Notice of Privacy Practices Distribution

The Notice of Privacy Practices or privacy notice is a document that describes how medical information about an individual may be used and disclosed and how that individual can gain access to this information.

HIPAA requires that covered healthcare providers make a good faith effort to distribute the Notice of Privacy Practices for Purdue’s Health Care Providers at the time of first service delivery and obtain an acknowledgement of receipt of the notice. This includes service by telephone.

The HIPAA Privacy Compliance Office recommends that when a health care provider delivers service by telephone that the following procedure should be used:

1. Determine whether the patient has already received a privacy notice. If they have received the notice, you do not need to do anything more.
2. If they have not received the notice, ask the patient whether they would like to receive the notice at their next office visit or whether they would prefer to have it mailed to them. If the patient prefers to wait until the next office visit, you have met your obligation.
3. If they would like to have the notice mailed to them, mail the notice with the standard letter which includes a request for the patient to return a signed acknowledgement. No followup on the acknowledgement is required. If the acknowledgement is received, it should be filed in the patient’s chart. The standard letter can be obtained from:

   http://www.purdue.edu/hipaa/genprofor/genprofor.htm

A health plan must distribute the Notice of Privacy Practices for Purdue University Health Plans to all members of the health plan at time of enrollment and must notify members at least once every 3 years that the notice is available and how to obtain a copy. Purdue’s healthplan has distributed the notice to all health plan members and will send a reminder of the availability of the notice to members annually.

** There may be differences in the way departments implement this procedure. It is wise to check with your HIPAA liaison prior to implementing any new procedure in your area!

Purchasing New Software or Making Software Changes?

If you are planning to either purchase new computer software or make changes to existing software in your area and that software stores or processes protected health information, please notify your HIPAA liaison immediately.

The HIPAA liaison should contact the ITaP Security and Policy department to be sure that the software’s security features are compliant with HIPAA, GL BA and FERPA regulations.

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
**Did You Know?...Accounting of Disclosures**

HIPAA regulations grant individuals the right to receive an accounting of disclosures of protected health information made by a covered component for the six years prior to the request, but on or after 4/14/2003.

The following disclosures need to be tracked:

- Required by law
- Required for public health activities
- For health oversight activities
- Reports of abuse
- For judicial and administrative proceedings (i.e., Subpoenas, court orders, etc.).
- For law enforcement purposes
- To the coroner
- For research (except where authorized or pursuant to a limited Data Set Agreement)
- To avert a threat of serious injury
- Unlawful or unauthorized disclosures

A **Record of Disclosure form** is used to record disclosures that need to be tracked. Your HIPAA Liaison can explain to you when disclosures need to be tracked in your area.

**Disclosures for which you obtained an authorization do NOT need to be tracked.**

**Did You Know?...Inadvertent Disclosures**

Any disclosure of protected health information that is unauthorized by the HIPAA regulations is an inadvertent disclosure.

These inadvertent disclosures need to be reported to your HIPAA Liaison so that they can be tracked, as they need to be reported to an individual who requests an accounting.

Examples of inadvertent disclosures include:

- A document containing billing information for treatment at the health center was left on the copy machine and found by another individual.
- A conversation between 2 staff members of the health plan about a member’s health plan selections occurred in an elevator and was overheard by a person who did not have a legitimate reason to know.
- A document containing protected health information was faxed by Accounts Receivable to the wrong fax number.

**FAQ of the Month**

Provided by the Office of Civil Rights

**Question:** Generally, what does the HIPAA Privacy Rule require the average provider or health plan to do?

**Answer:**

For the average health care provider or health plan, the Privacy Rule requires activities, such as:

- Notifying patients about their privacy rights and how their information can be used.
- Adopting and implementing privacy procedures for its practice, hospital, or plan.
- Training employees so that they understand the privacy procedures.
- Designating an individual to be responsible for seeing that the privacy procedures are adopted and followed.
- Securing patient records containing individually identifiable health information so that they are not readily available to those who do not need them.

Responsible health care providers and businesses already take many of the kinds of steps required by the Rule to protect patients’ privacy. Covered entities of all types and sizes are required to comply with the Privacy Rule. To ease the burden of complying with the new requirements, the Privacy Rule gives needed flexibility for providers and plans to create their own privacy procedures, tailored to fit their size and needs. The scalability of the Rule provides a more efficient and appropriate means of safeguarding protected health information than would any single standard. For example,

- The privacy official at a small physician practice may be the office manager, who will have other non-privacy related duties; the privacy official at a large health plan may be a full-time position, and may have the regular support and advice of a privacy staff or board.
- The training requirement may be satisfied by a small physician practice’s providing each new member of the workforce with a copy of its privacy policies and documenting that new members have reviewed the policies; whereas a large health plan may provide training through live instruction, video presentations, or interactive software programs.
- The policies and procedures of small providers may be more limited under the Rule than those of a large hospital or health plan, based on the volume of health information maintained and the number of interactions with those within and outside of the health care system.