UPMC Horizon

HIPAA Privacy & Security Awareness Training for Students

February 2010

1.Privacy and Security Awareness Introduction

Numerous federal and state laws require that UPMC protect information that is created or collected for a variety of purposes, including patient care, employment, and retail transactions. Education and training is a key element of an effective compliance program. The Privacy and Security Awareness training is an example of UPMC's commitment to educate and promote a culture that encourages ethical conduct and compliance with applicable laws.

After completing this course you should be able to explain:

- your obligations regarding privacy
- your responsibilities for protecting information
- what you should do in the event that you suspect that a breach may have occurred

Additionally, you should become familiar with the UPMC policies that discuss these subject matters. All policies that are mentioned in this course will be reviewed from time to time and may change. It is your responsibility to periodically check these and become familiar with any changes or updates.

1.1 What is Privacy and Security?

Privacy is UPMC's obligation to limit access to information on a need-to-know basis to individuals or organizations so that they can perform a specific function for or on behalf of UPMC. This includes verbal, written, and electronic information.

- **Security** - ensure that only those who need to have access to information can access the information. Security also includes ensuring the availability and integrity of information.
- **Need-to-know basis** - information should only be provided to those that need it to perform their assigned job responsibilities.

1.2 Complying with UPMC Privacy and Security Policies

As an employee/volunteer you are to comply with UPMC's Privacy and Security policies and procedures. To increase patient confidence, and ensure that information is protected at UPMC, all employees are required to:

- abide by UPMC policies and all applicable laws
- protect patient privacy
- safeguard confidential information
- read and understand policies related to their job function

Every employee/volunteer must respect our patient's expectations that their information will be kept confidential.

1.3 Consequences for Violating Privacy and Security Policies

Employees/volunteers who violate any UPMC policy that supports compliance with HIPAA regulations may receive disciplinary action, up to and including termination.

- The United States Department of Health and Human Services has appointed government agencies to enforce HIPAA compliance. Those who violate HIPAA can face the following penalties:
    - individual fines of up to $250,000
    - imprisonment up to 10 years

1.4 What is PHI?

Protected health information (PHI) includes any health information about our patients and is considered confidential. PHI can include, but is not limited to:

General Information:

- patient's name
- medical record number
- social security number
- address
- date of birth

Health Information:

- diagnosis
- medical history
- medications

Medical Coverage Information
Dental Coverage Information

2.Safeguarding Information

You are only permitted to access and use patient information as it relates to your job. If you see or hear patient information in the course of doing your job that you do not need to know, remember that this information is confidential. You are not permitted to repeat it or share it with others - even friends, family, or other employees who do not have a need to know it.

- Additionally, you are not permitted to share this information with others when you no longer work for UPMC.
- All UPMC staff members/volunteers play an important role in safeguarding sensitive information.
- You are obligated to maintain a patient's privacy and safeguard protected health information (P

2.1 Information Without Safeguards

An unauthorized individual may be able to gain access to information if sufficient safeguards are not in place. This information may reveal confidential patient, staff, financial, research, or other business information.

- **Places where this type of information may be accessed:**
    1. computers that were left logged into
    2. overheard in cafeterias or hallways
    3. found on fax machines and/or printers

4. found in a wastebasket
5. seen lying on a desk or counter

- **And it could be used in an inappropriate manner to:**

1. reveal confidential information
2. sell information to a tabloid
3. cause negative publicity

- **If this occurs:**

1. A patient's privacy rights may have been violated.
2. State and federal laws may have been violated.
3. UPMC and associated staff may be responsible for damages.

2.2 Potential Threats or Activities that May Compromise Information

There are many ways that confidential information can be inappropriately accessed or disclosed. All must be reported to your manager or Privacy Officer.

These may include:

- unauthorized access to information, either by an unauthorized individual or by an individual who has the right to access to information, but accesses the information for unauthorized reasons
- computer viruses
- inappropriately deleting information
- during a burglary, paper information may be accessed or duplicated
- theft of computer equipment, records, and/or information
- unauthorized disclosure of information

3.Protecting Privacy

By following certain guidelines, you can protect information and the privacy of our patients. Use the following safeguards in your daily activity.

