to do in particular circumstances. In these situations we need to resort to other sources of guidance. Fortunately, in the church these are not hard to find. Perhaps the best is the most well known - The Golden Rule.

When you, acting on behalf of the church, are contemplating the disclosure of health related information about someone else, first ask yourself what you would like done if you were in a similar position. Would you care whether you were first asked for your permission before disclosing the information? If you were incapacitated, would you prefer your family or friends to decide what should be disclosed and to whom? Would you possibly be embarrassed if this particular information was publicly disclosed? The answers to these questions will go a long way toward pointing us all in the right direction.

Additional Resources

<http://answers.hhs.gov> - The U.S. Department of Health and Human Services (HHS) web site containing "Questions and Answers" about the HIPAA Privacy Rule.

<http://www.hhs.gov/ocr/hipaa/> - The HIPAA web site of the Office for Civil Rights, HHS. (The Office for Civil Rights is the office within HHS responsible for enforcing the HIPAA Privacy Rule.)

This memorandum is intended to provide general information on certain topics. It is not intended to constitute legal advice and The General Council on Finance and Administration does not provide legal advice. If you have any questions concerning the application of the law to your particular circumstances, please consult with an attorney.