AMERICAN BAR ASSOCIATION

Technical Session Between the Department of Health and Human Services
and the Joint Committee on Employee Benefits

May 3, 2004

The following notes are based upon the personal comments of the various individuals from the Department of Health and Human Services, Office of the Secretary, the Office for Civil Rights and the Office of General Counsel who attended a meeting with the representatives of the various sections comprising the Joint Committee on Employee Benefits from the American Bar Association on Monday May 3, 2004. The comments were made by these individuals in their individual capacity and not as representatives of the Department of Health and Human Services and the Office for Civil Rights. These do not represent the position of the Department of Health and Human Services and the Office for Civil Rights or of any other government agency of office. None of the comments should be considered official guidance or the position of any agency.

This document has been prepared by private sector members of the American Bar Association’s Joint Committee on Employee Benefits who were present at the meeting and reflects their description of the answers to the questions that were discussed at the meeting. This document has not been reviewed or cleared by the government individuals involved in the meeting.
**Question 1:** Can you please provide a brief summary of any audit or enforcement activities that HHS/OCR has undertaken since April 14, 2003, with respect to the HIPAA Privacy Rule – particularly any such activities with respect to health plans?

**Answer:** HHS/OCR has focused on responding to the complaints that it receives regarding violations of the HIPAA Privacy Rule. The ten regional HHS offices receive the complaints and manage the complaints that are received. HHS has responded to approximately 6,000 complaints since April 2003, and continues to receive about 100 complaints per week. The complaints that HHS receives cover health plans and health care providers. A fair number of the complaints involve situations over which HHS has no enforcement role, such as complaints regarding entities over which HHS has no jurisdiction (*i.e.*, employers), that involve incidents that arose prior to the effective date of the HIPAA Privacy Rule, or that were not timely filed after the alleged violation of the Privacy Rule (*i.e.*, not filed within 180 days of the alleged violation). HHS has focused its enforcement efforts on resolving the complaints and has not undertaken independent compliance reviews.

HHS has an information management system that it uses to track the complaints that it receives. The top five entities against which complaints are made are private medical practitioners, general hospitals, pharmacies, outpatient facilities, and group health plans. There are a number of complaints about employers, but some of that concerns data that is actually employment information. HHS noted that the information regarding complaints might not always be accurate (*e.g.*, claims against plan sponsors may be incorrectly recorded as claims against group health plans, rather than as claims against an entity that is not covered under the HIPAA Privacy Rule).

HHS identified the five primary complaints that have been raised as follows:

- Impermissible uses and disclosures.
- Inadequate safeguards.
- Minimum necessary – more information is disclosed than is minimally required.
- Failure to give individual access to records.
- Failure to provide notice of privacy rights.

HHS has not yet imposed any civil money penalties with respect to violations of the HIPAA Privacy Rule. HHS has closed about one-half of the complaints that have been raised. One-third to 40% of those cases have been closed as being without merit.

HHS frequently hears about situations in which communication is not being made purportedly because of the HIPAA Privacy Rule – such as communications from health care providers to parents of minor children. HHS does talk to hospitals, etc., who are overreacting to the HIPAA Privacy Rule, to tell them that certain things ARE permitted by the rule.
Question 2: A health plan document and SPD provide that coverage may be terminated and warn that other disciplinary action, including termination of employment, may be taken if an employee or dependent file false claims or submits other fraudulent or misleading information under the plan. Under HIPAA’s privacy rule:

(a) May a business associate or plan sponsor (acting in a plan administrative capacity) audit claims to detect fraud?

(b) If fraud is discovered, may the business associate use or disclose that information to terminate the coverage of the employee and/or dependent?

(c) May that information then be used or disclosed to discharge the employee?

Proposed Answers: Exactly how this situation unfolds depends on the circumstances. At a minimum, the plan sponsor or business associate should be allowed to conduct the audit, use or disclose the information discovered to terminate coverage, and use or disclose certain information to advise a plan sponsor that enrollment has been terminated for fraud and of the magnitude of the problem, even though an employer may (and to a large extent to permit an employer to) terminate an employee’s employment or take other employment-related actions. More specific information should not be disclosed without individual’s authorization.