3.1 Oral communication

Confidential or sensitive information should only be communicated or accessed on a need-to-know basis. You should access only the minimum amount of this type of information needed to perform your job.

You can maintain privacy by:

- disclosing confidential information only to those who have a need to know it
- speaking in an appropriate tone of voice (lower your voice when others are nearby and may be able to overhear your conversation)
- moving the discussions to areas where others cannot overhear
- asking those around you who do not need to know this information to leave the area so you may have privacy

- not conducting conversations which include confidential information in high-traffic areas such as hallways, reception areas, waiting rooms, elevators, and cafeterias

3.2 What Should You Do?

A health care employee was using a cellular telephone when discussing protected health information (PHI) in a restaurant down the street from the hospital. Another hospital employee sitting nearby overheard the conversation and approached the individual.

The right thing to do . . .

- Employees/volunteers should never conduct hospital business and discuss confidential information in public areas.
- All hospital employees/volunteers have the responsibility to abide by hospital policies and to protect patient privacy.
- Protecting patient privacy is an expectation of all employees whether on duty or off duty.
- If you overhear others discussing confidential information, let them know that they can be overheard.
- In any event, any information that you overhear should not be repeated or communicated to others.
- You should report inappropriate incidents or situations to your hospital's privacy officer.

3.3 Physical Security

Simple measures can be taken to prevent an unauthorized individual from gaining physical access to confidential information.

These measures include:

- Question individuals you do not recognize if they are in or near areas that contain confidential information.
- Offer assistance to those who may be lost.
- Keep file cabinets, doors, and desks locked in nurses' stations, offices, etc.
- Insist that all repair/maintenance personnel show proper identification if they arrive in your work area to service equipment. If necessary, call the service company to have the identity of the repair or maintenance personnel confirmed. Accompany visitors and repair/maintenance personnel to and from their destinations.
- Notify Security when there is an unauthorized individual in a secured work area.
- Restrict access to computers and data centers to prevent unauthorized individuals from accessing electronic information.
- Ensure that any vendor representative, especially from the pharmaceutical, biotechnology, medical device, and hospital equipment industries, has registered with UPMC Supply Chain Management before they appear onsite.

3.5 Photocopiers

When making copies of confidential information, you should not leave the copier until your job is complete.

Additionally, employees/volunteers should:

- Remove all papers containing confidential information.

- Check all areas of the photocopier, including the output tray, the input feeder, and the top of the glass surface.
- Not allow others to see the information that you are copying. If someone is standing close enough to see this information, advise him or her that you are copying confidential information. Offer to let the person know when you are finished so that he or she may come back to use the machine.
- Destroy or return any confidential information that has been left on a photocopier to the owner.

3.6 Fax Machines

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, you are required to use the UPMC approved standard fax cover sheet. This sheet contains your contact information and a confidentiality disclaimer.

Additionally, employees/volunteers should:

- When possible, program automated dial buttons with frequently dialed fax numbers.
- Confirm the fax and telephone numbers of the person you are faxing to.
- Prior to faxing confidential information, let the person you are faxing to know so he or she may retrieve it from the fax machine immediately.
- Follow up with the person to verify that he or she received the fax.
- Destroy confidential information that has been received in error and advise the sender of the error.
- Periodically verify that pre-programmed fax numbers are still correct.
- Contact the privacy officer to report inadvertent faxing to the wrong person.
- Consider using other means as opposed to faxing.

3.8 Disposal of Confidential Information

Never discard paper, computer disks, or other portable media that contain patient information in a “routine” wastebasket. This makes the information accessible to unauthorized personnel. Such confidential information should be discarded in accordance with your business unit’s policies regarding the destruction of protected health information.

- Always shred or dispose of confidential information in an appropriate designated container.
- Check with your manager or supervisor to find out how your department disposes of confidential information.

3.9 News Media Inquiries

The news media may contact your facility for information if a well-known person or someone involved in a newsworthy situation, such as an accident, is being treated at your facility.

- Direct all news media inquiries to Public Relations, ext. 5782.

