Okay, We've Entered the World of Privacy… So What Now?
An Inside Look at Employer/Plan Sponsor Real-World Applications for the HIPAA Privacy Rule

By: Dorothy M. Cociu, RHU, REBC
President, Advanced Benefit Consulting & Insurance Services, Inc.

Last spring, I discussed in a related article the basic components of HIPAA's Medical Records Privacy, and attempted to simplify a very difficult topic. This article is intended to pick up where the last (related) article left off. Now that many health plans and employers sponsoring health plans have entered the world of privacy, where do we go from here? My purpose here is to supplement what the text books and lawyers are telling you (most of which may be a jumbled set of definitions and concepts) with some real world solutions and alternatives while making those critical initial decisions on how you will be implementing HIPAA privacy in your organization, if you sponsor a health plan.

Hopefully, by now, most carriers, providers and group health plan sponsors have learned about privacy, have implemented training for all in contact with protected health information (PHI) and have appointed a privacy officer responsible for implementation of the privacy rules. For those who have not yet begun, such as plans and plan sponsors which meet the small plan definition, and have until April 14, 2004 for implementation, you may still be wondering how all this will affect you. There is a lot to consider, so you'd be best served to start moving forward quickly.

The privacy rule covers many topics, from transferring data electronically to adopting medical code sets, from developing standards for unique identifiers to creating safeguards to protect confidential information, to protecting individually identifiable health information. Some of the requirements apply mostly to carriers and as well as third party administrators, who are involved with the actual processing of claims and claim payment issues, particularly the areas related to electronic data interchange. However, many other of the rule's requirements apply to all covered entities.

By way of review, keep in mind that the Privacy Rule requires plans and providers to comply with the privacy requirements by April 14, 2003, or April 14, 2004 for those who qualify under the small plan ($5 million or less in receipts) definition. The Privacy Rule for the first time creates national standards for protecting health information, by giving patients more control over their health information, setting boundaries for the use and release of health records, establishing safeguards that providers and others must achieve to protect the privacy of health information, and holding violators accountable with both criminal and civil penalties[1].

[1] HIPAA Privacy Guidance, December 3, 2002, Office of Civil Rights

In general, the Privacy Rule requires the average plan or provider to notify patients about their privacy rights and how their information may be used, adopt and implement privacy procedures, train employees so that they understand the privacy rule's implications, designate an individual to be responsible for privacy implementation (a privacy officer), and to secure all records containing individually identifiable health information[2].

For more information on these basic privacy concepts, please refer to my first article on the topic, "Entering the World of Privacy", or seek one of many websites or government offices for additional information.

There are many areas of confusion in the Privacy Regulations which may take years to unravel. Let's face it, this is a new law, and like COBRA when it was introduced, it seems scary and unworkable. But also like COBRA, not all questions were answered in the first one, two, or even three go-rounds. How many sets of regulations, how many court rulings, and how many lawyers were involved in COBRA implementation, to get it to where it is today? I suggest you keep that in mind when trying to understand Privacy. Here's another bitter truth about the implementation of Privacy. *No one wants to be the first case sitting in front of the first judge making the first ruling on privacy.* Therefore, at least for the foreseeable future, probably two to four years out, most implementing privacy procedures are doing so with a very conservative approach. We also subscribe to that concept and practice in our privacy training, implementations and consulting approaches.

So what areas are the major concerns, and where is the conservative approach coming from? To name a few: authorizations, and when you use them, understanding the training component and how it applies to internal staffing, how your supervisors and managers may be your greatest asset, as an employer plan sponsor, or your worst liability, depending on the training, the policies and procedures you implement, what role your own employees will play in enforcement, and even the basic understanding of PHI, and how broad the concept can be.

