Included in this newsletter is guidance on various HIPAA-related topics that impact your everyday work life. Hopefully, it will help answer some of your questions about how HIPAA relates to your work.

“HIPAA enforcement”. In fact, the amount of discussion has far outpaced the level of enforcement. There has been so little enforcement (up until now); that even mentioning enforcement in a crowd causes apathetic yawns from some listeners.

However, the times are changing and any entity that is subject to HIPAA should take notice. Although there have been numerous HIPAA enforcement warnings, two recent developments should not be ignored.

First, CMS or the Centers for Medicare and Medicaid recently entered into a year long contract with Pricewaterhouse Cooper (PwC) to conduct nation-wide security audits of covered entities (CE’s).

The CMS contract may allow PwC to audit for the following issues among others:
- Information access management (policies and procedures for authorizing access to PHI)
- Security awareness and training (implement a security awareness and training program)
- Access control (policies and procedures for granting access to PHI)
- Workstation use (addresses functions to be performed, the manner and physical surroundings)
- Device and media controls (policies and procedures to track equipment storing PHI)

A very important issue related to the CMS action is that the HIPAA Security rule audits also mean that covered entities must be compliant with the Privacy rule.

In another major enforcement development, the civil litigation arena has seen both federal and state level courts allowing individuals to bring negligence lawsuits by using HIPAA as a “standard of care” for justifying the lawsuit.

And, as if this increase in enforcement activity is not enough to motivate covered entities to begin to take compliance seriously, in July 2007, specific legislation has been proposed in the U.S. Senate to strengthen enforcement. The legislation is called “HIPSA” or the Health Information Privacy and Security Act.

HIPSA is focused on the protection of individual privacy rights, national security, intelligence and fighting identity theft related to medical information. The following summary shows how HIPSA would function if it is enacted.

HIPSA would NOT supersede or overturn HIPAA, but would amend and assist in enforcing HIPAA.

HIPSA would mandate internal audits on the Privacy and Security rules and the creation of Risk Management processes and procedures to ensure compliance by all organizations that handle PHI.

HIPSA would re-enforce the application of HIPAA to schools, universities, and governmental organizations while broadening the impact of laws protecting medical information to all types of entities that deal with PHI beyond those to which the federal courts have currently applied HIPAA.

HIPSA would increase the criminal liability, i.e., fines and jail time beyond those found in HIPAA.

HIPSA would provide for the “debarment” of all types of organizations, including governmental, health care providers, insurers, employers, schools, and universities, for criminal violations of laws designed to protect PHI; in other words, organizations will no longer be able to receive any benefits under any Federal health program or other Federal procurement program. Finally, covered entities may also be prohibited from doing business with any organizations that conducts business with the Federal government.

(Continued on page 2)

Where can I find the latest forms and other information about HIPAA?

The HIPAA Privacy Compliance Office has developed a website for Purdue staff to access forms and other HIPAA-related information. To access the site, please visit: [http://www.purdue.edu/hipaa](http://www.purdue.edu/hipaa) or contact:
John Vaughan, Director, HIPAA Privacy Compliance
telephone: (765) 496-1927
e-mail: jvaughan@purdue.edu

---


Since the enactment of the HIPAA Privacy rule over 5 years ago and the enactment of the Security Rule over 3 years ago, a great deal of discussion has focused on the topic of HIPAA enforcement. In fact, the amount of discussion has far outpaced the level of enforcement. There has been so little enforcement (up until now); that even mentioning enforcement in a crowd causes apathetic yawns from some listeners.

However, the times are changing and any entity that is subject to HIPAA should take notice. Although there have been numerous HIPAA enforcement warnings, two recent developments should not be ignored.

First, CMS or the Centers for Medicare and Medicaid recently entered into a year long contract with Pricewaterhouse Cooper (PwC) to conduct nation-wide security audits of covered entities (CE’s).

The CMS contract may allow PwC to audit for the following issues among others:
- Information access management (policies and procedures for authorizing access to PHI)
- Security awareness and training (implement a security awareness and training program)
- Access control (policies and procedures for granting access to PHI)
- Workstation use (addresses functions to be performed, the manner and physical surroundings)
- Device and media controls (policies and procedures to track equipment storing PHI)

A very important issue related to the CMS action is that the HIPAA Security rule audits also mean that covered entities must be compliant with the Privacy rule.