3.10 Report Inappropriate Use of Patient Information

If you feel that a patient’s privacy or confidentiality has been violated, report the incident to your facility’s or business unit’s privacy officer. If they are unavailable or you are not comfortable reporting it to them, you can also use the following options:

- UPMC HIPAA Program Office at 412-647-5757
- Compliance Helpline (anonymous option) toll-free at 1-877-983-8442

4.Protecting Electronic Information

Every UPMC staff member plays an important role in protecting UPMC's electronic patient, business, personnel, academic, and research information. Staff shall take reasonable precautions to ensure that electronic information is available, has integrity, and is secured against unauthorized access.

4.1 Creating and Protecting Passwords

A password is a unique combination of letters, numbers, and symbols that you use to verify your identity in a computer system. Your password is the electronic equivalent of your signature.

- Do not share your password with anyone (this includes your boss and the information technology staff).
- You are responsible for all actions performed under your username and password.
- Treat your password as you would treat any piece of personal and confidential information by taking measures to keep it confidential.

Passwords:

- are used to verify your identity in a computer system
- should be a unique combination of letters, numbers, and symbols
- is the electronic equivalent of your signature

4.3 Creating Complex Passwords

Knowing how to create a complex password (one that cannot be guessed easily by someone else) is one way to protect your password.

- Don't base your password on information that is commonly known about you, such as your birth date, the names of your children or pets, or a hobby.

- It's also best to avoid common words, such as mother or father.

Passwords should meet the following requirements:

- must not contain all or part of the user's account name
- must be at least seven characters long
- **must contain characters from three of the following four categories:**

1. uppercase characters
2. lowercase characters
3. numbers, 0-9
4. non-alphanumeric characters (!, #, %, *,)

- **Examples:**

1. I love to golf! = Iluv2GLF!

2. Opera singer = 0praS!ngr

3. I owe you $44.95 = iOu$4495

4.5 Protecting Your Password

Once you've selected a complex password, follow these tips to keep it confidential:

- Don't share your password with anyone.
- Memorize your password.
- Never store your password in a computer file or PDA.
- Do not keep a written password in plain view or easily accessible to others. All written passwords are to be kept secured.
- If someone learns your password, you should immediately:

  1. change your password
  2. tell your supervisor and privacy officer

Remember, you are accountable for any actions made under your username and password.

4.6 Protecting Your Computer from Viruses

A virus is a computer program that performs unexpected or unauthorized actions. A virus can occur without your permission or knowledge. Viruses threaten all types of information, can render a system unavailable, and corrupt information contained in a system.

A virus might:

- expose or change confidential information
- delete or remove important files
- display unusual messages
- e-mail everyone in your address book
- disable computers
- spread to other computers

4.7 Signs of a Computer Virus

Contact the ISD Help Desk at 412-647-HELP (4357) or the help desk for your UPMC facility if you notice any of the following which might indicate your computer is infected with a virus:

- antivirus software pop-up alerts
- missing files
- unusual activity (for example, programs opening that you did not open)
- responses to e-mails that you did not send
- drastic, unexplained reductions in your computer's memory or disk space

4.8 Preventing Viruses

Precautions that you can take to help protect your computer from becoming infected with a virus are:

- Never open or run unexpected e-mail attachments or other programs.

- Always use antivirus software and never disable it.
- Scan all e-mails and downloads.

4.9 Appropriate Use of E-mail

Electronic mail (e-mail) is provided for the purpose of conducting UPMC business and providing service to our customers. Appropriate use of e-mail can prevent the accidental disclosure of confidential information and the disruption of computer services.

As an employee/volunteer:

- Use e-mail only for official UPMC business and in accordance with UPMC policies.
- Do not use e-mail in a way that is disruptive, offensive, or harmful.
- Do not use e-mail to sponsor or promote a political party or candidate or to campaign against a political party or candidate.
- Do not use e-mail to solicit employees to support any group or organization.
- Confirm destination of e-mail addresses you are sending to.
- Do not use “reply all” unless necessary.