(a) Plan sponsors and business associates may audit claims under a plan generally and may specifically audit for fraudulent claims. These audits would be considered part of the plan’s health care operations. See 45 CFR 164.501 and 164.502(a) (1)(ii). The audit may be conducted by either a business associate pursuant to the terms of the relevant business associate agreement, 45 CFR 164.504(e), or by a plan sponsor pursuant to an appropriate plan amendment, 45 CFR 164.504(f)(2)(C). See also 45 CFR 164.502(e). An audit of an individual’s claims could be conducted pursuant to the written authorization of that individual, 45 CFR 164.508, but in these circumstances it would typically be impractical to obtain individual authorization.

(b) Both business associates and plan sponsors who discover evidence of false claims in the course of an administrative claims audit should be permitted to use that information for purposes of terminating the individual’s coverage under the plan. The termination of an employee for filing false claims constitutes an administrative action taken pursuant to the plan’s terms. Even if protected health information is deemed to be used in terminating the individual’s coverage, that use (or disclosure for that use) would be warranted as meeting the definition of either “payment” or “health care operations.” 45 CFR 164.501. Of course, the authority given to the business associate in the business associate agreement or plan sponsor in the plan document should be broad enough to allow them to use or disclose protected health information for this purpose.

In certain circumstances, the use and disclosure of protected health information may be limited. False claims may have little or nothing to do with an individual’s actual medical condition or health care. See 45 CFR 160.103 (“protected health information” and “individually identifiable health information”). For example, when an individual fraudulently loans out his or her HMO identification card or falsely obtains prescription drugs for resale, there may be little in the record that would constitute protected health information for that individual. The medical information at issue may be for another person or completely fabricated. The business associate or plan
sponsor (acting as plan administrator) should take reasonable measures to filter actual protected health information out of what it uses or discloses for these purposes to safeguard legitimate privacy interests.

(c) The potential use or disclosure of protected health information for purposes of employment actions raises greater concerns. While a plan sponsor may use and disclose protected health information for various plan administrative purposes, it may not use or disclose that information for employment-related actions. 45 CFR 164.504(f)(2)(ii)(C). Business associates would not ordinarily have a basis for disclosing protected health information to an employer for an employment action. The disclosure could not ordinarily be justified as treatment, payment or health care operations for the plan.

However, the fact that the plan itself has terminated the coverage of an individual cannot be kept from the plan sponsor or employer. Plan sponsors and ultimately employers need to be informed that the plan has disenrolled an individual for various purposes (such as premium payments and payroll deductions or reductions). Plans are expressly permitted to “disclose to the plan sponsor information on whether the individual is participating in the group health plan...” 45 CFR 164.504(f)(1)(iii). The question is how much information may accompany notice of this administrative disenrollment.

If the plan sponsor receives only the barest information, an employer may be placed in the position of making a decision about terminating an employee based solely on the knowledge that the plan administrator has terminated the individual’s coverage for reasons under the plan. It would be more sensible for an employer to have more information before making a decision as to whether to terminate the employee’s employment. The fact that coverage was terminated for filing false claims and the amount that the plan paid as a result of this fraudulent activity do not reveal anything about the individuals health condition or care or the benefits paid for actual health care. It would allow an employer to consider, for example, whether coverage were terminated because false claims were filed over a period of several years at a substantial cost to the plan. The provision of sufficient information for an employer to assess the extent of a problem that resulted in a termination of coverage would also be appropriate in light of concerns expressed in HIPAA (in provisions that extend beyond the administrative simplification provisions) about fraud in the health care industry. Further information could be obtained to the extent the individual authorizes the employer to have access to the information.