Let's start with the basics; PHI, and learning what it may mean to the employer plan sponsor. Looking back at the concepts and definitions discussed in last spring's article on privacy ("Entering the World of Privacy"), the definition of PHI itself is a potential problem. Protected Health Information is information that is held or disclosed by a covered entity, which attaches personal health information back to an individual. In other words, discussions about Jane Doe's appendectomy are PHI; they attach the health condition, or in this case the surgical procedure of an appendectomy, back to Jane Doe, an individual who is known to the plan sponsor. It hasn't been de-identified or summarized. It is, by definition, PHI. So in the basic employment situation, when an employer sponsors a group health plan, the employer as clarified in many cases is a covered entity. However, as discussed in the last article, the employer itself does not have to comply with the privacy rules (*but before you say "okay, so what am I doing learning this stuff" and figuring you can head for the door right about now, please read on…*), but the *plan sponsor personnel dealing with PHI* must create firewalls to protect

[2] HIPAA Privacy Guidance, December 3, 2002, Office of Civil Rights

PHI and must meet the privacy rule requirements. The problem here is that health plans don't have employees to do the work and administer the plan on behalf of its employees. Health plans don't have employees….Employers sponsoring health plans have employees, and therefore the employer is indirectly pulled into the role of protecting PHI and compliance with the privacy rule.

Now let's look back at the definition of PHI. Information contained orally (such as a discussion related to someone's health condition, even an employee walking into the HR department and asking for assistance on a claim), in written form (such as application received, or any other written documents which contain someone's PHI) or electronic form, all constitute PHI. Remember, PHI is any information held by a covered entity which contains any health information related to that person. If his name is attached, or any one of the 19 identifiers listed in the regulations, it is, by definition, PHI. So what are some examples of what the average employer contains in their files which may include some form of PHI? Health applications with medical questions, absolutely. Sick leave notes, return to work data, pre-employment physicals (assuming they were later hired, at which point this becomes potentially PHI), medical claims disputes, EOB's, would all be considered PHI. But what else in your personnel files contain anything which may meet the definition of PHI? How about a voluntary life application with three simple medical questions? How about an FMLA leave application? What about a disability claim, or a work comp claim? Are those PHI? According to the definition, it certainly sounds like it. If someone comes in to talk about FMLA, disability or work comp, just as when they walk in to discuss a medical claim, wouldn't they be disclosing health information to the human resources representative, or the privacy work group member? But what about excluded plans? Aren't life, disability, and workers compensation excluded? Yes, the plans are definitely excluded. But as discussed in the first article, what about the information held or disclosed by the covered entity related to those situations (which I call cross-overs, for lack of a better term)? Don't you then have your hands on PHI – health information which is held or disclosed, and which ties that health information back to an individual? Now you are beginning to see the first of many questions on privacy….. *What do we do about the cross-over situations?* That question may take years to answer. Do you use the covered and non-covered plans definition or the definition of PHI itself?

Although there are some lawyers who have said that you shouldn't be concerned about the excluded plans, as they are excluded, there are as many or more lawyers (at least what I've seen, heard, read, and discussed) who say *'hey, I don't want to be the first lawyer representing the first firm involved in the first case sitting in front of the first judge making the first decision on privacy, which results in a bad decision!'* In other words, the conservative approach by many law firms (our law firm included, which is an independent law firm specializing in employee benefits law) is that until that first decision is made, which is likely two to four years out, or until the regulators provide us with additional clarifications, we need to be conservative. The definition *does not say* that PHI is information *for covered plans* which attaches a health condition back to an individual. The definition is very broad. It says PHI is any information held or disclosed by a covered entity that has individually identifiable information related to a person's

past, present or future health condition. So, if you have possession of someone's FMLA file, or a disability or work comp issue, are you not in possession of their PHI in some format? When they come into your office to discuss these things, are they not discussing health information with you? *Do you want to be that first case sitting in front of that first judge making that decision?* My experience with federal court judges (I have run third party administrators and have acted as an expert witness on federal court cases on more than one occasion) tells me that they base decisions on case law (which there is none yet) or the regulation or law text. The text includes these definitions. If the judge makes a ruling, will it be based on the definitions, perhaps, assuming that the definitions may focus on the intent of the law? From a practical standpoint, this sounds logical to me…

I am not an attorney, so I am obviously not providing legal advice. As always, I highly recommend you consult your employee benefits law firm (preferably one who knows COBRA and ERISA and HIPAA issues, and has experience in federal courts) before implementing any privacy policies and procedures. I am, however, sharing my observations, as well as practical real-world situations.

Our conservative approach to Privacy is that until the courts, or the regulators, come up with tighter definitions or additional clarifications, including the cross-over situations, we'd better act accordingly, and conservatively.