Prior to communicating with patients via e-mail, review the UPMC policy HS-1SO147, Electronic Mail and Messaging. This will describe the guidelines to follow, such as:

- Getting the patient to sign a consent form.
- Using an appropriately worded footer in e-mails.

Although it is delivered electronically, e-mail is still a written form of communication. Approach it as you would other forms of written communication, such as a memo or fax.

You should:

- Delete unnecessary e-mail.
- Use additional security methods when sending confidential information.
- Include a confidentiality disclaimer on e-mails.
- Don’t write something in an e-mail that you would not say in an official memo.

4.11 Printers

Because many employees/volunteers often share one printer, it is necessary to take measures to protect confidential information when printing.

Follow these steps:

- If your business unit has a Xerox multi-function machine you should use the “Secure” printing option. This means the document will not print until you release it by entering a code number that you select.
- If your business office does not have a Xerox multi-function machine then you should retrieve your documents immediately.

No matter what type of machine you are printing to, you must:

- Confirm to which printer you are printing, especially if you share a network printer.
- Immediately remove confidential items.
- Cancel or retrieve any confidential information printed on the wrong printer.
- Deliver or dispose of confidential information found on a printer.
- Only print what is necessary if you need to maintain a hard copy.

4.12 Internet Use

The Internet is a great source of information and a way to improve business efficiency. UPMC provides Internet access to facilitate business and for educational purposes.

- Do not use the Internet in a way that violates UPMC policies.
- Do not download software that is not approved for UPMC computers, including screen savers and games.
- Do not view information that is offensive, disruptive, or harmful to morale.
- Use antivirus software.

4.13 Proper Computer Workstation Use

Be sure to restrict the view or access of others by positioning your computer screen so that others cannot view it. Place your computer workstation in a secure area that is not easily accessible by unauthorized personnel. Make sure your screen saver is set to automatically activate and lock your computer and hide confidential information when your computer is not in use. If you cannot restrict others from viewing your screen, ask your manager to order a privacy screen for you that will be placed over your monitor. The privacy screen prohibits people who are not directly lined up to the monitor from viewing the information on the screen.

Employees/volunteers should:

- restrict views of others
- place computers in secure areas
- use automatic screen savers that lock your computer

4.14 Log on and sign off procedures

Follow appropriate log on and sign off procedures. Follow these guidelines even when you are remotely logging into the UPMC system and accessing confidential information.

- Never use someone else's username and password or allow someone else to use yours.
- Don't offer to sign onto a computer so someone else may use it.
- Prevent another person from using your sign-on by locking or signing-off your computer workstation when leaving it unattended.
- To lock your workstation, press control/alt/delete, and select lock computer.
- Look away when other individuals are entering their passwords.
- Log off a computer when no longer using it.

4.15 Confidential Information Storage

Do not store sensitive and confidential patient information on local computer workstations (C Drive), laptops (C Drive), and mobile devices such as, flash drives or memory sticks unless you are authorized to do so. Instead, store information on your network shared drive or departmental shared folders.

- If you are authorized to store sensitive and confidential patient information on removable media such as, CD-ROMs, DVDs, floppy disks, flash drives, or memory sticks, then you must secure this removable media by keeping them in a locked drawer or cabinet.
- Delete files that are no longer needed.

4.16 Software installation/removal procedures

Follow software installation and removal procedures:

- UPMC must own a valid software license for all software installed on its computers.
- Unlicensed software shall be removed or a valid license shall be acquired immediately.
- Don't download software that is not approved for UPMC computers.

4.17 Technical support

Seek technical support when necessary, especially when installing and removing hardware or software. Do not attempt to fix computer-related problems yourself. You may cause more difficulties by attempting to resolve the problem on your own. Contact the ISD Help Desk at 412-647-HELP (4357) or the designated help desk for your facility about any technical support problems or questions. Do not install or remove hardware - for example, modems, sound cards, video cards, or CD-ROMs yourself. Submit a request to complete the project.

- Seek technical support for hardware installation and removal.
- Do not attempt to fix computer problems.
- Do not install or remove hardware.
- Contact the Help Desk for technical support at 412-647-HELP (4357).

