

Article 29

HIPAA for Dummies: A Practitioner's Guide

Melissa Niccole Freeburg and Ann Maureen McCaughan

Introduction

Six months ago, we walked into the conference room of the nonprofit mental health clinic that we work at only to be met by the stressed-out faces of four counseling peers. The news was that our clinic was to have a HIPAA review. We thought amongst ourselves, “HIPPA, they do reviews? And who exactly runs HIPAA?” We have heard of the privacy act, and as patients know the utter annoyance felt when signing the paperwork doctor visit after doctor visit. As providers, we know that compliance is necessary to safeguard our clients. Some of us even have a few basic concepts picked up at random from sources we can no longer remember to give credit to. We bet you do too.

At a psychiatric hospital one of us worked at on April 14, 2003, the date of compliance for HIPAA, the facility had a Compliance Officer who gave a brief seminar on the topic. But let's face it, back then I thought it was that guy's problem, not mine. Now that the ball was in my court it was time to buff up on the needs of our private practice.

During our review of how our current facility works it was shocking for us to realize the lack of general knowledge of our peers, and, of course, like many other things in our profession, the “gray”

area of it all. In the true spirit of the now famous ‘How To’ books, these authors have broken up a ‘Must do’ for practicing counseling professionals in manageable bites. So, for those entering into your first private practice, wait to hang up your shingle until you read the rest of this article, for your and your client’s safety (although you may want to order those business cards so they’ll be ready around the same time as you are).

HIPAA Basics

First, let’s get familiar with the acronyms. HIPAA stands for the Health Insurance Portability and Accountability Act (1996). HIPAA was enacted by the U.S. Congress in 1996. Those thoughtful people gave health professionals until April 14, 2003 to comply fully with all properties of the act. For those of you counting, that was seven years to get things in order. Lucky for you, with the help of this article, it will not take that long. The intent of this Act is to protect clients, reduce fraud, improve quality of health care, and set strict standards for how private information about clients is transmitted (the widespread use of electronic data transmissions made things faster but is considered risky; HIPAA, 1996). Think about the American Counseling Association (ACA) ethics code. Like the ethics code, HIPAA was presented to ensure that health providers have common standards of practice, legitimacy, and to protect our clients.

Ready for the next acronym? This is an important one, PHI, which stands for Protected Health Information. This concept is the backbone, the purpose, of HIPAA in that information must be protected for privacy and security. Finally, TPO stands for Treatment, Payment and Operations. This final acronym is really just interchangeable with PHI. Just think, now you can impress your friends by interchanging acronyms on your whim!

Next, get on-line and save <http://www.hhs.gov/ocr/hipaa> and <http://www.hipaa.org> on your browser’s favorites or the equivalent based on the service you use. Then, get into your email account and save these two addresses, AskHIPAA@cms.hhs.gov (transaction/code set issues) and ocrprivacy@hhs.gov (privacy questions). Finally, go

to the phone and save the Office for Civil Rights (OCR) hotline number (1-800-537-7697). Now, at the ease of your fingertips you can have your questions answered. Face it, there is no way we can cover it all for you here.

The biggest asset you just gained for yourself is that of our government's Office for Civil Rights (OCR) web page. Spend some time making your way through all of the links. The web page offers a wealth of information under seven main categories: What's New in Privacy, For Consumers, General Background Information, HIPAA Regulations & Standards, Educational Materials, HIPAA-Related Links, and Compliance & Enforcement. While you are there make sure to sign up for the Privacy Listserv (occasional emails will be sent to your account to help you stay current) and get your printer warmed up. Our suggestion is to print off the complete Act and the Fact Sheets, just to get started. Then move on over to the Education Materials and start from the top, we particularly like the sample Business Associate contract. Make sure to take advantage of the forms available in Spanish too!