**Answer:** HHS did not respond to this question, other than to state that it has provoked considerable discussion.
**Question 3:** Employer E outsources its health plan enrollment functions (and a range of other functions) to Vendor V. E provides V with a payroll data feed that includes considerable identifying information about its employees, but not their health plan enrollment elections. Employees enroll for health coverage directly through V. All of this data is collected and maintained in accordance with V’s own content and format requirements, which are not consistent in all respects with the standards for enrollment transactions set forth in 45 CFR 162.1502. HMO H provides one of the coverage options under the health plan. H has informed V that it will begin to accept the transmission of enrollment information electronically as a standard transaction. If V accommodates this request, will it be regarded as a health care clearinghouse?

**Proposed Answer:** No. To be a health care clearinghouse in these circumstances, V would need to receive health information in a nonstandard format or containing nonstandard data elements from another entity and process or facilitate its processing into standard data elements or a standard transaction. 45 CFR 160.103. The only health information that V receives is the health plan enrollment information. This information is furnished directly by individuals, not an entity.

While E is an entity, the information that E provides includes employee data. E provides some of this information to H as part of the standard transaction, but E is not providing the actual enrollment election (which is the health information) that V would process.

**Answer:** HHS did not answer this question, other than to note that it is an issue that is under discussion. HHS did state that this issue is more frequently discussed by CMS, and that HHS is not ready to discuss issues as to what is a health care clearinghouse. HHS indicated they would be willing to coordinate with CMS if the designation of an entity in this type of situation is a significant issue. HHS also noted that there is a FAQ (Frequently Asked Question) on the CMS website that deals with clearinghouses and billing services, although it does not specifically answer this question. The FAQ that HHS referred to is titled “When would a billing service be considered a health care clearinghouse?” on the CMS website, at [http://questions.cms.hhs.gov](http://questions.cms.hhs.gov).
**Question 4:** Under the HIPAA Privacy Rule, is it permissible for a plan sponsor of a group health plan to obtain and disclose protected health information for purposes of (1) obtaining bids for insurance under insured plans, (2) obtaining bids for stop loss coverage under self-insured plans, (3) making claims for coverage under existing stop loss policies (either on an individual claim or aggregate basis)? I am specifically interested in the sharing of PHI and not Summary Health Information (SHI). In addition, the response should take into account that the plan sponsor and not the plan is the owner and beneficiary of the stop loss insurance policy.

Assuming the answer to all of these questions is yes, will CMS be issuing any guidance to provide covered entities that are group health plans and their sponsors comfort in this regard, either in the form of an FAQ or additional regulatory guidance?

**Answer:** HHS stated that this question may boil down to whether stop-loss insurance is treated the same as reinsurance. HHS has issued an opinion saying they are treated the same. (See 9/17/2003 letter to George Pantos, Self-Insurance Institute of America, on next page.)
September 17, 2003

Mr. George J. Pantos, Esq.
Washington Counsel
Self-Insurance Institute of America, Inc.
1250 H Street, NW
Suite 901
Washington, D.C. 20005

Dear Mr. Pantos:

Thank you for your letter regarding the requirements of the health information privacy regulation (Privacy Rule) issued pursuant to the Health Insurance Portability and Accountability Act (HIPAA). We appreciate your request for clarification of the Privacy Rule’s applicability to stop-loss insurance carriers and managing general underwriters. We hope this letter will address some of the questions that you have raised, and apologize for the delay in our response.

Specifically, you asked whether stop-loss insurance carriers who indemnify self-insured health plans are considered business associates for purposes of the Privacy Rule. We have issued guidance stating that a reinsurer does not become the business associate of a health plan simply by selling a reinsurance policy to the health plan and paying claims under the policy. Similarly, we have stated in the preamble to the Privacy Rule that stop-loss and excess of loss insurance are functionally equivalent to reinsurance. 65 Fed. Reg. 82609 (2000). Therefore, just as a reinsurer does not become the business associate of a health plan simply by selling a policy or paying claims under the policy, a stop-loss insurance carrier would not become a business associate when providing stop-loss insurance.