4.18 Remote access procedures

UPMC offers ways to access its network resources from off-site (remote) locations. Regardless of where you access information, remote or on-site, this information must remain confidential and secure. Follow established remote access procedures. Contact your Help Desk to discuss these solutions.

- You should not install any hardware, such as a modem or software used for remote connections, on a UPMC computer.
- Always contact your Help Desk for this service.
- Use approved solutions for accessing UPMC's network.
- Do not install any hardware that would allow remote connections.

4.19 Laptops and PDAs

Laptops and personal digital assistants (PDAs) often contain confidential information. Therefore, all staff should take the following security measures. Contact the ISD Help Desk with any questions.

- Physically secure laptops and PDAs.
- Use a password.
- Encrypt information.
- Do not leave a laptop or PDA unattended in a public place.
- The use of any unsecured wireless network is not allowed, unless the appropriate approval has been obtained.
- Confidential information should not be accessed without approval.

4.20 Disposal of Electronic Media

Electronic media must be disposed of properly.

- Floppy disks, CD-ROMs, DVDs, and backup tapes containing confidential information should be physically destroyed.
- This can be done by using a CD-ROM shredder or placing the items in designated shredding bins, which is the preferred method. Caution: The process of manually breaking a CD-ROM can cause sharp pieces of plastic to fly through the air.
- Special measures must be taken to remove confidential information from fax machines, copiers, printers, and other devices capable of data storage.
- Contact the ISD Help Desk at your facility to have the appropriate technical support staff remove all traces of confidential information from a computer hard drive and other devices.

5.UPMC Privacy and Security Policy Overview

- You are required to understand all UPMC privacy and security related policies. This section provides an overview of these policies. In addition to these, your business unit or facility may have additional privacy and security related policies or procedures. If you do not understand a policy or procedure, ask your manager for clarification.

Some forms such as the Authorization for Release of PHI, have been updated in accordance with applicable regulations.

5.1 UPMC Privacy and Security Related Policies

UPMC developed privacy and security policies that address a variety of topics. The complete text of these policies can be found in the system-wide policy manual located on Infonet.

5.2 Release of PHI

Strict rules apply to the release of protected health information (PHI) when necessary for reasons other than treatment, payment, or health care operations (TPO). These rules vary based on the sensitivity of the information. Please direct questions related to releasing patient information to your HIM department or your privacy officer.

- If you are involved with disclosing PHI, you are responsible for being aware of these rules.
- Generally patients must sign an Authorization to Release their PHI if for reasons other than TPO.
- If a patient pays for services out of pocket in full and supplies in writing their request that we do not share this information with their insurer we are not to release this information.
- A valid authorization must contain certain information.

5.3 Notice of Privacy Practices for PHI

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. Patients should acknowledge that they have received a copy of the notice. At UPMC, patients acknowledge they have received the notice by signing the Consent for Treatment Form. If you are unable to obtain a patient's acknowledgement, you must document the effort and the reason why the acknowledgement was not obtained. During emergency situations, the acknowledgement should be obtained within a reasonable amount of time.

- All staff should read the Notice of Privacy Practices. The notice may be downloaded from the HIPAA section of UPMC Infonet.

Notice of Privacy Practices (NOPP) describes:

- how PHI may be used or disclosed
- patient rights under HIPAA
- who to contact if patients believe their rights have been violated

5.4 Business Associates (Guidelines for Purchasing)

A business associate is an external individual, business, or vendor that uses Protected Health Information (PHI) to perform a service or provide a product on behalf of UPMC. These services may include, but are not limited to, legal, actuarial, accounting, consulting, management, administrative, accreditation, data aggregation, or financial services.

- UPMC is required to enter into a contract with a business associate that clearly defines the business associates responsibilities for using, sharing, and safeguarding PHI, including the reporting of any breach of protected health information.
- All business associates must enter into an agreement with UPMC to safeguard PHI.
- For more details about these terms and conditions, business associates should refer to the Purchasing section of UPMC's public website.

5.5 Use of PHI for Marketing

Marketing is defined as any type of communication that seeks to convince an individual to use or purchase a product or service. UPMC must request and obtain written authorization from an individual to use or disclose his or her PHI for marketing purposes.