Something important to know is that in some cases a clinic may not be required to adhere to the rules and regulations of HIPAA. The Office for Civil Rights will definitely help you decipher whether or not you need to maintain compliance. Not having to would be a relief wouldn't it? Don't get too excited, whether or not you *have* to maintain compliance, our suggestion is to go ahead and do so. First, you may eventually evolve into a practice in which you will have to be in compliance, and hey, look you already are! Second, it simply gives you professionalism, it will legitimize your work, and increase confidentiality for your clients, and are they not who you work for?

Title I

Now, let us shift our focus to the materials included in HIPAA. In a snapshot, this regulation is broken up into two Titles. Title I: *Health Care Access, Portability, and Renewability* is designed to protect health insurance coverage for workers and their families when they change or lose their jobs. This title stops group health

plans from creating eligibility rules or assessing premiums for individuals in the plan based on health status, medical history, genetic information, or disability (HIPAA, 1996). Also, limits on restrictions that a group health plan can place on benefits for preexisting conditions are provided. Title I also forbids individual health plans from denying coverage or imposing preexisting condition exclusions on individuals who have at least 18 months of creditable group coverage without significant breaks (any 63 day period) and who are not eligible to be covered under any group, state, or federal health plans at the time they seek individual insurance (HIPAA, 1996).

Title II

Title II: *Preventing Health Care Fraud and Abuse; Administrative Simplification; Medical Liability Reform*, is broken into five rules. These rules include: The Privacy Rule; The Transactions and Code Sets Rule; The Security Rule; The Unique Identifiers Rule; and The Enforcement Rule. This title is focused on defining offenses relating to health care and sets civil and criminal penalties for them. The rules apply to health plans, health care clearinghouses, billing services, community health information systems, and health care providers (you) that transmit health care data (HIPAA, 1996).

Privacy Rule

Two of the Title II rules are of the most interest to us as providers: The Privacy Rule and The Security Rule. The Privacy Rule establishes regulations for the use and disclosure of PHI (HIPAA, 1996). In case you have already forgotten, PHI is Protected Health Information. *Generally*, PHI is any information about health status, provision of health care, payment, and medical records (HIPAA, 1996). Basically, *anything* that identifies an individual. Now you can see why TPO (Treatment, Payment and Operations) is an interchangeable acronym with PHI. Now you have a general idea of what PHI is, ready for the specifics? The list reads as follows: name

address, name of relatives, name of employers, date of birth, telephone number, fax number, e-mail address, social security number, medical record/account number, health plan number, certificate/license number, any vehicle or serial number, URL, finger or voice prints, photographic images, and any other unique identifying code or characteristic (HIPAA, 1996). Which even means using the word “blonde” in an elevator could be a violation (as if talking about a client in an elevator isn’t bad enough).

A common concern for providers is the terms in which information can, should, or must be disclosed. If your client requests their information you have 30 days to provide it. Also, by law a provider can be required to disclose information. For example, if child abuse is a concern with a client then your state child welfare agency requires some identifiable information. Give it to them, but limit what you provide to the minimal amount that still allows you to achieve your intended purpose.

So now that you know that information can leave your office it is time to hear the catch. The Privacy Rule requires that you keep a record of your disclosures (HIPAA, 1996). For a counselor this means that you should chart your interactions with others, file your Release of Information forms, and make sure you have privacy policies and procedures created and available upon request. Ready to add a new title to your resume? Your private practice needs to appoint a Privacy Official and contact person responsible for receiving complaints, and train all members of your office how to handle PHI.

Security Rule

The Security Rule is broken into three specific types of security safeguards: administrative, physical, and technical. For each of the three types the Rule identifies security standards and both required and addressable implementation specifications. Required specifications are *a must* and are expected to be followed down to the letter. The term addressable means there is some flexibility so that a clinic can evaluate how to best address the specifications with consideration to their unique situation (HIPAA, 1996). *Administrative*

