

## HIPAA Tutorial

- 1: As a UPMC employee, you are expected to keep your password confidential, log off computers when not in use and not to download information from sources you cannot trust. You are also expected to keep PHI confidential and properly dispose PHI as necessary.
- 2: Private and confidential information should only be accessed by employees when performing their job responsibilities.
- 3: Employees should never conduct hospital business or discuss confidential information in public areas.
- 4: If you overhear others discussing confidential information, let them know that they can be overheard. You should also report the incident to your hospitals' privacy officer.
- 5: Employees are prohibited from accessing medical records of their spouses, children, relatives, and others. Employees are permitted only to access information needed to perform their job.
- 6: Always discard confidential information in a shredding bin. Never discard paper, computer discs, or other portable media that contain patient information in a routine wastebasket. This makes the information accessible to unauthorized personnel.
- 7: Always direct news media inquiries to UPMC Media Relations department.
- 8: Remember, you are accountable for any actions made under your username and password. If someone learns your password, you should immediately change your password and tell your supervisor and privacy officer.
- 9: It is every employee's responsibility to be alert to unethical behavior or possible violations of UPMC policies, which includes but is not limited to inappropriate use or disclosure of protected health information.
- 10: Do not give your supervisor your password. Treat your password as you would any other piece of personal and confidential information by taking measures to keep it confidential. Remember, you are accountable for any actions made under your username and password.
- 11: Because many staff often share one printer, it is necessary to take measures to protect confidential information when printing. Follow the guidelines outlined in this course and if you have any questions ask your supervisor or manager.

12: Strict rules apply to the release of protected health information when necessary for reasons other than treatment, payment, or health care operations (TPO). These rules vary based on the sensitivity of the information. If you are involved with disclosing PHI, you are responsible for being aware of these rules as outlined in the policy.

13: The facility must notify the patient in writing of whether the request to amend was approved or denied. The patient may submit a statement of disagreement which will become part of the patient record when an amendment request is denied.

14: Notice of Privacy Practices (NOPP) describes how PHI may be used or disclosed, patient rights under HIPAA, and who to contact if patients believe their rights have been violated. The Notice of Privacy Practices is to be posted and made available in public areas of health care facilities, such as a registration area. The notice also must be given to patients during their first visit to UPMC and offered each additional time a patient registers for services.

15: The faxing of protected health information (PHI) should be performed only when absolutely necessary. Other, more secure ways of sending information should be considered (i.e., secure e-mail, registered/insured mail, etc). When you are asked to fax information to a UPMC location, determine if they can access the information electronically which would eliminate the need to fax the information.

If you must fax, use a cover sheet that shows your contact information and contains a confidentiality disclaimer. If pre-programmed fax numbers are available use these to dial when faxing information. After the fax has been transmitted, verify with the recipient that the fax had been received. Follow the guidelines outlined in this course.