In another major enforcement development, the civil litigation arena has seen both federal and state level courts allowing individuals to bring negligence lawsuits by using HIPAA as a “standard of care” for justifying the lawsuit.

And, as if this increase in enforcement activity is not enough to motivate covered entities to begin to take compliance seriously, in July 2007, specific legislation has been proposed in the U.S. Senate to strengthen enforcement. The legislation is called “HIPSA” or the Health Information Privacy and Security Act.

HIPSA is focused on the protection of individual privacy rights, national security, intelligence and fighting identity theft related to medical information. The following summary shows how HIPSA would function if it is enacted.

HIPSA would NOT supersede or overturn HIPAA, but would amend and assist in enforcing HIPAA.

HIPSA would mandate internal audits on the Privacy and Security rules and the creation of Risk Management processes and procedures to ensure compliance by all organizations that handle PHI.

HIPSA would re-enforce the application of HIPAA to schools, universities, and governmental organizations while broadening the impact of laws protecting medical information to all types of entities that deal with PHI beyond those to which the federal courts have currently applied HIPAA.

HIPSA would increase the criminal liability, i.e., fines and jail time beyond those found in HIPAA.

HIPSA would provide for the “debarment” of all types of organizations, including governmental, health care providers, insurers, employers, schools, and universities, for criminal violations of laws designed to protect PHI; in other words, organizations will no longer be able to receive any benefits under any Federal health program or other Federal procurement program. Finally, covered entities may also be prohibited from doing business with any organizations that conducts business with the Federal government.

(Continued on page 2)
ABOUT THE WORKER'S SITUATION, INCLUDING ALL DETAILS OF THE ILLNESS AND THE TREATMENT SHE HAS

You have an employee who calls in stating she won't be at work today. During the brief conversation, she tells you she has had a severe reaction to poison ivy. She has been to her health care provider, has been given some medication, and cannot come to work because she is too uncomfortable and miserable. She is hopeful she will be back to work in two or three days.

There are several people in your office that will be affected by this employee’s absence. You wonder what you could and should communicate to them. Here are three choices. Pick the one you think works best for this situation:

1. **You send an e-mail** to the entire office telling them the person won’t be in, sharing all the details of the situation the employee shared with you.

2. **You talk individually, in person, with each staff member** about the coworker’s situation, including all the details of the illness and the treatment she has sought.

3. **You talk directly with the individuals affected by the employee’s absence** and indicate that the employee won’t be at work for two or three days. No information is shared about the reason the employee is out. You discuss how the work will be accomplished in her absence.

The first choice seems quick and sufficient. Everyone gets the e-mail and you shouldn’t have any questions later about why the person is absent, etc. However, as a supervisor, sharing details about the reason an employee is on leave is not leave is not appropriate and putting medical information in an e-mail is not secure.

While the second choice is a little better than the e-mail approach, you still have shared inappropriate information about an employee to other employees.

Choice number three is the better choice. You have not disclosed why the employee cannot be at work but rather, you have talked directly with her coworkers affected by the absence and you have discussed what needs to be done while she is not at work.

While some of us consider others as our “family” at work, as a supervisor, you have different responsibilities. In general, supervisors should simply state that the employee is out for the day. A supervisor should not ask the employee for details about a medical diagnosis or treatment.

While employees are not obligated to share medical information with supervisors, it frequently occurs. With the employee’s permission, the supervisor can share the reason for the absence with coworkers, but should not share details. If an employee wants to provide medical information to coworkers or others, that is his or her choice to do so.

If anyone has any questions or concerns they can contact their employee relations consultant. Following is a link to consultants that was prepared by a third party:

http://www.purdue.edu/hr/Employee_Relations/employrelations_team.htm

### Communications Regarding Employee Leaves

**Article provided by Purdue Human Resources**

**What Should Supervisors Say?**

You have an employee who calls in stating she won’t be at work today. During the brief conversation, she tells you she has had a severe reaction to poison ivy. She has been to her health care provider, has been given some medication, and cannot come to work because she is too uncomfortable and miserable. She is hopeful she will be back to work in two or three days.