Safeguards are the policies and procedures designed to clearly show how your practice will comply with HIPAA (1996). Make a list and start checking things off. First, write a set of privacy procedures and make sure to cite: the Privacy Official, reference management (who will also be in compliance with security and any one that will have access to PHI), authorization, establishment, modification, and termination. Second, make a plan that outlines ongoing training regarding the handling of PHI. Third, if you use any outside business as a support to your practice, such as a transcription company, make sure to ensure that they also have a framework in place to comply with HIPAA requirements. Fourth, create a contingency plan for responding to emergencies, include data priority and failure analysis, testing activities, and change control procedures. Fifth, make a plan for internal audits to monitor security violations. In this plan, document the scope, frequency, and procedure of audits. Audits need to be routine and event-based, meaning if something seems fishy, do an audit. The final component of your procedure creations is that of a document that addresses how security breaches that are discovered will be addressed. Remember, you do not have to reinvent the wheel. Examples of these procedures are available through the web site you so smartly saved.

Physical Safeguards are those expectations to physically monitor any inappropriate access to protected data. This part of the Rule states that hardware and software must be introduced to your clinic safely and be removed properly (HIPAA, 1996). For example, if you hire a technician to come into your clinic to add new technology, make sure they can not access clients' information. If you decide to get a new computer, make sure the old one is completely cleared out before you donate it. Keep your records in a place that no one can get to unless they are authorized. Employ the double lock rule, which means that someone must get through two locks before getting to any PHI (e.g., locked door to file room and locked filing cabinet). Now, PHI is not the only information you need to keep in secure areas, do not forget the facility security plans, maintenance records, visitor sign-in, and even parking permit lists, just to name a few (HIPAA, 1996).

The design of your office must also be a physical safeguard in itself. Have the workstations removed from high traffic areas and make sure your computer screens face away from anyone other than the person sitting at the desk. Computer screen attachments are available that add additional safety in that the user must be directly in front of the screen to view material. Critically examine the work places and remember that ancillary workers such as cleaning staff and paper shredding companies may make their way through the areas and you are responsible for their training or ensuring their knowledge of physical access responsibilities (HIPAA, 1996).

Technical Safeguards speak to your responsibility to govern your computer systems and people you deal with through technological means (fax, email, phone, etc.). Think to yourself, “How will I ensure the person I intend to receive this material REALLY receives it?” To do this, you should employ encryption systems and make sure that the people you deal with do the same (HIPAA, 1996). Remember, you need to have your plan for virtually everything written out and you should make them available to the government to prove that your counseling practice is in compliance.

Compliance

Compliance is taken seriously by the United States Government. Just say the word “audit” and watch people sweat. As with any offense there comes fines and time behind bars. Compliance violations start with \$100 fines and can go all the way up to \$250,000 and 10 years in prison (HIPAA, 1996). Value your clients and do not ever consider compromising their privacy whether inadvertently or with intent for personal gain.

Now, after hearing those scary fines we imagine you are ready to throw in the towel and just hire some outside consultant to come in and do it for you. You need to be aware that there have been reports of fraudulent consulting companies claiming to have the endorsement of the Office of Civil Rights. If you decide the task is too challenging, first, review the web sites again and seek support through the email addresses and hotline number you saved earlier.

Second, go to your favorite book retailer and ask them to help you find a resource guide, there are a number of quality books in publication focused completely on HIPAA regulations. If you still feel the need to hire a consultant, demand them to show you proof of their accreditation by the United States Government, Office of Civil Rights, and then follow that up by checking with the Office itself to confirm the legitimacy of the accreditation.

Conclusion

If you take nothing else from this article, please remember to use the Office of Civil Rights by emailing or phoning them to seek consultation. Keep in mind that there are simple ways to ensure the safety of our clients and their sensitive materials. For example, knock on doors before entering, use professional shredding companies to ensure proper disposal, do not talk about clients in public areas, clear PHI from your computer screen before walking away, do not leave messages on answering machines regarding clients, and do not mix PHI files with other files.

References

- Health Insurance Portability and Accountability Act (HIPAA) of 1996, P.L. 104-191, 119 Stat.
- United States Health and Human Services. (2007). *Office of civil rights – HIPAA*. Retrieved October 26, 2007, from <http://www.hhs.gov/ocr/hipaa>