In addition, we stated in the preamble to the Privacy Rule that “activities related to ceding, secur[ing], or placing a contract for reinsurance, including stop-loss insurance, are health care operations . . . .” 65 Fed. Reg. 82568 (2000). A group health plan may disclose information, as a health care operation, to a stop-loss insurance carrier in order to obtain stop-loss coverage. If the disclosure by the group health plan is to obtain payment under the contract for stop-loss insurance, it is a permitted disclosure for payment.

Finally, based on the information you provided, we are unable at this time to articulate every scenario whereby managing general underwriters may be required to comply with the business associate provisions of the Privacy Rule. Generally, if they are providing services on behalf of the group health plan, such as actuarial services, they may be considered business associates of the group health plan. However, if they are providing services on behalf of the stop-loss
insurance carrier, such as underwriting and pricing stop-loss coverage, then they may not be considered the business associate of the group health plan.

We thank you for seeking clarification of these issues, and hope that this information is helpful. We will continue to publish guidance and offer technical assistance to covered entities in order to assure that the Privacy Rule is implemented in an effective and efficient manner.

Sincerely,

Susan McAndrew
Senior Health Information Privacy Policy Specialist
**Question 5:** Is a voluntary injury benefit plan that provides benefits for workplace injuries and illnesses and is maintained by a Texas employer that does not subscribe to the state workers’ compensation system a “health plan” under the HIPAA Privacy Rule?

**Proposed Answer:**

**Background:** The workers’ compensation system in Texas is purely voluntary. (See, Texas Labor Code § 406.002.) Employers in Texas may elect whether to provide state regulated worker’s compensation benefits, i.e., “subscribe” to the state program. Employers who subscribe to the state regulated workers’ compensation program may either pay into the state system on an insured basis or may self-insure the state provided benefits. (See Texas Labor Code § 406.003.) Alternately, an employer may elect to be a non-subscriber. Under Texas law, a non-subscriber is not required to provide workers’ compensation benefits for its employees and may be sued for any workplace injury or illness. However, to limit their liability most non-subscribers provide an occupational injury plan (referred to as a “Texas Injury Benefit Plan”) that provides medical and salary continuation benefits for Texas employees who experience a workplace injury or illness. Some Texas Injury Benefit Plans also provide death, dismemberment, income replacement and other forms of work-injury related benefits. These Texas Injury Benefit Plan benefits are generally structured to be similar to the state workers’ compensation system. Under Texas Injury Benefit Plans, all employees of the employer that work in Texas automatically participate in the plan. However, only those employees who actually experience a workplace injury or illness are eligible to receive plan benefits.

**Status Under ERISA:** ERISA § 4(b)(3) provides that ERISA shall not apply to any employee benefit plan if the plan “is maintained solely for the purpose of complying with applicable workmen’s compensation laws or unemployment compensation or disability insurance laws.” Because Texas Injury Benefit Plans are not maintained “solely to comply with” workers’ compensation laws, they are not eligible for this ERISA exception that covers substantially all other state workers’ compensation systems. As a result, Texas Injury Benefit Plans satisfy the definition of an “employee welfare benefit plan” under ERISA § 3(1) and are required to comply with the provisions of ERISA.

**Status under HIPAA Privacy Rule:** Section 160.103 of the HIPAA Privacy Rule provides that a “health plan” includes a “group health plan” or employee welfare benefit plan within the meaning of ERISA § 3(1) to the extent that the plan provides medical care. Because of this cross-reference with ERISA and the status of Texas Injury Benefit Plans as ERISA plans, a Texas Injury Benefit Plan is initially included as a “health plan” under the HIPAA Privacy Rule. However, the analysis does not end there because the definition of a “health plan” excludes any plan that provides or pays the cost of “excepted benefits” within the meaning of 42 USC 300gg-91(c)(1). This section provides in pertinent part that an “excepted benefit” includes benefits under “workers’ compensation or similar insurance.”