Now, let's look at policies and procedures which are intended to represent your decisions on how to protect PHI held in your office. We generally recommend a separation of files in each plan sponsor's office; your "red files" should include any information which contains PHI. This may include your health applications, your sick leave information, your FMLA files, your work comp claim files, pre-employment physicals, disability files, or any files which may contain any type of PHI. Your "white files" include all other employment data. Keep in mind, anyone handling "red files" needs proper training on privacy; they are behind your firewall. Supervisors and managers, and others, however, may not need access to the "red files." They may only need access to the white files. Remember, the privacy rule specifies that only "minimum necessary" information is to be shared. Does a supervisor or manager really need to know why someone is out on an FMLA leave or a disability leave, or out sick? Or do they simply need to know that they will be out, and that they need to cover the shift(s)? Likely, under the minimum necessary definition, they would only need the latter. Therefore, your separation of files is suggested. Only properly trained personnel who are required to have access to PHI for their job functions need access to the "red files."

What other policies and procedures may need to be reviewed in order to comply with the privacy rules? If only "minimum necessary" information is allowed by law, will your sick leave policies need to change? Perhaps. Perhaps not. I suggest you think about this…. Who takes sick leave calls? The human resources department, or supervisors and managers, or both? How about a receptionist on occasion? Perhaps HR opens at 8 am, but the early shift of drivers or warehousemen opens at 5 am, or perhaps you run 3 shits. If someone is calling in sick, can they call HR, which is perhaps where the majority of the privacy team is located? Are they required to call their supervisor? If so, what type

of information is collected by the supervisor or manager when they take a sick leave call? Do they ask why they are sick, what's wrong with them, and ask for details? Most likely, they do. Or at least they have in the past. In part because they care, in part because they may be frustrated about someone not being in today and wanting to know all there is to know. But is that "minimum necessary"? I think not. We've found alternative means for sick leave calls work well, such as specific voicemail call-in phone numbers, which take the necessary information, and transmit it via text messaging perhaps to a cell phone or pager of a supervisor – allowing them to know what they need to know; this person is out sick, and we need to cover the shift. In addition, training of supervisors and managers is vitally important. The privacy rule does not have specific training requirements for supervisors and managers, nor do they have specific training requirements for privacy officers (they only specify training is required specific to job functions), but we applied logic to this and concluded that these are individuals who would definitely need training. Do you want them behind the firewall where they may have access to such information? Probably not. Usually there are far too many supervisors and managers, and you can't control things with too many people behind your firewall. A better decision may be "don't ask, don't tell" sick policies, returning doctors' notes to the privacy officer only, and not to the supervisor, and a number of other real-world alternatives.

Each employer/plan sponsor has to determine what types of policies and procedures regarding sick leave to implement, who takes the calls, how can we limit the amount and type of PHI received and how can we protect it best….and so much more.

What types of firewalls are needed? Only the plan sponsor can determine that. You need physical, technical and administrative safeguards, which are normally explained fully in training. Physical safeguards are fairly easy – locks on file cabinets, restricted access to keys, physically relocating work areas or computers which can be viewed by non-trained, non-authorized personnel, to name a few. But more are needed.

What have you witnessed in the real world to date on firewalls? The provider side varies, but examples of some of the changes, or firewalls created to protect PHI, may assist you in thinking about your firewalls. Some provider firewalls include the physical relocation of some hospital waiting rooms and/or nurses stations, so that patients cannot overhear health discussions of patients (as previously many waiting areas were located next to nurses stations), doctor's offices have had sign-in sheets, then immediately covered your name after your attendance is recorded with white tape, so that the other patients in the reception area do not know who you are, and others assign patients a number. In some hospital maternity wards, babies have been identified by number only, and in some cases, flower deliveries are allowed only if you know the room number in advance. Some pharmacies have displayed footprints telling you to stand here, along with a stop sign that says "Wait here to protect patient privacy." Their firewall is an invisible one; if you stand behind this line, you're not supposed to overhear the discussion taking place between the pharmacist and the patient having a prescription filled. The reality is, you may be able to overhear the conversation, as I did, but their policy and procedure is in

place, and they have created their firewall. Each plan, provider or plan sponsor must determine its own firewalls.