Examples not considered marketing:

- face-to-face communications, such as when pharmaceutical samples are given to a patient during a doctor's office visit
- communicating additional treatment options, care management activities, or alternative care settings

5.6 Use of PHI for Fundraising

Fund raising refers to any activity to raise charitable donations that support research, education, or the advancement of health care activities within UPMC.

- Types of PHI that may be used for fund-raising purposes without obtaining the patient's authorization must be de-identified and include:
  - demographic information that does not identify the patient (age, race, gender, etc.)
  - dates that health care was provided to a patient
  - demographic information that does not identify the patient (age, race, gender, etc.)dates that health care was provided to a patient
- The Notice of Privacy Practices describes how a patient's PHI may be used for fund-raising activities.
- Use of other types of PHI which identifies the patient, requires a separate authorization from the patient.

5.7 Use and Disclosure of PHI for Research Purposes Pursuant to the HIPAA Privacy Rule

All research activities must be conducted in accordance with the rules of the Institutional Review Board (IRB).

- Patients must sign a research authorization for their PHI to be used or disclosed.
- De-identified information (as described in the HIPAA Privacy Rule) may be used for research without the patient's authorization.
- UPMC also uses external institutional review boards for clinical trials such as the Independent Investigational Review Board. For a complete list, contact the UPMC Clinical Trials Office.

5.8 Accounting of Disclosures of PHI

Accounting of Disclosures (AOD) is a summary of where a patient's PHI was disclosed and includes a list of those people who have received or accessed protected health information.

- Patients have a right to receive an accounting of disclosures and AODs must be maintained for six years.
    - Subject to a schedule established by federal law, UPMC must provide an accounting of disclosures of all individuals who have received or accessed a patient's electronic record for a period of three years prior to the date on which the accounting is requested.
    - In addition, business associates will also be required to supply an accounting of disclosures when requested.

5.9 Filing a Complaint - Complaint Management Process

Patients and staff have a right to file a complaint if they feel their privacy rights have been violated. There are many options for filing a complaint.

Staff can file a complaint by first contacting their manager or supervisor. If they are unable to or uncomfortable with doing so, then complaints can be filed by using the same methods available to patients as described below.

Patients (or parent/guardian/other authorized person) can file a complaint by:

- Informing a UPMC employee
- employee receiving a complaint must report it to the entity privacy officer
- contacting the entity's privacy officer

calling the:

- HIPAA Helpline - 412-647-5757
- Compliance Helpline - 1-877-983-8442 (anonymous option)
- Writing (paper or electronic) to the:

Secretary of the United States Department of Health and Human Services, 200 Independence Ave, SW Washington, DC 20201

5.10 Patient Access to PHI

Patients have a right to access and review their PHI. A patient must submit a written request and schedule an appointment at the facility where the treatment was provided in order to access his or her PHI.

UPMC may deny a patient access under certain situations:

- contains psychotherapy notes
- compiled for court proceedings
- physician determines not appropriate
- could result in danger to another person
- prohibited by law
-

5.11 Employees Accessing PHI

If an employee has an account for a UPMC clinical system, the employee is generally permitted to access the employee's medical information on that system. The exceptions are that (a) an employee is not entitled to access his/her behavioral health or drug/alcohol treatment information; (b) UPMC reserves that right to limit an employee's access to his/her medical information on UPMC Clinical Systems; and (c) an employee's use of UPMC clinical system must not interfere with the employee's or other staff's work.

- 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.
- Employees will be subject to disciplinary action if PHI has been accessed inappropriately and may be subject to fine, imprisonment and termination.

5.12 Patient Amendment to PHI

Patients may request to amend or correct their PHI, if they feel that UPMC has recorded incorrect or incomplete information about them. A patient who wants to amend his or her PHI must make a written request to the facility holding this where the medical information was created. The request must include the reason the information should be amended.