**Texas Injury Benefit Plans are Similar Insurance to Workers’ Compensation:** Texas Injury Benefit Plans provide insurance to Texas workers for workplace injuries and illnesses, thereby making these plans similar to the workers’ compensation system in Texas. The phrase “solely to comply with” under ERISA means that the exclusive reason to maintain the Plan must be to comply with the workers’ compensation system of Texas. Because a Texas Injury Benefit Plan
is voluntary on behalf of non-subscribing employers, these plans do not meet the “solely” or “exclusiveness” test and constitute ERISA plans. Alternatively, the phrase “similar to” in the exception for HIPAA Privacy Rule, does not require that the exclusive purpose of the Plan be to comply with workers’ compensation system. Rather, the phrase only requires that the Plan be “similar to” or have characteristics that are in common with workers’ compensation in order to be an excepted benefit under HIPAA.

Texas Injury Benefit Plans are similar to and have many characteristics in common with the Texas workers’ compensation system. For example, the Plans offer (1) salary continuation at a determined rate and (2) payment of medical expenses directly related to an on-the-job injury. Thus, while Texas Injury Benefit Plans constitute ERISA plans because they are not maintained solely to comply with the workers’ compensation system of Texas, they provide benefits that are similar to the workers’ compensation system of Texas. Therefore, they satisfy the definition of an “excepted benefit” within the meaning of 42 USC 300gg-91(c)(1)(D), and are not “health plans” under the HIPAA Privacy Rule.

This result is not atypical with certain other ERISA-covered benefits that are treated as “excepted benefits” under HIPAA Privacy Rule. For example, many accidental death and dismemberment (AD&D) benefits and disability benefits that are sponsored by an employer constitute welfare benefit plans under ERISA. Because these plans, in part, also provide for medical care they would be considered “health plans” under HIPAA Privacy Rule. However, because these types of benefits are considered “excepted benefits” under subparagraph (A) of 42 USC 300gg-91(c)(1), they are not required to comply with the HIPAA Privacy Rule. Similarly, as “excepted benefits,” Texas Injury Benefit Plans should also not be required to comply with the Privacy Rule.

**Answer:** HHS stated that they are not in a position to answer this question. In general, HHS would tend to look at these kinds of programs to see if the program is functionally equivalent to a workers’ compensation program so that HHS could determine whether the program was an excepted benefit that otherwise trumps the program’s health plan designation; in other words, if something is essentially workers’ compensation, HHS might be willing to treat it as such, even though the program does not really constitute workers’ compensation. Any such issues would have to be approached on a “facts and circumstances” basis.
**Question 6:** If a self-funded group health plan contracts with a business associate (e.g., a third-party administrator) to perform one or more plan administration functions, must the plan have policies and procedures to cover the functions performed by that business associate?

**Proposed Answer:**

Section 164.530(i) of the HIPAA Privacy Rule requires the covered entity, i.e., the group health plan, to implement policies and procedures that “are reasonably designed, taking into account the size of and the type of activities that relate to the protected health information undertaken by the covered entity, to ensure [Privacy Rule] compliance.” Pursuant to Section 164.530(j)(1), the policies and procedures must be maintained by the covered entity in written or electronic form.

The typical single-employer group health plan does not have employees and can only act through its business associates and sponsor. Further, it is common for much of the general operations and administration of a group health plan to be delegated to a third party administrator that is a business associate of the plan. Thus, some activities for which a plan is required to have policies and procedures are performed not by the “plan” itself, but by a business associate. For example, records held in designated record sets are typically maintained by a third party administrator. Neither the plan (which has no employees and can only “act” through its business associates and sponsor), nor the plan sponsor typically have custody of the records. In this situation, the plan complies with its obligation to have policies and procedures related to a specific function under HIPAA if the plan sponsor (acting in its capacity as plan administrator) (a) delegates the responsibility for the function to a third party administrator, and (b) documents the delegation of the function.

Therefore, using the above situation as an example, the plan sponsor (acting in its capacity as plan administrator) could delegate to the third party administrator that maintains the records the task of responding to and processing DRS access requests. If the third party administrator agrees that it will process such DRS access requests in a HIPAA-compliant manner, then the policies and procedures of the “plan” regarding such requests could consist of only the general statement that all such requests will be directed to the third party administrator. The process of responding to and processing such requests would then follow the third party administrator’s own policies and procedures.