As an employer/plan sponsor, your firewalls will likely be different than providers. The privacy rule provides the right to have confidential communications, so how does this apply to your office? If nine people are located in an open HR office, and only three have access to the "red files," what happens when someone walks in and wants to talk about a health issue? Can an individual assume his communication will be confidential? We suggest a designated area for confidential communications. It may be a private office, or it may a small conference room, but we'd suggest that the invisible firewall concept here may lead to serious problems later on, if and when someone files a complaint stating their privacy rights were violated. This suggestion carries forward for workers' compensation issues as well. Although the work comp plan is excluded, we suggest a similar cross-over concept, and suggest business as usual for work comp, with one exception; take the interviews of witnesses and the conversations regarding the work comp claim to a designated, confidential communications area. Again, perhaps conservative, but at this point, we are concerned about the potential for complaints and their impact. Again, some trainers, consultants or attorneys will disagree with our approach.

How will the privacy rule be enforced? HHS/OCR stated in its April 11, 2003 guidance that a formal complaint process is available for persons feeling their privacy rights have been violated. A complaint could be filed for any number of privacy violations, including not receiving privacy notices, not having confidential communications, not enforcing your policies and procedures related to privacy, and so much more! So what will trigger audits and investigations? Your own plan participants, your employees, may be the ones filing complaints against you, which could result in audits and investigations, which could result in penalties….

Privacy violations have severe penalties. On the civil side, which is enforced by HHS, penalties can be assessed at $100 per violation, with a $25,000 maximum per year[3]. The maximum, however, applies to each separate provision violation, so the actual cost could be substantially higher. There are exceptions for reasonable cause, and we feel that supervisor and manager training could play an important role here. On the criminal side, with enforcement under the Department of Justice (i.e., our legal system), penalties and jail time for plan fiduciaries could apply. Penalties for knowingly or wrongfully disclosing or receiving protected information could result in fines of up to $50,000, plus up to one year in prison, or both. For releasing information under false pretences, you're looking at up to $100,000 in fines and five years in prison or both, and for intent to sell protected information, or other criminal activities, fines can apply up to $250,000, with up to ten years in prison, or both[4]. So, to quote one of our lawyers, if you thought you'd simply wait until the 'HIPAA Posse' shows up on your doorstep before you worry about Privacy, you may want to think again! This privacy thing can truly be expensive if not

[3] SSA Section 1176
[4] SSA Section 1177

implemented properly! I can't say this enough: training is so important; for your privacy team, your supervisors and managers, and your employees in general.

Training is required by the privacy regulations[5]. The regulations do not require a specific seminar or a specific training, but the regulations do state that all plans must appoint a privacy officer, receive training and implement policies and procedures to accommodate the privacy rule's requirements. In general, all personnel coming in contact with any type of PHI need training specific to his or her job functions. Anyone behind your firewall needs fairly extensive training (we feel 4-6 hours is appropriate). Supervisors and managers need training, as they are your enforcers of your policies and procedures, and they need to know what they can and can no longer do. Employees need training so that they know about the privacy laws and how things will change in their workplace.

Can you not tell your employees that they have the right to file a complaint against you? No, you can't just simply *not* tell them. Employees covered under health plans have rights, and one of their rights is to receive a privacy notice, and the right to file a complaint needs to be stated in that notice. In addition, they have rights related to confidential communications, the right to access, inspect and obtain a copy of their PHI, the right to amend their PHI if something is stated inaccurately, the right to receive an accounting of their PHI, and to request restrictions on uses or disclosures of their PHI[6]. As far as complaints are concerned, they have the right to file a complaint with the covered entity, and to file a complaint directly with the Department of Health and Human Services or the Office of Civil Rights (HHS/OCR). A privacy complaint form is prominently displayed on the HHS/OCR website.

My concern for plan sponsors is that the employee who is later disgruntled, due to employment issues non-related to privacy, for example, not receiving the promotion they wanted, or being disciplined, or being fired, may decide that they now want to file a privacy complaint. The plan sponsor needs to have their complaint process in place, and administrative procedures to handle all the privacy requirements.

As I stated above, your supervisors and managers, we feel, can be your greatest asset, or your worst liability, depending on how you train them, and the policies and procedures you implement. The privacy rule requires that plan sponsors develop and apply a system of sanctions for those who violate the privacy rules; however, you cannot require individuals to waive their rights to file a complaint with HHS/OCR, or waive any other rights related to the Privacy Rule, and you must refrain from intimidation or retaliatory acts[7]. In other words, you cannot fire someone for filing a complaint against you!

