



*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 Privacy Rule Enforcement Highlights  
 (As of November 30, 2010)**

*Provided by the Office for Civil Rights*

The HIPAA Privacy Rule is a set of federal standards to protect the privacy of patients' medical records and other health information maintained by covered entities: health plans, which include many governmental health programs, such as the Veterans Health Administration, Medicare and Medicaid; most doctors, hospitals and many other health care providers; and health care clearinghouses. These standards provide patients with access to their medical records and with significant control over how their personal health information is used and disclosed. Compliance with the standards was required as of April 14, 2003 for most entities covered by HIPAA. On that date, OCR began accepting complaints involving the privacy of personal health information in the health care system.

**Privacy Rule Enforcement Results as of the Date of This Summary**

HHS / OCR has investigated and resolved over 12,336 cases by requiring changes in privacy practices and other corrective actions by the covered entities. Corrective actions obtained by HHS from these entities have resulted in change that is systemic and that affects all the individuals they serve. HHS has successfully enforced the Privacy Rule by applying corrective measures in all cases where an investigation indicates noncompliance by the covered entity. OCR has investigated complaints against many different types of entities including: national pharmacy chains, major medical centers, group health plans, hospital chains, and small provider offices. In another 6,500 cases, our investigations found no violation had occurred. In the rest of our completed cases (32,883), HHS determined that the complaint did not present an eligible case for enforcement of the Privacy Rule. These include cases in which:

- ✿ OCR lacks jurisdiction under HIPAA – such as a complaint alleging a violation prior to the compliance date or alleging a violation by an entity not covered by the Privacy Rule;
- ✿ the complaint is untimely, or withdrawn or not pursued by the filer;
- ✿ the activity described does not violate the Rule – such as when the covered entity has disclosed protected health information in circumstances in which the Rule permits such a disclosure.

In summary, since the compliance date in April 2003, HHS has received over 56,754 HIPAA Privacy complaints. We have resolved over ninety-one percent of complaints received (over 51,719): through investigation and enforcement (over 12,336); through investigation and finding no violation (6,500); and through closure of cases that were not eligible for enforcement (32,883).

From the compliance date to the present, the compliance issues investigated most are, compiled cumulatively, in order of frequency:

Impermissible uses and disclosures of protected health information;

- ✿ Lack of safeguards of protected health information;
- ✿ Lack of patient access to their protected health information;
- ✿ Uses or disclosures of more than the Minimum Necessary protected health information; and
- ✿ Complaints to the covered entity.

The most common types of covered entities that have been required to take corrective action to achieve voluntary compliance are, in order of frequency:

- ✿ Private Practices;
- ✿ General Hospitals;
- ✿ Outpatient Facilities;
- ✿ Health Plans (group health plans and health insurance issuers); and,
- ✿ Pharmacies.



**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, x61927



## New Security Educational and Training Resources

Article from the SecurePurdue News & Alerts

### 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 has recently created an Educational Resources webpage. The new webpage features new and revised data handling training resources.

<http://www.purdue.edu/securePurdue/policies/dataStewards.cfm>

The newest resources include a data handling power point presentation and an updated version of the “Keys to Securing Purdue’s Data” pamphlet.

<http://www.purdue.edu/securePurdue/procedures/dataClassif/Resources.cfm>



### New Purdue Cybersecurity Training Video

View the latest [SecurePurdue Cybersecurity Training Series Video on Social Networking](#). The video was created by the Video and Multimedia Production Services (VMPS) group within Information Technology at Purdue (ITAP).

You can view the video at:

<http://www.purdue.edu/se-curepurdue/videos/socialNetworkPrivacy.wmv>

You can view other videos at:

<http://www.purdue.edu/securepurdue/training/>

## Social Networking Sites

Social networking sites (e.g. Facebook, Myspace and Twitter) are increasingly used by staff to maintain social and professional relationships with friends and colleagues. Care should be taken in ensuring that conversations do not include topics that may breach the confidentiality of employees or patients or that may cause embarrassment to Purdue University. You should not expect that any information shared on a social media site will remain “private” regardless of your settings. As stated in University HIPAA policy and within the HIPAA confidentiality agreement that you signed, no protected health information



## Social Networking Sites...continued

may be disclosed, other than for appropriate business purposes, and only using approved tools and methods. Social networking sites are not approved, and no protected health information should ever appear on these sites. Protected health information includes any information that can be used to identify an individual, even if the individual’s name is not mentioned. Noncompliance with HIPAA policies and procedures may result in sanctions up to and including termination.

Therefore, staff are prohibited from posting on any social media site any content that includes protected health information and/or patient images (including patient photographs, x-ray and other diagnostic images, as well as any photographs that may depict protected health information in the background). Even though a patient’s name is not shared, other information included in the discussion may be enough to identify an individual and, therefore, violate their privacy and violate HIPAA laws. This prohibition applies even in cases in which you believe there is no HIPAA violation because the patient has consented, or for any other reason.



Additionally, benefit or claims details about employees should not be shared on these sites, even for business purposes.



Opinions about process improvement or errors in providing services should be expressed to the staff member’s supervisor, not on social networking sites.



Also prohibited is usage of social media sites to provide medical advice or medical commentary on the behalf of Purdue or to use the sites to make, recommend or increase referrals to physicians.



Sharing on social networking sites of any confidential information pertaining to Purdue University practices or administration is prohibited.

Risks to security are also present in using these sites. Information shared among participants may not be encrypted and others outside of your workgroup, including friends or friends of friends, may have access to this information.