**Answer:** If the plan hires a third-party administrator to do plan administration functions, the plan can contract out the obligations to comply with the HIPAA Privacy Rule’s policies and procedures to the third-party administrator. HHS suggested that if the third-party administrator does all the functions of the covered entity (in this case, the health plan), it would make sense for the covered entity to require the third-party administrator to comply with all the responsibilities of the covered entity under the HIPAA Privacy Rule, including the covered entity’s responsibilities to create policies and procedures. This could include having the third-party administrator designate the privacy officer.

Nonetheless, the covered entity (i.e., the plan) is still on the “hook” for compliance because HHS can only enforce the compliance obligation against the plan, and not the third-party administrator. So the plan needs to be certain that the third-party administrator does everything that it needs to do to comply with its contractual responsibilities under the HIPAA Privacy Rule.
**Question 7:** Plastic surgeons in the Los Angeles area frequently receive large payments in cash for certain procedures which they do not want made public. The celebrity clients frequently make payments of over $10,000 for these adjustment procedures. The IRS requires that cash payments of over $10,000 be reported on a Form 8300 which gives the identity of the payer, at least to the IRS.

**Proposed Answer:** This does not fit within the health oversight disclosures in 164.512(f) since the IRS is not commonly thought of as in the health oversight business and does not neatly fit in that permitted disclosure. The disclosure should be permitted under 164.512(f)(1) as a disclosure pursuant to process and as otherwise required by law.

**Answer:** If the IRS requires this disclosure by law or regulation, then the disclosure is required by law and, therefore, a permissible disclosure.
**Question 8**: May a representative of the plan sponsor who is assisting an individual participant with obtaining payment under a claim for benefits under a self-insured plan obtain protected health information from a third-party administrator that provides services to the group health plan without obtaining an authorization from the participant?

**Proposed Answer**: If the participant is present, either in-person or on the phone, when the PHI is to be disclosed to the representative of the plan sponsor, then consent to receive the information is implied and no authorization is necessary.

Section 164.510(b)(1)(i) provides that a covered entity may disclose PHI about an individual to a third person identified by the individual, provided that the PHI disclosed is relevant to the third person’s involvement with the individual’s care or payment related to the individual’s health care. The regulation states that if the individual is present for that use or disclosure, the covered entity may disclose the PHI if (i) the individual agrees, (ii) the covered entity provides the individual with the opportunity to object to the disclosure and the individual does not express and objection, or (iii) the covered entity reasonably infers from the circumstances, based on the exercise of professional judgment, that the individual does not object to the disclosure.

So, for example, if a human resources representative of the plan sponsor was on the phone with the participant, the HR representative could conference in a representative third-party administrator to discuss an issue related to care or payment for care without the individual completing an authorization. In this situation, the third-party administrator could reasonably infer that the covered individual does not object to the disclosure in the presence of the HR representative.

Even if the participant does not complete an authorization, under the Privacy Rule, employees who perform plan administrative functions can assist a participant with a claim for benefits without an authorization so long as: (i) the plan document has been amended in accordance with the requirements section 164.504(f)(2); (ii) the employees who are providing help to the participant have been identified by the employer/plan sponsor as persons who receive protected health information to perform group health plan administrative functions; and (iii) the employees are using and disclosing the participant’s protected health information to determine proper reimbursement for health care, for quality control, or for other payment or health care operations purposes. For example, if the plan documents have been duly amended, a human resources employee who has been designated as having health plan responsibilities can call the group health plan’s third-party administrator (TPA) to inquire about why the participant’s claim was not paid because this is a permitted payment function. Requiring a participant to provide a HIPAA authorization to permit the employer/plan sponsor to comply with its plan administrator obligations would be inconsistent with the spirit of the Privacy Rule.

If the participant is not present, an employee who has *not* been identified as a person with plan administrative functions *cannot* obtain a participant’s protected health information without an authorization unless some other exception under the Privacy Rule applies.