Another area of confusion is authorizations. Keep in mind that the HIPAA privacy rule does not require an authorization for treatment, payment, or health care operations. That

---

[5] 45 CFR Section 164.530(a)(1)(i)

[6] Standards for Privacy of Individually Identifiable Health Information, 45 CFR Section 164.524, 164.526, 164.528

[7] Standards for Privacy of Individually Identifiable Health Information, 45 CFR Section 164.530(2)(g), 45 CFR Section 164.530(2)(g)(2)(h)

means that for seeing a physician, for claims related activities, and all related health care operations, you do not need an authorization. This, at least, applies to covered plans. So how come my carrier is requiring an authorization before they can assist me? Because one of many things may apply. You may be in a state which requires authorizations for certain types of plans or issues (like California). Or perhaps it is that carrier's policy and procedure decision. Or perhaps that carrier does business in many states, some of which have authorization requirements, and they chose to implement HIPAA privacy policies and procedures across the board, and train their employees at one level due to cost-effectiveness. What about the cross-over situations? Again, an unanswered question. So, for the time being, we suggest (again, taking the conservative approach) you have an authorization completed for any cross-over discussions, such as workers' compensation, disability, or FMLA. It certainly can't hurt, and if it's a policy and procedure, and your employees are aware of it, it shouldn't be a problem with your employee population, assuming they are trained and know you are requiring an authorization under these circumstances. What this would do is limit liability. The discussion then takes place in a confidential communications area, and you have written authorization to discuss those issues with that individual. No questions…. In a workers' compensation situation, I'd suggest you consider listing the supervisor or manager on the authorization as someone authorized to receive and use that information, for basic work comp reasons. Again, until all questions are answered, you have a good policy and procedure in place to protect PHI and individual rights.

When does the privacy rule *not* apply? For public policy exceptions, including when required by law; for public health or threats to public health or safety; when the incidence is related to victims involved in domestic violence, abuse or neglect; for judicial and administrative proceedings related to court activities; for law enforcement; for decedents (coroners, medical examiners, funeral directors); for government functions, such as military, veterans, national security, protective services, state department, or correctional institutions; and for workers' compensation[8]. Under these circumstances, you can throw the privacy rule out the window. If you receive a court order, abide by the order, and if there is a police or fire activity, do what the police or fire department tell you to do.

As some final words of caution, remember, state rules apply, so check with your own state's department of insurance or privacy office to determine what, if any, additional requirements you are obligated to comply with in your own state. Also, again, seek the advice of a qualified legal expert before implementing any privacy policies, as situations vary greatly. ##

Author's Note and Disclaimer: *The information herein should not be construed as legal or tax advice in any way. Regulations, guidance and legal opinions continue to change with this any new law. Dorothy Cociu of Advanced Benefit Consulting & Insurance Services, Inc. and her law firms have gathered public information and have attempted to present it in an easily readable and understandable format. Situations vary. Technical corrections and future opinions may vary from what is presented in this article. This is meant for informational content only. Neither the author, this publication, Advanced*

[8] Standards for Privacy of Individually Identifiable Health Information, 45 CFR Section 164.512

Benefit Consulting, or its company affiliations or sources referred to make any warranty of any kind concerning this information. You should seek the advice of your attorney or tax advisor for additional or specific information.

About the Author: *Dorothy M. Cociu, RHU, REBC, is the President of Advanced Benefit Consulting & Insurance Services, Inc. She is a qualified HIPAA expert and a nationwide speaker and author, as well as a HIPAA privacy trainer. She is the author of The ABC's of HIPAA Compliance; An Employer's Simplified Guide to HIPAA Compliance, and has nearly 19 years experience in the sales and administration of employee benefit programs. For information on HIPAA privacy training, privacy materials and other information, please visit her firm's website at www.advancedbenefitconsulting.com, or call (866) 658-3835, or (888) 288-0164. For a copy of the previous article mentioned, you can find it on the above-referenced website. Privacy training is available nationwide through public seminars or private seminars, and a variety of training tools are available for purchase. See the ad in this issue for more information.*

Reference Sources: Standards for Privacy of Individually Identifiable Health Information, Regulation Text, 45 CFR Parts 160 and 164; HHS Guidance December 3, 2002, HHS Guidance, April 11, 2003, Public Law 104-191, August 21, 1995, HHS/OCR Website Data, 2002-2003, HHS HIPAA Privacy Final Regulation Text, August 14, 2002.