There are several people in your office that will be affected by this employee’s absence. You wonder what you could and should communicate to them. Here are three choices. Pick the one you think works best for this situation:

1. **You send an e-mail** to the entire office telling them the person won’t be in, sharing all the details of the situation the employee shared with you.

2. **You talk individually, in person, with each staff member** about the coworker’s situation, including all the details of the illness and the treatment she has sought.

3. **You talk directly with the individuals affected by the coworker’s absence** and indicate that the employee won’t be at work for two or three days. No information is shared about the reason the employee is out. You discuss how the work will be accomplished in her absence.

The first choice seems quick and sufficient. Everyone gets the e-mail and you shouldn’t have any questions later about why the person is absent, etc. However, as a supervisor, sharing details about the reason an employee is on leave is not appropriate and putting medical information in an e-mail is not secure.

While the second choice is a little better than the e-mail approach, you still have shared inappropriate information about an employee to other employees.

Choice number three is the better choice. You have not disclosed why the employee cannot be at work but rather, you have talked directly with her coworkers affected by the absence and you have discussed what needs to be done while she is not at work.

While some of us consider others as our “family” at work, as a supervisor, you have different responsibilities. In general, supervisors should simply state that the employee is out for the day. A supervisor should not ask the employee for details about a medical diagnosis or treatment.

While employees are not obligated to share medical information with supervisors, it frequently occurs. With the employee’s permission, the supervisor can share the reason for the absence with coworkers, but should not share details. If an employee wants to provide medical information to coworkers or others, that is his or her choice to do so.

If anyone has any questions or concerns they can contact their employee relations consultant. Following is a link to consultants that was prepared by a third party:

http://www.purdue.edu/hr/Employee_Relations/employrelations_team.htm

### FAQ of the Month

**Provided by the Office for Civil Rights**

**Question:**

Does the Privacy Rule permit a covered entity to use or disclose protected health information pursuant to an Authorization form that was prepared by a third party?

**Answer:**

Yes. A covered entity is permitted to use or disclose protected health information pursuant to any Authorization that meets the Privacy Rule’s requirements at 45 CFR 164.508. The Privacy Rule requires that an Authorization contain certain core elements and statements, but does not specify who may draft an Authorization (i.e., it could be drafted by any entity) or dictate any particular format for an Authorization. Thus, a covered entity may disclose protected health information as specified in a valid Authorization that has been created by another covered entity or a third party, such as an insurance company or researcher.

Note: HIPAA does not require a covered component to draft the HIPAA authorization to be used, however, the covered component does need to ensure that the authorization contains all of the statements required by HIPAA. If an authorization is to be used for a disclosure where a HIPAA authorization is required, the authorization must be reviewed by the HIPAA Privacy Compliance Office prior to the disclosure!

### Enforcement Heats Up....Continued from page 1

HIPAA would allow individuals to sue directly on the federal level for compensatory and punitive damages for knowing or negligent violations relating to the individual’s right to privacy in medical information. In addition, it would make the covered entity or a “principal” jointly and severally liable with the principal’s “agent” for these types of damages for any actions of the principal’s agent acting within the scope of the agency.

HIPPA would allow for enforcement by State Attorney Generals or local law enforcement agencies able to prosecute consumer protection laws, to bring civil actions in the Federal District Court to “obtain civil penalties of not more than $1,000 per day per individual whose personally identifiable information was, or is reasonably believed to have been, accessed or acquired by an unauthorized person, up to a maximum of $50,000 per day”.

HIPSA would protect employees against employers that “discharge, demote, suspend, threaten, harass, retaliate against, or in any other manner discriminate or cause any employer to discriminate against an employee,” that blows the whistle against the employer for violations of the HIPSA Act.

In summary, HIPAA / HIPSA enforcement is not going away. “Band-Aid compliance” efforts, i.e., using canned policies and procedures without taking any real compliance actions or relying on “inaccurate advice” from naysayers who believe that the privacy regulations are inconsequential may backfire on organizations that don’t take steps towards real compliance. Also see: http://lists.essential.org/pipermail/med-privacy/2007q3/000794.html

Purdue University is an equal access/equal opportunity university