**Answer**: HHS does not agree with the text of the proposed answer. Rather, HHS suggested that 45 C.F.R. § 164.510(b) addresses this situation.
HHS noted that there needs to be a way for individual to indicate that the representative of the employer is involved in the individual’s care. The Privacy Rule does not require any specific verification regime if an individual is present or on the phone assuming, in the exercise of reasonable professional judgment, that the person on the phone is the person who they claim to be and that the person wants the employer involved in his/her care.

Someone who has plan administrative duties for a self-insured plan may receive this type of information because this is a function of payment and health care operations. Therefore, a person with plan administrative duties may receive this information without an authorization or the individual’s identification of wanting the employer “to be involved in the individual’s care.”

If the plan is a fully-insured plan, HHS suggested that the employer should get an authorization, so that the employer does not end up in possession of PHI and having to comply with the panolopy of all the requirements of the HIPAA Privacy Rule.
**Question 9:** Do the regulations allow a family member to execute a HIPAA authorization on behalf of the covered individual where the covered individual is incapacitated or unable to understand the authorization?

**Proposed Answer:** Although not expressly addressed by the regulations, a family member can execute an authorization on behalf of an incapacitated employee.

The HIPAA regulations permit, at 45 CFR 164.510(b)(1), disclosure to a family member, other relative, a close personal friend of the individual, or any other person identified by the individual, of PHI directly relevant to such person's involvement with the individual's care or payment related to the individual's health care. There is, however, no provision in the regulations that allows someone else to execute an authorization on behalf of the covered individual where the covered individual is incapacitated.

The preamble to the regulations states that the rule allowing disclosure to those with the closest relationships with the individual is to be construed narrowly. The preamble states that the Plan does not have to verify the identity of the relatives or other individual. As an example, the preamble states that the fact that a friend arrives at a pharmacy and asks to pick up a specific prescription for another person effectively verifies that the friend is involved in the individual’s care, and allows the pharmacist to give the prescription to the friend.

Given that a family member can act on behalf of an individual with respect to a covered individual’s health care, a family member should be able to execute an authorization if the covered individual is incapacitated or unable to understand the authorization.

**Answer:** The Privacy Rule’s provisions on personal representatives are intended to allow an individual to execute an authorization on behalf of an individual who is incapable of executing an authorization. There must be a personal representative relationship between the individual and the representative; a friend or family member cannot sign authorizations.

If there is not a specific HIPAA personal representative, the matter becomes one of the intention of the individual, which may be gleaned from other powers of attorney that the individual may have completed. The PHI that is disclosed may be limited. For example, a financial power of attorney only allows access to financial information and, by extension, the only authorization that can be signed is one having to do with financial matters (e.g., billing information). A medical power of attorney, on the other hand, would allow the family member to sign an authorization for any purpose if the individual could not do sign by himself.

The Frequently Asked Question that is posted on the website may be worded more broadly than is appropriate. HHS is going to reconsider the wording of the Frequently Asked Question.

The treatment of children in the custody of one parent presents a lot of issues that are hard to address in formal guidance. State laws come into play as well as court orders. HHS did not specifically answer the question concerning the treatment of children.
**Question 10:** Do fully insured plans that only disclose to the plan sponsor summary health information for the purpose of obtaining premium bids from health plans or modifying, amending or terminating the group health plan, or enrollment information need to amend their plan documents in accordance with 45 CFR 164.504(f)?

**Analysis:** By its terms, 45 CFR § 164.504(f)(1), which is the section that governs plan amendments, indicates that a plan amendment is not necessary in this situation.

But 45 CFR § 164.530(k) states that a fully insured plan is subject to the documentation requirements set out in section 164.530(j) “only with respect to plan documents amended in accordance with sec. 164.504(f).” This requirement seems to indicate that fully insured plans should include HIPAA plan amendments as required by 45 CFR § 164.504(f).

**Answer:** A fully-insured plan that is only getting enrollment/disenrollment or Summary Health Information (SHI) does not need a plan amendment.