A Notice of Proposed Rulemaking concerning the accounting of disclosures requirement under the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule, is available for public comment. The proposed rule would give people the right to get a report on who has electronically accessed their protected health information.

The U.S. Department of Health and Human Services’ (HHS) Office for Civil Rights (OCR) is proposing changes to the Privacy Rule, pursuant to the Health Information Technology for Economic and Clinical Health (HITECH) Act. HITECH is part of the American Recovery and Reinvestment Act of 2009.

“This proposed rule represents an important step in our continued efforts to promote accountability across the health care system, ensuring that providers properly safeguard private health information,” said OCR Director Georgina Verdugo. “We need to protect peoples’ rights so that they know how their health information has been used or disclosed.”

People would obtain this information by requesting an access report, which would document the particular persons who electronically accessed and viewed their protected health information. Although covered entities are currently required by the HIPAA Security Rule to track access to electronic protected health information, they are not required to share this information with people.

The proposed rule requires an accounting of more detailed information for certain disclosures that are most likely to affect a person’s rights or interests. The proposed changes to the accounting requirements provide information of value to individuals while placing a reasonable burden on covered entities and business associates.

People may now read the proposed rule at: http://www.federalregister.gov/ and submit comments to http://www.regulations.gov/ (search for Proposed Rule) through August 1, 2011.

People who believe a covered entity has violated their (or someone else’s) health information privacy rights or committed another violation of the HIPAA Privacy or Security Rules, may file a complaint with OCR at http://www.hhs.gov/ocr/privacy/hipaa/complaints/index.html. Additional information about OCR’s enforcement activities can be found at http://www.hhs.gov/ocr.

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 or contact:

Joan Vaughan, Director, HIPAA Privacy Compliance
telephone: (765) 496-1927
e-mail: jvaughan@purdue.edu
New Data Handling Educational Resources Available

How the University handles the vast amounts of data entrusted to it continues to be something that every Purdue employee is interested in. The Purdue University Data Stewards Organization (http://www.purdue.edu/securePurdue/policies/dataStewards.cfm) has recently created a Educational Resources webpage (http://www.purdue.edu/securePurdue/procedures/dataClassif/Resources.cfm). The new webpage features new and revised data handling training resources. The newest resources include a data handling power point presentation and an updated version of the “Keys to Securing Purdue’s Data” pamphlet.

Security Policy Exception Process

From the March 2011 Secure Purdue News

Purdue’s information security policies and standards are designed to protect Purdue University data and IT Resources. These documents set the minimum levels of security that are necessary to protect these resources while still allowing University business to carry on in an efficient fashion.

IT Networks and Security (ITNS) is responsible for administering Purdue’s information security policies. ITNS is also responsible for administering the Security Policy Exception process. The security policy exception process is used when unique situations require a deviation from an identified policy or standard. Any exception to an information security policy or standard weakens protection for our IT Resources and underlying data. However, sometimes circumstances require an exception.

Under the Security Policy Exception process, there are only two reasons that justify an information security policy exception.

> The first is when compliance with an information security policy or standard adversely affects business objectives.

> The second reason is when the cost to comply with an information security policy offsets the potential risk or cost of non-compliance. Departments and units requesting an exception work with ITNS to describe the reasons needed for an exception.

To learn more about the Security Policy Exception Process or to view the Request for Security Exception Form, please visit: http://www.purdue.edu/securepurdue/bestPractices/deviationProcedure.cfm

Information security policy exceptions are valid for a one-year period. ITNS works with departments and units annually to determine whether any previously approved exceptions are still valid. You can send questions about the Security Policy Exception process to securepurdue@purdue.edu.

Communications Regarding Employee Leaves

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 to call for your area: http://www.purdue.edu/hr/Employee_Relations/employ-relations_team.htm

Purdue University is an equal access/equal opportunity university