Employee Wellness Program Safeguards

With the prevalence of employer-sponsored employee wellness programs, there is the concern that information collected about participants could be used by employers in making employment decisions. Where a workplace wellness program is offered through a group health plan, protections are in place under HIPAA with respect to access by the employer as plan sponsor to individually identifiable health information about participants in the program.

The HIPAA Privacy and Security Rules place restrictions on the circumstances under which a group health plan may allow an employer as plan sponsor access to protected health information (PHI), including PHI about participants in a wellness program offered through the plan, without the written authorization of the individual. Often, the employer as plan sponsor will be involved in administering certain aspects of the group health plan, which may include administering wellness program benefits offered through the plan. Where this is the case, and absent written authorization from the individual to disclose the information, the group health plan may provide the employer as plan sponsor with access to the PHI necessary to perform its plan administration functions, but only if the employer as plan sponsor amends the plan documents and certifies to the group health plan that it agrees to, among other things:

- Establish adequate separation between employees who perform plan administration functions and those who do not;
- Not use or disclose PHI for employment-related actions or other purposes not permitted by the Privacy Rule;
- Where electronic PHI is involved, implement reasonable and appropriate administrative, technical, and physical safeguards to protect the information, including by ensuring that there are firewalls or other security measures in place to support the required separation between plan administration and employment functions; and Report to the group health plan any unauthorized use or disclosure, or other security incident, of which it becomes aware.

Further, where a group health plan has knowledge of a breach of unsecured PHI at the plan sponsor (i.e., an unauthorized use or disclosure that compromises the privacy or security of the PHI), the group health plan, as a covered entity under the HIPAA Rules, must notify the affected individuals, HHS, and if applicable, the media, of the breach, in accordance with the requirements of the Breach Notification Rule.

Where the employer as plan sponsor does not perform plan administration functions on behalf of the group health plan, access to PHI by the plan sponsor without the written authorization of the individual is much more circumscribed. In these cases, the Privacy Rule generally would permit the group health plan to disclose to the plan sponsor only:

1. information on which individuals are participating in the group health plan or enrolled in the health insurance issuer or HMO offered by the plan; and/or
2. summary health information if requested for purposes of modifying the plan or obtaining premium bids for coverage under the plan.

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: Joan Vaughan, HIPAA Privacy Officer
telephone: (765) 496-1927
e-mail: jvaughan@purdue.edu
The Threat of Cyber-Attacks
Most everyone has seen news reports of cyber-attacks against, for example, national retail chains or the information networks of the federal government. Health care providers and covered entities may believe that if they are small and low profile, they will escape the attention of the “hackers” who are running these attacks. Yet every day there are new attacks aimed specifically at small to mid-size organizations because they are less likely to be fully protecting themselves. Criminals have been highly successful at penetrating these smaller organizations and carrying out their activities, while their unfortunate victims are unaware until it is too late.

Cybersecurity refers to ways to prevent, detect, and respond to attacks against or unauthorized access against a computer system and its information. Cybersecurity protects your information or any form of digital asset stored in your computer or in any digital memory device.

It is important to have strong cybersecurity practices in place to protect patient health information, organizational assets, your operations, and your personnel, and of course to comply with the HIPAA Security Rule. Cybersecurity is needed whether you have your protected health information locally installed in your office or access it over the Internet from a cloud service provider.

The Office of the National Coordinator for Health Information Technology (ONC) offers online Cybersecurity information, including the Top 10 Tips for Cybersecurity in Health Care, to help you reduce your risk. For a full overview of security standards and required protections for ePHI under the HIPAA Security Rule, visit OCR’s HIPAA Security Rule web page.

- [http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/](http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/) (Continued left-FAQ’s from OCR)

FAQ’s from OCR

Question: Do the HIPAA Privacy Rule’s provisions permitting certain incidental uses and disclosures apply only to treatment situations or discussions among health care providers?

Answer: No. The provisions apply universally to incidental uses and disclosures that result from any use or disclosure permitted under the Privacy Rule, and not just to incidental uses and disclosures resulting from treatment communications, or only to communications among health care providers or other medical staff. For example:

- A provider may instruct an administrative staff member to bill a patient for a particular procedure, and may be overheard by one or more persons in the waiting room.

- A health plan employee discussing a patient’s health care claim on the phone may be overheard by another employee who is not authorized to handle patient information.

If the provider and the health plan employee made reasonable efforts to avoid being overheard and reasonably limited the information shared, an incidental use or disclosure resulting from such conversations would be permissible under the Rule.

Question: Can a postsecondary institution be a “hybrid entity” under the HIPAA Privacy Rule?

Answer: Yes. A postsecondary institution that is a HIPAA covered entity may have health information to which the Privacy Rule may apply not only in the health records of nonstudents in the health clinic, but also in records maintained by other components of the institution that are not education records or treatment records under FERPA, such as in a law enforcement unit or research department. In such cases, the institution, as a HIPAA covered entity, has the option of becoming a “hybrid entity” and, thus, having the HIPAA Privacy Rule apply only to its health care unit. The school can achieve hybrid entity status by designating the health unit as its “health care component.” As a hybrid entity, any individually identifiable health information maintained by other components of the university (i.e., outside of the health care component), such as a law enforcement unit, or a research department, would not be subject to the HIPAA Privacy Rule, notwithstanding that these components of the institution might maintain records that are not “education records” or treatment records under FERPA.

To become a hybrid entity, the covered entity must designate and include in its health care component all components that would meet the definition of a covered entity if those components were separate legal entities. (A covered entity may have more than one health care component.) However, the hybrid entity is not permitted to include in its health care component other types of components that do not perform the covered functions of the covered entity or components that do not perform support activities for the components performing covered functions. That is, components that do not perform health plan, health care provider, or health care clearinghouse functions and components that do not perform activities in support of these functions (as would a business associate of a separate legal entity) may not be included in a health care component. Within the hybrid entity, most of the HIPAA Privacy Rule requirements apply only to the health care component, although the hybrid entity retains certain oversight, compliance, and enforcement obligations. See 45 CFR § 164.105 of the Privacy Rule for more information.