UPMC may deny a request when:

- request to amend is not in writing
- patient does not include a reason to support the request
- information was not created by the facility
- health care provider verifies the existing information is true and accurate
- facility must notify the patient in writing 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
-

5.13 Minimum Necessary Standards for Using PHI

Protected health information (PHI) is available to UPMC staff on a need-to-know basis. Need-to-know means that you rely on or need PHI in order to do your job.

- However, you should access only the minimum amount of information that you need to perform your job.
- For example, all of the patient's health information is available for a physician, nurse, or other staff member to use to provide direct patient care. However, this same information is not available to the hospital's telephone operator. The need-to-know information the telephone operator requires is the patient's name and room number.
- Accessing patient information that is not relevant to your job may result in disciplinary action, up to, and including termination.
- A log of all users accessing PHI via electronic means is available to monitor this.

If you are required to disclose PHI to someone for purposes other than treatment, payment or operations, such as a court order, **you must verify:**

- who the requesting party is
- that they have a need-to-know this information
- that only the minimum necessary information is provided

- If a patient pays for services out of pocket in full, and supplies in writing their request that we do not share this information we are not to release this information.
- Questions regarding the minimum necessary standards for using or disclosing PHI should be directed to your privacy officer or Health Information Management (medical records) department.

5.15 Reporting of Suspected Problems

It is every employee/volunteer's responsibility to be alert to unethical behavior or possible violations of UPMC policies.

There are many examples of inappropriate use or disclosure of protected health information.

These include but are not limited to:

- Faxing - If the patient's information is sent to the wrong fax number or wrong location, the doctor's office or requesting agent must report this to either HIM or their Privacy officer.
- Patient Identification - If a patient presents with identification that does not appear to be consistent with existing information, contact your privacy officer to notify him or her of the possibility of identity theft.
- Access/Disclosure - All inappropriate PHI access or suspected breach in security shall be reported in accordance with appropriate UPMC Policies.

Communicate your concerns and observations in a manner consistent with the chain of command. You should first contact your manager if you need assistance. If you are not comfortable or unable to follow the chain of command, the following additional resources are available:

- privacy officer
- compliance officer
- Corporate Compliance Office
- Human Resources
- Legal
- UPMC Compliance Helpline toll-free at 1-877- 983-8442 (anonymous)
-

UPMC prohibits retaliation against anyone for raising, in good faith, a concern or question about inappropriate or illegal behavior. Retaliation is not allowed against anyone participating in an investigation or providing information related to an alleged violation.

5.17 "Red Flag Rules": Reporting Suspected Identity Theft

Congress enacted the Fair and Accurate Credit Transaction Act (FACTA) of 2003 which amended the Fair Credit Reporting Act (FCRA) in response to the increase in identity theft. Subsequently, the Federal Trade Commission (FTC) issued the "Red Flag Rules".

The Red Flag Rules aim to protect the consumer from identity theft. This rule requires that any business entity ("creditors") who maintain an account ("covered account") which allows deferred payment and or credit to a client must implement a program to identify, detect, and respond to identity theft.

Identity theft occurs when someone uses another person's personal information to fraudulently obtain medical services (e.g. name, address, Social Security number, credit card number insurance information or other identifying personal information).

Red Flags are defined as any pattern, practice, or specific activity that could indicate identity theft.

- If you suspect that identity theft has occurred communicate your concerns and observations in a manner consistent with the chain of command. You should first contact your manager or supervisor who will perform an initial investigation. If you are not comfortable or unable to follow the chain of command, additional resources are available:

- privacy officer
- compliance officer
- UPMC Compliance Helpline toll-free at 1-877- 983-8442 (anonymous)

5.18 Theft and/or Breach of Personal Information

In General: A breach occurs when there is an unauthorized acquisition, access, use, or disclosure of protected health information. If you suspect that a breach has occurred, you should notify your supervisor or entity Privacy Officer immediately. If it is determined that there was a breach, UPMC will need to report the breach, including providing written notification to the affected patient(s).

- **Example:** Without a work related need, a nurse intentionally opens her co-worker's record.
- **Exceptions:** There are a variety of exceptions where a breach does not need to be reported, including situations, where it is unlikely that the information could be misused. However, this decision may only be made following an investigation by UPMC.